S. Hrg. 114–428

THE IRS DATA BREACH: STEPS TO PROTECT AMERICANS' PERSONAL INFORMATION

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

JUNE 2, 2015

Available via the World Wide Web: http://www.fdsys.gov/

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
95–655 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin *Chairman*

JOHN McCAIN, Arizona
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
KELLY AYOTTE, New Hampshire
JONI ERNST, Iowa
BEN SASSE, Nebraska

THOMAS R. CARPER, Delaware
CLAIRE McCASKILL, Missouri
JON TESTER, Montana
TAMMY BALDWIN, Wisconsin
HEIDI HEITKAMP, North Dakota
CORY A. BOOKER, New Jersey
GARY C. PETERS, Michigan

Keith B. Ashdown, *Staff Director*
Gabe Sudduth, *Senior Professional Staff Member*
Gabrielle A. Batkin. *Minority Staff Director*
John P. Kilvington, *Minority Deputy Staff Director*
Stephen R. Viña, *Minority Chief Counsel for Homeland Security*
Laura W. Kilbride, *Chief Clerk*
Lauren M. Corcoran, *Hearing Clerk*

CONTENTS

WITNESSES

Tuesday, June 2, 2015

Alphabetical List of Witnesses

APPENDIX

THE IRS DATA BREACH: STEPS TO PROTECT AMERICANS' PERSONAL INFORMATION

TUESDAY, JUNE 2, 2015

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 2:03 p.m., in room SD–342, Dirksen Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

Present: Senators Johnson, Ayotte, Ernst, Carper, Baldwin, Booker, and Peters.

OPENING STATEMENT OF CHAIRMAN JOHNSON

Chairman JOHNSON. This hearing is called to order.

I want to thank the witnesses for appearing here today and for your thoughtful testimony. I am looking forward to it as well as your answers to our questions.

We are going to have a little bit of a scheduling struggle here. We have some votes at 2:30, and I think we will try and keep the hearing going as best as possible, depending on what Members we have that can maybe fill the chair. But, again, this hearing is all brought about by the revelations last week. I got a call from the Commissioner of the IRS informing me of the—it is not necessarily a breach. I guess you could call it a breach, but it is not your standard cyber attack that we have been talking about. This is just simply a breach of confidentiality in a system that is meant to assist taxpayers, and it brought all kinds of questions to mind: What type of authentication system, what kind of security system is being utilized here, not only within the Internal Revenue Service (IRS) but also other agencies in the government? And what we are starting to find out is, well, different agencies—the Social Security Administration (SSA), we have the Centers for Medicare and Medicaid Services (CMS) with Healthcare.gov, similar types of systems. I know the IRS now has shutdown the Get Transcript program. These are some serious issues that we need to address.

Because we are short on time, I will have my opening statement entered into the record,[1] without objection.

Senator CARPER. Without objection.

Chairman JOHNSON. Senator Carper is generally pretty good about that. But, again, these are serious issues. Because we had the compromise of about 100,000 taxpayer Get Transcript accounts,

[1] The prepared statement of Senator Johnson appears in the Appendix on page 47.

the IRS has already tracked that we have had about 13,000 questionable tax returns filed, and that is, of course, why the hackers are doing this, is to get the information to quickly file a tax return with good information so it is not flagged by the IRS so they can claim tax refunds and obtain those before the taxpayer whose identity has been stolen even knows about it.

According to my briefing here, about $39 million has already been transferred from the IRS to those criminals. We do not know how much more widespread this will be, not only in the IRS but also Social Security, CMS, the Consumer Financial Protection Board (CFPB). We have a lot of questions that will—this is just the beginning hearing to get to the bottom of it.

With that, I will turn it over to our Ranking Member, Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thanks, Mr. Chairman. Thanks for holding the hearing, and to each of our witnesses, thanks so much for joining us.

I had a Finance Committee hearing earlier today, and John Koskinen, who is the Commissioner of the IRS, was one of our two witnesses, joined by the Inspector General (IG) for the IRS as well, General George, so I am getting a full dose of this today. In fact, we are getting a full dose of this across America. And it is a timely hearing. Sorry we have to have this kind of hearing, but it is important that we do have a number of them.

Nearly every day, we learn of another major cyber attack or data breach on an American company or organization. In many ways, we are dealing with what is really an epidemic of online theft and fraud. That epidemic is growing at an alarming rate and continues to victimize and frustrate more and more of us, including my own family.

Over the past several months, for example, we witnessed several major companies in the health care sector suffer major data breaches. And, of course, we know that our government networks are under constant attack in cyberspace. These attacks are growing ever more sophisticated, too. That is happening at least in part because our defenses are getting better. Still, we must do more to stay ahead of those that would do us harm. And we must learn from those instances when criminals have been successful in getting past the protections we have put into place and can create havoc for us.

Today we are going to take a closer look at the recent cyber attack on the IRS. We will examine what went wrong, how the IRS is trying to repair the damage, and what we can do to reduce the likelihood that something like this does not happen again, either at the IRS or some other place.

From what we know so far, though, the attack on the IRS appears to have been an especially sophisticated one. We also know that the IRS had defenses and fraud prevention measures in place at the time of the attack. Yet despite the precautions that were taken, skilled criminals were able to use innovative tactics to trick the IRS system into releasing past tax returns. Given the vast amounts of sensitive information the IRS possesses, it is critical that the agency continues to do more to protect the American taxpayer. In fact, all agencies need to step up their efforts and improve their cybersecurity posture. The wake-up call has been ringing for years now, and we need an all-hands-on-deck effort to respond to it.

As we know, cybersecurity is a shared responsibility. Those of us here in Congress have an obligation to ensure that agencies have the funding, the tools, and the authority that they need to adequately protect their systems from attack. Unfortunately, Congress has significantly reduced IRS funding in recent years, and we have done so while also tasking the agency with far greater responsibilities. In fact, the IRS is operating at its lowest level of funding since fiscal year (FY) 2008. These cuts have had real consequences for the agency and for American taxpayers. I look forward to hearing from the Commissioner today about what he needs to better protect his agency from fraud and cyber attacks.

Here in the Committee, we have been working hard to address our country's cybersecurity challenges, I think to good effect. Last year, our efforts led to the enactment of four key pieces of cybersecurity legislation. One of these bills updated the Federal Information Security Management Act (FISMA), to better protect Federal agencies from cyber attacks. Another codified the DHS cyber operations center. And two others strengthened the cyber workforce at the Department of Homeland Security (DHS).

This year, I introduced an information-sharing bill and have been working closely on this issue with our colleagues on the Senate Intelligence Committee. I have also been working closely with Senator Blunt on data breach legislation that will create a national standard for how we protect data and consumers.

We must move these important pieces of legislation and provide our agencies with the resources they need to tackle the growing cyber threats.

With that, let me thank you again for joining us here today. We all look forward to your testimony.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Senator Carper.

It is the tradition of this Committee to swear in witnesses, so if you will all stand and raise your right hand. Do you swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. KASPER. I do.

Dr. FU. I do.

Mr. GREENE. I do.

Chairman JOHNSON. Please be seated.

Our first witness is Michael Kasper. Mr. Kasper is a software engineer from Poughkeepsie, New York—love that name—testifying as a victim of identity theft in the IRS data breach that is the subject of this hearing. Mr. Kasper.

TESTIMONY OF MICHAEL KASPER,[1] POUGHKEEPSIE, NEW YORK

Mr. KASPER. Yes, I should clarify. I am one of those 13,000 who had their transcript and their refund stolen. But before I launch into my story, I want to share a few of the things I learned along the way, specifically that the Get Identity personal identification number (PIN) function on the IRS website uses the same authentication as the Get Transcript, so I think that that should also be investigated before any of the victims are hit 2 years in a row. E-file PINs are even easier to get. In my opinion, PIN numbers should probably only be sent by mail, like banks and credit cards do at this point.

I do not believe that punishing the IRS by cutting funds is the answer. Indiana is an example where they spent $8 million on ID theft and saved $88 million as a result, preventing that. So I think you could see a large return because there is so much of this going on. Over a million people were victims of stolen identity refund fraud last year, $5.8 billion lost. I was trying to look for analogies for that. There are usually around 5,000 bank robberies a year averaging a similar amount, $6,000 each. So this is equivalent to 1 million bank robberies every year. In other words, those 5,000 banks are each getting robbed again 200 times. It is a massive problem. If the IRS cannot handle investigating these cases, maybe they should be given to the Federal Bureau of Investigations (FBI). I mean, single-digit audit rates for taxpayers make sense, but I do not think single-digit criminal investigation rates for these cases do make sense. I have heard that that is around what they do. I have a source I can give you offline.

The other thing they could do, which the Senator from New Hampshire brought up, about sharing information with the taxpayers so that they can pursue it themselves, like I did, giving you a copy of the tax return so you can call the bank, call the local police. It is important when they share those that they do not redact the payment address or bank account information, because that is how I was able to get a result in my case.

On February 6, I tried to file my taxes. Later that night, Friday evening, I got a rejection. Someone had already filed.

So on Monday morning, I called the IRS, and they confirmed my identity by asking tax history-related questions and showed me that a deposit was being made the same day that I was calling into somebody's account, but that it was too late to stop it at that point. And because I had not called a day earlier, now they had to wait until all my paperwork was processed by mail, which could take up to 6 months.

They said they would not contact the bank to tell them about it, and they would not tell me what the bank account information was so I could do that myself. So I was frustrated by that. That is when I tried the Get Transcript function on the IRS website to see if I could get a transcript and found out someone else had already registered their e-mail address with my Social Security number (SSN). IRS e-Services was able to disable online access to my account, but they would not tell me what the e-mail address was, but they did

[1] The prepared statement of Mr. Kasper appears in the Appendix on page 51.

think it was suspicious for some reason. So that was February 9 when I called and talked to them about that.

I was able to get a transcript by mail, though, which is when I found out that whoever had filed had seen my 2013 return because the information was almost identical. It was kind of scary.

So then I found out I could get a photocopy for $50. They had been telling me I could not get the information, but if I paid $50, I could get it. So March 17, I got a photocopy of the return and saw the bank account number. I also saw they filed a corrected W–2 to get $6,000 more, almost $9,000 total.

But I contacted the bank in Pennsylvania. They confirmed a deposit was made in—I guess the meta data in the deposit actually showed my name and my Social Security going into someone else's checking account. So they told me the location, Williamsport, Pennsylvania, where all the money was withdrawn, and I contacted the local police there. The bank fraud department also investigated and asked them to return it. But the local police called me back right away, actually, and went and interviewed the person, and it was ironic because the same day that they interviewed the suspect, I got a letter in the mail from the IRS that they had 6 weeks later received my documentation and that they would get back to me in 6 months. So it was a pretty stark contrast.

I also got a letter that week from Anthem Health Care offering me free credit monitoring. I do not really know if that is related to how my information was obtained. But at this point, it seemed like the case was solved, but it turned out to be more complicated because the account holder claimed she had responded to a Craigslist ad offering a job opportunity. Money was deposited into her account, and then she wired large amounts of it to Nigeria through Western Union, apparently not really suspecting there was anything wrong, or at least not at first. But she also got someone's deposit from South Dakota.

I finally got my refund check on May 12. I really think contacting the bank myself helped make a difference. The woman who got my refund has been arrested by the Williamsport police, so that is some progress on my case. But I have heard from the IRS my case is confirmed, but I do not know if they investigated it criminally.

Chairman JOHNSON. Thank you, Mr. Kasper.

Our next witness is Dr. Kevin Fu. He is an associate professor of electrical engineering and computer science at the University of Michigan where he specializes in cybersecurity and trustworthy computing. Dr. Fu.

TESTIMONY OF KEVIN FU, PH.D.,[1] ASSOCIATE PROFESSOR, DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE, UNIVERSITY OF MICHIGAN

Dr. FU. Good afternoon, Chairman Johnson, Ranking Member Carper, and distinguished Members of the Committee. I am testifying before you today on the use of what is known as "secret questions and instant knowledge-based authentication (KBA), related to the recent IRS breach. I will explain the key properties of instant KBA and try to give you a better understanding of the current challenges and vulnerabilities, and I will close with some recommendations on what can be done in the future to avoid similar large-scale breaches.

At Michigan, we teach programming to over 1,300 undergraduates each year, but we teach a rigorous course in computer security to just slightly more than 400 students, and I regret that means most of these programmers have no formal security training in case you are wondering how the security vulnerabilities are born.

But there are three basic ways to authenticate an identity; that is, something you are, such as a fingerprint; something you have, such as mobile phone; or something you know, like a password or, in this case, a secret question. Or as we like to say in the academic circles, it is something you were, something you lost, or something you forgot. But today we will talk mostly about knowledge-based authentication, and financial websites often ask users to opt in to store answers to personal questions, such as "Where did you meet your spouse?" to serve as a backup mechanism to reset lost or stolen passwords. However, this is not the kind of instant KBA we are talking about today.

In instant knowledge-based authentication, there is no opt-in process. Instead, the website—in this case, the IRS Get Transcript site—quizzes a user with information gathered from credit reports and other sources to gain confidence in a claimed identity. For example, a user might be asked to identify the bank holding their mortgage from a multiple choice list.

Now, let me highlight some of the strengths and weaknesses of instant KBA. The main strength is that it is fairly easy to use, relatively easy to use. However, the major limitation is that the security rests on the crumbling assumption that personal information is secret.

Now, instant KBA does increase the difficulty of attack, but sophisticated adversaries can, nonetheless, circumvent the protections at unprecedented scale. A seemingly unrelated compromise at one site, such as Target or Anthem, could affect the security at a different site, such as IRS.

Now, only using a stolen wallet, an attacker may struggle to answer four instant KBA questions like you will find on the IRS website. Unfortunately, this threat model is no longer realistic as countless databases of personal information have been breached.

Also, taxpayers get no chance to opt out of the risks of instant KBA, and let me point out that the National Institute of Standards and Technology (NIST) explains in a technical report—I will just cite one phrase—that they write that it is "inappropriate to invol-

[1] The prepared statement of Dr. Fu appears in the Appendix on page 53.

untarily expose the privacy of unknowing citizens to the risks of an instant KBA authentication scheme unless the risks for any individual citizen is very close to zero."

Now, there are alternatives that might improve the effectiveness of the authentication at IRS and other Federal agencies serving the citizens of this country. One example is what is known as "second-factor authentication." The use of a second factor paired with instant KBA can make it more difficult for an adversary to impersonate a taxpayer. So a popular second factor is possession of a mobile phone, proving that you have a mobile phone associated with your account.

Now, notification is also a challenge. The IRS could attempt to use contact information from tax returns to reach out to the taxpayer or the accountant to warn of an attempted download of a transcript, but such systems are still subject to things known as "phishing attacks" or "social engineering" and also would remove the instant gratification of the download.

Now, NIST launched the National Strategy for Trusted Identities in Cyberspace (NSTIC) to improve authentication of identities, and has a 10-year road map that may help the IRS to develop a more cost-effective authentication strategy that works well.

I would like to draw attention to what is used in the financial sector, which has been subject to widespread fraud by callers on the phone who attempt to engage in identity theft. One novel approach already being used today is to identify repeat fraudsters by the manner in which they speak and their cadence. So it makes it harder for an adversary to impersonate 100,000 people at once.

Now, let me summarize and I will leave the rest for my written testimony. There will always be fraud, but a reasonable goal is to make it difficult for a single adversary to commit wide-scale automated fraud. Some recommendations include asking NIST to help develop KBA security and performance standards so that Federal agencies can more meaningfully debate acceptable residual risk to avoid using Social Security numbers or financial records as secrets for single-factor authentication and consider pairing KBA with a second factor of authentication, such as Short Message Service (SMS) messages or voice-based fraud detection.

Finally, encourage research collaboration between cybersecurity experts and social and behavioral science to carry out human subjects experiments that help to measure the risks and benefits of knowledge-based authentication.

Thank you. I am happy to answer any questions you may have. Thank you.

Chairman JOHNSON. Thank you, Dr. Fu.

Our next witness is Jeff Greene. Mr. Greene is the Director of government affairs, North America, and senior policy counsel at Symantec Corporation where he focuses on cybersecurity, the Internet of Things, and privacy issues. Mr. Greene.

TESTIMONY OF JEFFREY E. GREENE,[1] DIRECTOR, GOVERNMENT AFFAIRS, NORTH AMERICA, AND SENIOR POLICY COUNSEL, SYMANTEC CORPORATION

Mr. GREENE. Chairman Johnson, Ranking Member Carper, Members of the Committee, thank you for the opportunity to testify. I am going to talk a little bit about the broader cyber threat environment to put this particular attack into context.

As the largest security software company in the world, our global intelligence network is made up of millions of sensors, so we have a pretty broad perspective on what is going on in the Internet today and the Internet threat landscape.

Recent headlines about cyber attacks have focused a lot on data breaches across the spectrum of industries. These compromises have deep impacts on individuals who have their identities compromised and have to worry about it, companies that have their systems penetrated, and also government worried about protecting their citizens and also about how to catch the criminals.

The magnitude of the theft of personally identifiable information (PII), is really unprecedented. Over the past 3 years, approximately 1 billion identities have been exposed, and those are just from the breaches that we know about today.

The attackers run the gamut. They can include highly sophisticated, highly organized criminal enterprises, individual cyber criminals, so-called hactivists, or State-sponsored groups. Different attacks range from distributed denial of service (DDoS), attacks to highly targeted to widely distributed financial fraud schemes.

Now, a DDoS attack is an attempt to overwhelm a system with data. Targeted attacks will typically try to trick someone into opening either an infected file, go to a bad link, or something similar. And, of course, there are scams and blackmail schemes trying to gain money that are still out there.

Some of these will fill your screen with pop-ups telling you that your computer is infected with a fake virus. Other of them will lock your computer, purport to be from law enforcement, and assert that you have some type of illegal content, asking for a fine to be paid in order to regain your computer.

The most recent scheme, though, has gone from trickery to straight-up blackmail. Your computer will be locked. You will get a screen saying your hard drive is encrypted. Typically it will be, and the only way you get access to your data is by paying a ransom.

We are also seeing increasingly complex and sophisticated efforts by criminal syndicates to use personal information, some stolen, some publicly available, to perpetrate a variety of different scams, and that is what happened here with the IRS.

Critical infrastructure like the power grid, the water system, and mass transit are also at risk. Last year, we issued a report about an attack that we called “DragonFly” that was focused on the energy sector. It was not the first we have seen on the energy sector. In fact, in 2012, cyber attackers mounted a campaign against the Saudi Arabian national oil company and destroyed 30,000 com-

[1] The prepared statement of Mr. Greene appears in the Appendix on page 66.

puters. They essentially wiped them and had them display an image of a burning American flag.

Last year, the German Government disclosed that there was a cyber attack on a steel plant that resulted in massive physical damage. So we are seeing it across sectors.

Most of these attacks start with a common factor, a compromised computer, and we frequently hear about advance persistent threats (APTs). But the discussion of cyber attacks too often ignores the psychology of the exploit. Most rely, as Dr. Fu said, on social engineering, essentially trying to trick you into doing something that you would never do if you were fully aware of the import of your actions. In short, a successful attack is usually as much psychology as it is technology.

Good security stops most of these attacks, which often seek to exploit older, known vulnerabilities. But many organizations and individuals do not have security in place or have not patched their systems, and they remain vulnerable to existing problems.

Systems that use these knowledge-based authentication systems, or KBA, are increasingly under attack, and we are seeing an uptick of these second-generation compromises where attackers are using this personal information previously stolen or publicly available, harvesting it and using it to either access data or establish new accounts for future fraud or direct theft.

To combat these threats, we work with government and industry across the world. We have been involved in several major botnet takedowns. These are networks of zombie computers that have led to some prosecutions. And we also are part of what we call the "Cyber Threat Alliance." We joined with the Palo Alto Networks, McAfee, Fortinet last year to co-found this. This is a group of cybersecurity providers. We share advance cyber threat information, at the same time protecting the privacy of our customers.

So what can all of us do at an individual level? Good protection requires a plan. Strong security should include intrusion protection, reputation-based security, behavioral based blocking, data encryption backup, and data loss prevention tools. That is organizationally. While the criminals' tactics are constantly evolving, basic cyber hygiene is still the simplest and the most cost-effective way to stop a lot of the attacks out there.

In fact, early this year, the Online Trust Alliance issued a report that showed that 90 percent of the major breaches from last year would have been prevented if businesses had implemented basic cyber best practices.

With that, I appreciate the opportunity. I am happy to take any questions you may have.

Chairman JOHNSON. Thank you, Mr. Greene.

I will start the questioning with Dr. Fu or Mr. Greene, whoever can answer the question. Where does the IRS obtain the information they use for the knowledge-based authentication? Where is all the data coming from?

Dr. FU. So I am not entirely familiar with where IRS obtains its data. I am familiar with sister sites where they obtain their data.

Chairman JOHNSON. OK, go ahead. I just want to know where most people obtain this, because this is all commercially available, correct?

Dr. FU. Correct. The private sector offers services for this instant KBA. For instance, one provider, Experian, is used by some Federal sites to do exactly the same kind of purpose as the Get Transcript, for instance, the Social Security Administration.

Chairman JOHNSON. And where does Experian get all the data from?

Dr. FU. I believe they obtain it from credit reports and other financial data.

Chairman JOHNSON. Does anybody else want to add to that? Go ahead, Mr. Greene——

Mr. KASPER. On the IRS website, if you have an Equifax credit freeze, they will not get asked the questions, which makes me suspect it might come from Equifax for the IRS.

Chairman JOHNSON. OK. What I am trying to get at is where do the data mining companies obtain the information from. Every time you click on an app, agree to the privacy contracts, applications, the cookies? In other words, there is a constant flow of information and personally identifiable information when we are all using our iPhones and our mobile devices. Correct?

Mr. GREENE. Sure. The individual app will depend upon what is in the end-user license agreement. There are data aggregators whose business it is to aggregate data from whatever sources and to sell it. And as Dr. Fu said, a lot of it is available from credit reports and elsewhere. So the data aggregators put that together, and they use that. And most, whether government or private companies, that use KBA use one of the credit bureaus or some similar type of data aggregator for their KBA services.

Chairman JOHNSON. What I would like to do, because I think, Dr. Fu, you have been prepped for this, we have a chart[1] here of four questions this was taken from the Healthcare.gov website in terms of the authentication we are talking about here. Let us just go through and can you describe for the audience and for the Members here exactly how easy this is to defeat with very limited information or knowledge? The first question is, “Please select the county for the address you provided.”

Dr. FU. Right. So I think some context is important. This is the screen presented for the instant KBA. You get four questions about your personal finances to answer, but before you get to this page, you first have to enter your name, your Social Security number, and your address. So the adversary who has already reached this stage already has quite a bit of personal information.

So, for instance, if you already know the address of the taxpayer, it is very easy to figure out where the taxpayer lives, in what county.

Chairman JOHNSON. So not a real challenge.

Second question: “According to our records, you previously lived in Pickwick. Please choose the city from the following list where the street is located.”

Dr. FU. Yes, so in this particular case, you could rule out streets that make no sense in the particular address of the taxpayer and basically have a very good chance of getting the correct answer.

[1] The chart referenced by Senator Johnson appears in the Appendix on page 85.

Chairman JOHNSON. No. 3: “Please select the city you previously resided in.”

Dr. FU. Right. So because these are culled from financial records and if the adversary does have access to breach data, this will be readily available.

Chairman JOHNSON. And, “According to our records, you graduated from which of the following high schools?”

Dr. FU. Right. So with Facebook accounts today, it is fairly trivial to figure out a high school somebody goes to. Moreover, if one of your friends posts something about you and you can figure out their high school, there you have it as well.

Chairman JOHNSON. Again, when we go back to just these highly publicized cyber attacks where all this PII has been mined, an earlier witness—I cannot remember which one—said about a billion individuals with their PII compromised, within the criminal networks, this is the kind of information that a criminal would have. They would basically have all this information already, correct? Because it is the exact same information that these data mining companies are already obtaining. So you have a perfect match of the information that the data mining companies are using with the information that has been criminally obtained through these attacks. Is that roughly correct?

Mr. GREENE. Roughly correct, yes. As more PII is stolen, the effectiveness of the KBA is going to go down, and you need to look at other steps to—you can still use KBA as part of the security procedure, but there are new steps, there are additional steps you can put in place to try to raise the level of security there. And Mr. Kasper mentioned out-of-band of communication like mail. So you go through these steps. You get to the end of it. Instead of saying, OK, we now know you are Jeff Greene, it says we are going to send a piece of mail to Jeff Greene’s address with a PIN number or some identifying number, and that would make it much more difficult for the criminals because that relies on the known address.

Chairman JOHNSON. So, again, the point of this is if a criminal has all that personal information, they have all this information already, basically. So this is very easy for them to accomplish what they did with the IRS. Correct?

Mr. GREENE. Yes——

Chairman JOHNSON. And, obviously, it is pretty simple, because they attempted 200,000 accounts, and they got into 100,000.

Mr. GREENE. Correct, on an individual level, yes.

Chairman JOHNSON. Mr. Kasper, I would like to just have you describe your frustration in trying to deal with the IRS once you understood—which, by the way, your case was first published, what, March 15?

Mr. KASPER. Well, March 30. I think it was March 30.

Chairman JOHNSON. OK. But, again, it was somewhat publicized. I know we have either from the testimony and discussions with the IRS, they were fully aware of this, and yet they made a decision to continue with this type of authentication.

Mr. KASPER. I remember Brian Krebs said that the U.S. Treasury Inspector General for Tax Administration (TIGTA) web was a frequent visitor to his site in his refers when he posted the article. So I think TIGTA was aware.

Chairman JOHNSON. So, again, just describe to us, kind of tell your story in terms of when you found out about this, you started contacting the IRS, how they responded.

Mr. KASPER. Yes, it was frustrating not being able to find out who had stolen my information because I did not know how they had gotten it. I did not know if there was a virus on my computer. I did not know if someone had stolen something from my home. I did not know how the information had gotten out there. And there was nothing that I could do about it other than wait 6 months. I went to my local IRS office. They said, “We cannot help you.” They literally, could not give me any more information now that I had reported it as fraud.

Chairman JOHNSON. Did they give you any reason why they could not help you further?

Mr. KASPER. They said privacy rules. At every step of the case, when I tried to get more information, they would say privacy rules prevented them from doing that, when the person who they were protecting had already taken advantage of my privacy.

Chairman JOHNSON. OK. Well, we will have the Commissioner here in the next panel, so we will ask him exactly what those privacy rules are. Senator Carper.

Senator CARPER. Thanks, Mr. Chairman.

Mr. Kasper, you talked about what might not be helpful in deterring similar attacks in the future, and I think you mentioned the amount of resources that we, the Congress, provide to the IRS to do the job. Would you just go back and sort of revisit what you said to us?

Mr. KASPER. Yes, I was referring to how in Indiana they were using analytics-based methods of detecting fraud and additional verification, and basically had invested $8 million additionally into trying to prevent this thing; whereas, at the IRS I understand they have had like a 5-year hiring freeze, 20-percent budget cuts, so that they are not doing those types of things, as far as I understand.

Senator CARPER. Commissioner Koskinen was before us today in the Finance Committee this morning, and we talked a little bit about this. We talked about cost-benefit payoffs, and he was talking about fairly senior-level IRS employees that are schooled in the cyber world, cyber warfare, and that they are unable to retain a lot of them. These people are highly in demand. And for a relatively modest amount of money, we will say in the million dollars or two, they were—instead of paying that money in order to attract and retain the kind of talent that they needed, they incurred losses many times that amount. How does that strike you?

Mr. KASPER. Yes, it seems like there could be a very big return on investment for trying to prevent this fraud more, and especially in the technology industry, there is a lot of competition for talent. And going to work for the IRS is not on the top of people’s list when they are looking at which high-tech company they want to go work for, when you have the budget restrictions and just other factors with trying to get people to go and work there and help them with this problem—although, they have a lot of people working on it who are doing a lot of good things, but they are not able to keep up with the cyber criminals.

Senator CARPER. All right. When we had Commissioner Koskinen before us this morning, I asked him, in terms of the way the IRS is treating folks who are victimized, if you will, because of these attacks, I asked him how the Golden Rule played into that in terms of treating people, in this case those who were victimized. How do we treat them in a way that is consistent with the Golden Rule, treat other people the way we want to be treated? Would you just maybe draw on your own experience and see if the way you were treated was consistent with treating others the way we would want to be treated?

Mr. KASPER. Well, I made the analogy to my contact with the local police department, which was not even in the same State where I lived, but the IRS has an identity theft hotline dedicated for all the people who call, but all they do is sort of like empathize with you, tell you, the different steps you can take to put a freeze on your account. They cannot really do anything for you. So you really cannot get any help directly from the IRS. They go off and they investigate your case, which they tell you right off the bat could take 6 months, and you really do not get any more information than that once you report it. It either gets resolved or it does not. They never tell you why. Wanting to know is a big part of the problem. You want to know what happened, and you cannot find out.

Senator CARPER. Let me ask Dr. Fu and Jeff Greene, and we will come back to you, Mr. Kasper. But if you were in our shoes and you were a member of the Homeland Security Committee interested and concerned about these issues, maybe you know people who have been hacked, maybe you have been hacked yourself, give us one or two things that you would do if you were in our shoes. I think one of you maybe once worked over in the House and had a chance to wrestle with these kinds of policy issue. So, Dr. Fu, give us one or two things that we ought to be doing in response.

Dr. FU. Well, from a policy point, actually I will refer to Mr. Greene; he talked about the psychology of the exploit. And one of the problems is on the science and engineering side there is very little understanding about how to measure these kinds of authentication systems, how well they work. There are quite a few negative results about how they do not work, but there is very little on the instant KBA. So encouraging those in academia, for instance, who work in cybersecurity to also work with those in the social and behavioral sciences could be helpful in discovering what kinds of authentications will work well for the entire U.S. population. That is one example.

Senator CARPER. OK. Do you have another one?

Dr. FU. Well, on the technological side, there are issue approaches like the two-factor authentication I mentioned. It is interesting to note that IRS did use a second factor of e-mail confirmation and, in fact, Google in a recent report published last week has recommended that you do that. And so the IRS did follow that recommendation, yet the intruders did still circumvent it.

Senator CARPER. How do you suppose they did that?

Dr. FU. I would imagine——

Senator CARPER. They work for Google?

Dr. FU. No, I do not work for Google.

Senator CARPER. No, I was saying that——

Dr. FU. Oh, I am sorry. My understanding when you register on the Get Transcript site is that you register an e-mail address, and you have to wait to receive a confirmation before you can go to the next step of filling out those four personal questions. So the adversary had to set up presumably a large number of e-mail accounts in order to receive that confirmation code to go to the next step. However, had they instead also paired it with some kind of phone number, it would increase the difficulty of having to compromise multiple systems.

Senator CARPER. All right. Thanks.

Mr. Greene, let us just say you are back in your old job over in the House and giving advice to guys and gals like us. What advice would you have for us?

Mr. GREENE. I think on the technical side, Dr. Fu said about encouraging two-factor authentication and recognizing there is a difference between identity verification when you initially set up an account. If you are sending the confirmation to the e-mail you asked for when they set up the account, it is circular. So you are still dealing with the same person, some type of out-of-band communication, whether through the phone or through a letter. So that is on the front end.

On the back end, once you have established the account, using some kind of two-factor authentication to make sure that no one has the stolen information the Chairman was talking about is important on the policy side. Research and development (R&D) and technical experts, the Science, Technology, Engineering and Math (STEM) training, I am sure you have heard that frequently we need more STEM experts. Information-sharing legislation will help, it will not be a panacea. We do encourage it. We just caution that it is incremental steps to fighting this. Those are several of the things that we would like to see. The government can set an example. If we can improve the use of KBA through two-factor in the government, I think the market and the private sector will follow.

Senator CARPER. All right. Thank you so much.

Chairman JOHNSON. Senator Ernst.

OPENING STATEMENT OF SENATOR ERNST

Senator ERNST. Thank you, Mr. Chairman, and thanks to our panelists for being here today. This is a very timely issue. I am glad we are able to discuss it right away, so I thank the Chairman and the Ranking Member for calling this hearing.

I do have, as I am sure most folks do, very serious concerns about the implications of this type of data getting out there and how easily it seems to be obtained by these people hacking into different systems. So I look forward to learning more about it and hearing your additional thoughts on it.

But what I would like to find out just from you, either Dr. Fu or Mr. Greene, is: Are there readily available private sector solutions for this that could be compared? The website you talk about the KBA. Are there private sector firms that use this type of information? And what is the best way to replace what we are doing now with a better, more secure system?

Mr. GREENE. So there are security measures, certainly, Senator, you can put in place. Many of the KBA back ends are provided by the private sector and, in fact, are used by the private sector. The security that worked 3 to 5 years ago is not working as well today because of the information that was stolen.

Through the initial log-in process, when you are setting up the account, there are two ways I look at it. One is: How do you prevent a fraudulent account from being set up? How do you stop it before it happens? And that would be through some form of two-factor authentication, improving KBA, and there are different ways to do it, one of which we have talked about, the phone or a letter.

On the back end, to try to see who is doing this activity, there are ways to basically take the data logs from the servers that are logged in, perform analytics on them, and see if you are seeing a pattern of activity that is indicative of some level of fraud.

Now, to some degree, for a few people, the horse is going to be out of the barn at that point, because you may already have some false log-ins. But you need to be looking at it from both ends, and we are never going to be able to stop 100 percent of it. But as the criminals get more sophisticated, the tools that worked well become less effective. And I think that is where we are with KBA, and there are ways to improve it going forward.

Senator ERNST. Dr. Fu.

Dr. FU. Well, let us see. I think I have two different responses. One is NIST, so NIST actually has proposed this 10-year road map called the National Strategy for Trusted Identities in Cyberspace, and, in fact, they already have given advice to IRS, and there is a published report. And I think that the Federal systems will find better authentication systems if they do engage with NIST and take the advice of NIST's independent, non-regulatory experts. They have a wealth of information on the technologies, the risks, the benefits.

There is also a number of companies working in the two-factor authentication space. I do not know any that specifically work on, for instance, protecting taxpayer information, but one company local in Ann Arbor, Duo Security, for instance, uses a mobile phone as a second factor. So when they attempt to have their customers log in to some kind of service, not only do you need to have a password, but you need to have a mobile phone present, and the idea is that it is more difficult for an intruder to physically steal your mobile phone if they are somewhere in a foreign country.

There is also some interesting innovation by a company that I believe had come out of Georgia Tech, PinDrop Security. They actually work for financial services companies. They listen to the audio of the phone calls as people call in, and they are able to actually identify the repeat offenders who are calling in pretending to be other people based on the delay in the phone line from what country they are coming from, some interesting characteristics of the copper wires. You could use some of these advanced technologies not to eliminate but at least reduce the risk of fraudsters trying to go from one fraudster doing 100,000 accounts to at least making it more difficult to scale up to so many different accounts from one adversary.

Senator ERNST. Thank you. And, Mr. Kasper, I am sorry you have had to go through this experience, as so many others have. You had indicated that the IRS thought the e-mail account—and maybe I read this somewhere, that the e-mail account was suspicious. Was that from your testimony or was that somewhere else that I read that?

Mr. KASPER. Yes, I do not remember the exact words that they used, but when I was on the phone with them, they said, "Hmm, yes, that does not seem right," or something like that.

Senator ERNST. Yes, it makes me wonder, especially if these are coming from foreign adversaries, that if they have a different e-mail address that indicates it is coming from, originating from a foreign nation, that that is something that could be flagged to require additional information. I do not know if that is something else that could be considered.

Mr. KASPER. Yes, there are probably some analytics they could do just on the domain name, because they highlighted that 200,000 had these suspicious domain names. But it is also very easy to get a Hotmail or Yahoo e-mail account and automate that and have some type of process for taking advantage of it.

So there are things that it seems like they were not doing with monitoring those servers and transactions that they could have been doing.

Senator ERNST. Well, thank you.

Mr. KASPER. Like the Internet Protocol (IP) addresses and all that.

Senator ERNST. Exactly. And do any of you know, has the IRS reached out to any private sector providers to try and correct the system that they have now or done any sort of control measures? Do any of you know?

[No response.]

OK. That is a question for our next panel. Well, I appreciate it very much. I thank you for your time, and hopefully we can get to the bottom of this and find better ways of utilizing our information systems. Thank you.

OPENING STATEMENT OF SENATOR AYOTTE

Senator Ayotte [Presiding.] While the Chairman is voting, I am going to sit here, but it is my turn to ask questions, so I actually wanted to ask you, Mr. Kasper, you referenced the recent response I got from the Commissioner of the IRS, and what actually prompted me to write this letter, similar to your experience, is that I have had a number of constituents come to me and some really troubling cases where they just were getting the runaround from the IRS, that they could not actually get the fraudulent return so that they could then pursue protecting themselves in the way that you did. And so I was glad, obviously, to hear that the Commissioner is now—they are going to change their policy, and I am going to have some followup questions on how they intend to implement that going forward in the next panel. But what I wanted to ask you about was a couple of things.

First of all, you referenced a $50 fee. Who did you have to pay the $50 to?

Mr. KASPER. Well, the check was to the U.S. Treasury, but it was IRS Form 4506, and I mailed it to Missouri or somewhere, or Kansas City, and paid $50. It was an IRS fee to get that photocopy.

Senator AYOTTE. So you had to pay the $50 to get what you were able to get about your return?

Mr. KASPER. To get a photocopy of the return which showed the account number, I had to pay the $50.

Senator AYOTTE. And then, also, how were you originally notified that you were a victim of identity theft?

Mr. KASPER. On February 6, I got the e-mail notice that my attempt to file was rejected. So I got the rejection notice, and there was a code in there and an explanation that it was a duplicate tax identifier, which just a little time on Google I figured out that is identity theft, so I need to call the identity theft hotline.

Senator AYOTTE. And when you called, how many different people did you deal with?

Mr. KASPER. At least four or five. It was about 1 or 2 hours on hold each time that I called.

Senator AYOTTE. So four or five different people and each time 1 or 2 hours on hold?

Mr. KASPER. That is correct.

Senator AYOTTE. And so did you have to retell your story each time to each new individual?

Mr. KASPER. I believe so. I mean, like I said, they were very sympathetic, but they really could not do much for me.

Senator AYOTTE. You really used your own thought process and investigating your own case. I mean, you did a really good job investigating your own case.

Mr. KASPER. So far. It was really bothering me not knowing who had gotten this information.

Senator AYOTTE. Right. But the IRS would not give any information about what they were actually doing to pursue the case?

Mr. KASPER. Correct, other than that it seemed very unlikely they were investigating it.

Senator AYOTTE. Did they tell you even that they had reported it to law enforcement?

Mr. KASPER. No. They never told me they had reported it to law enforcement or even to the bank. When I contacted the bank, the bank specifically said 6 weeks later, “The IRS never contacted us about this deposit.”

Senator AYOTTE. And, obviously, then they said that they did not give you any followup of whether there was any kind of investigation conducted or any outcome of it?

Mr. KASPER. No, I got a letter saying they had received my fraud affidavit, which was the one I got the same day the police were interviewing the person. And then at the end, after the bank had reported it to the IRS and then the case was resolved, the day after I got the check, I got a letter saying, “Your identity theft case has been confirmed,” the day after I got the check.

Senator AYOTTE. After you got the check?

Mr. KASPER. Yes.

Senator AYOTTE. And one of the things that, as I listen to what you have to say, this is something I have been hearing time and time again, and obviously I think why we are having this hearing and how important it is that we get to the bottom of not only preventing these types of thefts, but also a better response to them from the IRS. And what I wanted to followup with, Dr. Fu and Mr. Greene, is on the issue of—you mentioned, Dr. Fu, one potential third-party fraud prevention tool based on voice analysis, as I understand it. What other fraud prevention tools exist in the private sector could the IRS harness potentially to help us address this? And was this something you think that we should be pursuing as we talk to the IRS about this issue? Because it seems to me that there is already a lot being done in the private sector that could be transported to the government sector as we look at this growing challenge.

Dr. FU. Well, I think one of the challenges for the Federal Government is that—especially the IRS, you cannot deny any particular customer, so you have a very diverse customer base compared perhaps to the typical private sector enterprises. Now, there are a number of fraud detection systems out there, but it would be difficult to legislate technological solutions. But I think it would be worth at least conducting studies to understand if some of these approaches might work at all, a pilot program, for instance.

NIST in particular has quite a bit of expertise in carrying out pilot programs and making strategic recommendations on authentication in particular.

Senator AYOTTE. Do you have any thoughts on that?

Mr. GREENE. The IRS Commissioner, this morning when he spoke, recognized that prior security measures become obsolete pretty quickly, and it is the proverbial race. You are constantly needing to improve, going beyond. KBA may have worked well in the past. Going beyond that in the future to step it up, there are ways. You can add the other factors. You can add the type of data analytics that Mr. Kasper talked about. Putting some of that in place can help you detect it a little sooner. Looking for patterns with certain e-mails, if they are very similar—if an e-mail has a string of letters or numbers and you keep seeing incremental increases and you see a pattern like that, those are the types of tools that you can put in place monitoring on the back end.

Senator AYOTTE. I thank you all. We are at the tail end of a vote here, so I am going to adjourn this, and I believe Chairman Johnson will be back. But we will be right back in the Committee, and we will take a recess, not adjournment. Sorry. Thank you.

[Recess.]

Chairman JOHNSON [Presiding.] We would like to call the hearing back to order.

What we would like to do is just give the witnesses an opportunity, if there is something that you have not been asked, if there is another comment or another piece of information you would like to provide in testimony, why don't you do that right now? Then we will dismiss you and seat the next panel.

So we will start with you, Mr. Kasper.

Mr. KASPER. I just wanted to mention that I have been watching a lot of the hearings on the subject, and John Valentine from the State of Utah had testified previously that he had talked to someone at the IRS who told him they were seeing a pattern of previous years' tax information being used to submit fraudulent returns as early as last year, which, coincidentally, is the same time the Get Transcript function was introduced.

Chairman JOHNSON. Who is Mr. Valentine?

Mr. KASPER. I do not remember the name of the agency, but it is the agency that handles the State taxes for Utah. He had testified in the Senate Finance Committee about that issue and about their lack of getting information from the IRS at that time.

Chairman JOHNSON. OK.

Mr. KASPER. Because they noticed a bunch of these suspicious returns this year and reported them to the IRS that they had this pattern. Data from last year was being used this year, and they reported that to them early in February of this year that that was going on.

Chairman JOHNSON. OK. Well, thank you, Mr. Kasper. Dr. Fu.

Dr. FU. Yes, well, I would like to just comment that with regards to the sample four questions to authenticate with this instant KBA, I think it would be rather relatively easy to actually write a program to rule all this out, and perhaps that is actually what was done to accomplish this particular breach. And in computer security, we often refer to these technologies as sort of "security theater" where they can give a sort of happy, squishy feeling for the consumer because you are doing some action to make you feel good, but it is always hard to know whether it is actually improving your security. And, in particular, with instant KBA there is very little understanding right now about how to measure the quality of the security of KBA, and I think we need improvements in that space if we are going to continue to use it.

Chairman JOHNSON. Let me quickly ask you, because I actually had a conversation with another Senator on the walk down, in terms of what happened here, would there be computer programs that are programmed to utilize all this personal information and do this quickly? Or is this going to be a very manual process in terms of logging on to Get Transcript and logging in the information? Do you understand the question?

Dr. FU. Are you asking me——

Chairman JOHNSON. Can this be——

Dr. FU. The attacker, how automated it is?

Chairman JOHNSON. Yes.

Dr. FU. I believe this can be fairly automated. In fact, when I used to work in the industry, we would write scripts to automate filling out web forms. So this is something you would almost be taught as an undergraduate. So I would expect a sophisticated adversary to be able to do it quite well.

Chairman JOHNSON. And then because the IRS was having that second layer—I forget exactly what you called it, but they were asking the hacker to enter——

Dr. FU. An e-mail address.

Chairman JOHNSON. An e-mail address, and then that was reauthenticated. Would they had to have separate e-mail addresses? Would they had to have 200,000?

Dr. FU. I do not know the answer to that. My guess would be that—you would have to talk to the IRS, but I would imagine they would be very easily able to audit if somebody reuses an e-mail address. But as we know, it is fairly easy to create a new e-mail address, and I have to say so many of them are just gmail.com that the domain is not always going to be too telling.

Chairman JOHNSON. OK. So they would not necessarily have to be real e-mail accounts—or they would have to be real e-mail accounts, so you would just be setting these things up by literally hundreds of thousands if not millions to do this.

Dr. FU. Correct.

Chairman JOHNSON. OK. Mr. Greene.

Mr. GREENE. Senator, your question about automating, I asked that precise question of some of our experts who spend their days analyzing attacks and malware. They did not have any specific knowledge of this attack, but their response was this would be very easy to automate soup to nuts.

Now, it still is a complex logistical effort. There was a big effort involved, but the tack of writing the scripts was not—they expect it was automated and do not believe that it was not the most highly sophisticated scripting. I guess what I would add is this is not the first successful compromise of KBA, but it has certainly received the most publicity, and most people do not get into crime to work hard. Copycats are pretty common. So I think we are likely to see more KBA attacks both on the private sector entities that use it and the government. Now is the time, I think, to look at your organization, if you are using it, to make sure that you have some type of second factor or are dialing up the sensitivity of your monitors, of your sensing, to look for anomalous activity, because I suspect that there are criminals out there right now looking at this successful attack and saying, “How can I duplicate that somewhere else?” They are going to reuse what they can.

Chairman JOHNSON. This really does answer the question why are these cyber attackers accessing this PII from all these different companies, accumulating it. This is the reason why, so they can utilize it this way. Correct?

Mr. GREENE. Well, and the information itself has value. This is an interesting attack, and this is different in kind than a lot of the major breaches we have seen in the sense that—I view this as not a breach, but 100,000 individual compromises. There are major breaches that have led to the release of millions of identities. These attackers stole money. In a lot of the breaches, they are stealing identity information to sell it. But at the same time they stole the money, they also acquired a lot of information. Mr. Kasper’s tax records, his tax transcript has information that has—it is akin to breaking—if I broke into your house to steal $1,000 and I saw a valuable ring, I am going to grab the ring, too, and then try to sell that. So they stole the money, but they now have more data that they will sell to others to use. There are very active black markets trading in this information.

Chairman JOHNSON. And, again, what is the use for that personal information then?

Mr. GREENE. It can be anything from future tax fraud to trying to open credit cards. Health care records are now very valuable. We have seen the value of them jump up dramatically. Some health care records we have seen are worth 2 to 10 times as much as a credit card nowadays.

I joke that if, I carry a Fitbit that transmits my data of my steps. That is not the Fitbit specifically, but there is a lot of data being transmitted that is not particularly secure. But if there is a way to monetize it, there is a criminal out there trying to figure out how to do it.

Chairman JOHNSON. And, again, once you automate an attack like this or a breach like this, you have already got the automated program; you have the software. It is very easy to replicate it or modify it for a new type of criminal scheme. Correct?

Mr. GREENE. Correct, to modify it, and most of the data that was used for these 100,000 compromises was probably previously stolen or just sucked off of a public website. It is a combination. We are all putting information out there that we do not even know about. Dr. Fu said our friends post stuff.

Chairman JOHNSON. So, again, with the software program, one individual could have pulled this thing off.

Mr. GREENE. I think it would probably be a more sophisticated, more organized effort than that, from soup to nuts, to go through it. It might have been only one——

Chairman JOHNSON. How many people?

Mr. GREENE. I would be happy to get back to you. I can check with some of our experts to see what they would say.

Chairman JOHNSON. OK. Again, I am just trying to get, the scope of this, the ease, how to replicate this. Is this a harbinger of things to come? Is it just the tip of the iceberg? Again, we have a billion people who have had their PII stolen, and this is what it is being used for, among many other things.

Mr. GREENE. The experts in our response team thought that this is most likely, again, from reading the outside reports, a criminal organization. So this is—and they have business plans. They have organizations set up to do all this, and they are looking, I am sure, at their next target.

Chairman JOHNSON. OK. Again, I want to thank all three of you for your thoughtful testimony, your thoughtful answers to our questions, and we appreciate it. This will be very helpful in terms of us building the record of exactly why this Congress really needs to pass a bill that at least takes the first steps in providing, for example, the information sharing or the threat signatures, these types of attacks, so that when other people experience something similar, we can maybe prevent some of these things.

So, again, thank you for your testimony, and have a good day. And we will call the next panel.

[Pause.]

This is perfect. Welcome back.

Senator CARPER. Thank you.

Chairman JOHNSON. I will have to be leaving here pretty quickly myself.

Again, I would like to thank the Commissioner and Mr. Millholland for coming to testify. It is the tradition of this Committee to swear our witnesses in, so if you would rise. I should be able to have this thing memorized. That is OK. There we go.

Do you swear the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. KOSKINEN. Yes.

Mr. MILLHOLLAND. I do.

Chairman JOHNSON. Thank you. Please be seated. I really do have that memorized, but I like to get it accurate.

Our first witness will be John Koskinen. Mr. Koskinen is the 48th Commissioner of the Internal Revenue Service, a position he has held since his confirmation in December 2013. Previously, Commissioner Koskinen served as the non-executive chairman of Freddie Mac from 2008 to 2012. Mr. Commissioner.

TESTIMONY OF HON. JOHN A. KOSKINEN,[1] COMMISSIONER, INTERNAL REVENUE SERVICE, U.S. DEPARTMENT OF THE TREASURY; ACCOMPANIED BY TERENCE V. MILLHOLLAND, CHIEF TECHNOLOGY OFFICER, INTERNAL REVENUE SERVICE, U.S. DEPARTMENT OF THE TREASURY

Mr. KOSKINEN. Chairman Johnson, Ranking Member Carper, and Members of the Committee, thank you for the opportunity to appear before you today to provide information on the recent unauthorized attempts to obtain taxpayer data through the IRS's "Get Transcript" online application.

Securing our systems and protecting taxpayers' information is a top priority of the IRS. Even with our constrained resources as a result of repeatedly decreased funding over the past few years, we continue to devote significant time and attention to the challenge. At the same time, it is clear that criminals have been able to gather increasing amounts of personal data as the result of data breaches at sources outside the IRS, which makes protecting taxpayers increasingly challenging and difficult.

The unauthorized attempts to access information using the Get Transcript application were made on approximately 200,000 taxpayer accounts from questionable e-mail domains, and the attempts were complex and sophisticated in nature. These attempts were made using taxpayers' personal information already obtained from sources outside the IRS.

It should be noted that the third parties who made these unauthorized attempts to obtain tax account information did not attempt to gain access to the main IRS computer system that handles tax filing submissions. The main IRS computer system remains secure, as do other online IRS applications such as, "Where's My Refund?"

To access Get Transcript, taxpayers must go through a multistep authentication process to prove their identity. They must first submit personal information, such as their Social Security number, date of birth, tax filing status, and home address. The taxpayer then receives an e-mail from the Get Transcript system containing a confirmation code that they enter to access the application and request a transcript.

Before the request is processed, the taxpayer must respond to several out-of-wallet questions designed to elicit information that only the taxpayer would normally know, such as the amount of their monthly mortgage or car payment.

[1] The prepared statement of Mr. Koskinen appears in the Appendix on page 79.

During the middle of May, our cybersecurity team noticed unusual activity on the Get Transcript application. At the time our team thought this might be a “denial of service attack,” where hackers try to disrupt a website’s normal functioning. They ultimately uncovered questionable attempts to access the Get Transcript application.

Of the approximately 100,000 successful attempts to access the application, only 13,000 possibly fraudulent returns were filed for tax year 2014 for which the IRS issued refunds totaling about $39 million. We are still determining how many of these returns were filed by the actual taxpayers and which were filed using stolen identities.

For now, our biggest concern is for the affected taxpayers to make sure they are protected against fraud in the future. We have marked the accounts of the 200,000 taxpayers whose accounts were attacked by outsiders to prevent someone else from filing a tax return in their names, both now and in 2016. Letters have already gone out to the approximately 100,000 taxpayers whose tax information was successfully obtained by unauthorized third parties. We are offering credit monitoring at our expense to this group of taxpayers. We are also giving them the opportunity to obtain an identity protection personal identification number (IP PIN) as it is known. This will further safeguard their IRS accounts.

We are also in the process of writing to the 100,000 taxpayers whose accounts were not accessed to let them know that third parties appear to have gained access from outside the IRS to personal information such as their Social Security numbers. We want these taxpayers as well to be able to take steps to safeguard that data. The Get Transcript application has been taken down while we review options to make it more secure without rendering it inaccessible to legitimate taxpayers.

The problem of criminals using stolen personal information to impersonate taxpayers is not a new one. The problem of tax refund fraud exploded from 2010 to 2012. Since then we have been making steady progress both in terms of protecting against fraudulent refund claims and prosecuting those who engage in this crime. Over the past few years, almost 2,000 individuals were convicted in connection with refund fraud connected with identity theft.

Additionally, as our processing filters have improved, we have also been able to stop more suspicious returns at the door. This past filing season our fraud filters stopped almost 3 million suspicious returns before processing, an increase of over 700,000 from the year before. But the criminals continue to become more sophisticated and creative. For that reason, we recently held a sit-down meeting with the leaders of the tax software and payroll industries and State tax administrators. We all agreed to build on our cooperative efforts of the past and find new ways to leverage this public-private partnership to help battle identity theft. We expect to announce more details shortly.

Congress plays an important role as well and can help by approving the President’s fiscal year 2016 budget request, which provides for $101 million specifically devoted to identity theft and refund fraud. A key legislative request, among others in the budget, is a proposal to accelerate information return filing dates generally to

January 31. This would assist the IRS in identifying fraudulent returns and reduce refund fraud related to identity theft.

Ranking Member Carper, Members of the Committee, this concludes my statement, and I would be happy to take your questions.

Senator CARPER [Presiding.] Mr. Commissioner, I do not want you to assume that because all of my colleagues have left that we are not interested in what you and Mr. Millholland have to say. We are very much interested. We have a series of five or six votes in a row, and we are voting about every 10 minutes, and we are trying to keep this moving. This bipartisan cooperation, this is what happens when you can collaborate. We will see if we can keep it going, but thank you for bearing with us, and hopefully we will be able to sit back down and ask some questions when we are all together.

All right. Mr. Millholland, nice to see you. Thanks for joining us. I have not seen Commissioner Koskinen since this morning. He testified before the Finance Committee.

Mr. KOSKINEN. I am fondly referring to this as a "double header."

Senator CARPER. There you go. Day-night. What did Ernie Banks used to say? Remember Ernie Banks, great shortstop for the Chicago Cubs, on weekends when they played Sunday double headers, he would say to his teammates before the game would start, he would say, "Let us play two."

Mr. KOSKINEN. That is exactly where I picked it up.

Senator CARPER. Go ahead.

Mr. MILLHOLLAND. Sir, I do not have an opening statement.

Senator CARPER. All right. Mr. Commissioner—are you here to correct his answers? Is that what your role is? OK. He is actually pretty good, so you may not have much to do.

As we have discussed a time or two before, Congress has not given the IRS the funding that you need to fulfill your missions, have not done it for a while, and I think that is unfortunate because every additional dollar spent by the IRS, as we know, to ensure tax accuracy and improve program integrity brings in at least $6, and I have heard even greater amounts than that. We had some conversation today about what investments in compensation, ways to attract and retain some of the senior-level, most difficult to hire and find skill sets in cybersecurity, how those investments pay way more than $6 for every dollar we invest.

But what has been the practical impact of the budget cuts on your operations, such as staffing levels, investments in technology, and your ability to engage in program oversight and integrity activities, please?

Mr. KOSKINEN. Well, I would stress that the particular challenge we are faced with the Get Transcript application was not a result of a budget issue.

Senator CARPER. I understand.

Mr. KOSKINEN. It is an authentication question that we need to continue to deal with. Authentication is a challenge for us across the entire spectrum.

The budget challenge is that this is really a shot across the bow. As noted, this attack was sophisticated, complicated, run by apparently organized crime syndicates who operate here and around the world. And the challenge for us is not just the authentication for this application, which has now been taken down and which we will improve. The challenge is the continual attempts and attacks the agency is under with regard to its basic database. As noted, our basic filing system was not affected by this attack, and it is secure. But we run an antiquated system, and over the last several years, the underfunding of the information technology (IT) investment has meant that we have been able to replace a lot of antiquated systems less quickly, less rapidly as we would like. It leaves us more vulnerable. We are running some applications that have been running for 50 years. We are running other applications that are no longer supported by the software developers and manufacturers.

So we have a difficult challenge competing with organized criminals who have resources and have turned this into a business. They have collected almost unbelievable amounts of personal information from people here and around the world in massive databases, and they have one commitment, which is to attack not just the IRS but attack across the board other financial institutions and individuals.

I referred to a website yesterday that has indications, reports of 25 data breaches and identity theft activities that took place in May. We are one of the 25. There are 24 others that took place around the world. So it gives you an idea of the magnitude of the challenge we are facing. It continues to be one of our highest priorities to make sure we do everything we can to protect taxpayers, but that means we are going to have to continue to invest in the system and in the people who run those systems to make sure they are as secure as possible.

Senator CARPER. OK. Thank you. You spoke to us earlier before the Finance Committee today about the streamlined critical pay program. You may have alluded to that in your comments here before this Committee. But could you talk a little bit about why that program is worthwhile and why investing in it can pay way more dividends in terms of reducing the impact on the Treasury, adverse impact on the Treasury?

Mr. KOSKINEN. When the restructuring act for the IRS was passed in 1998, the agency was given the ability to hire up to 40 executives with streamlined critical pay.

Senator CARPER. Tell us what that means. I think I know.

Mr. KOSKINEN. Streamlined critical pay means much as if you were in the private sector, you can find someone, as we did with the head of our Information Technology, Mr. Millholland, you can find them in the private sector, you can recruit them, select them, offer them a job. They can take it immediately and begin to work immediately. That is the streamlined part.

The critical pay part allows you to pay, if necessary, above the Senior Executive Service (SES) level, although a number of people that participated in that program did not get additional pay, but that is the critical pay aspect of it. It has been used primarily for information technology and other critical technological and intellectual capacity. The Inspector General issued a report last December in which he noted the program had been run appropriately over the period of time.

Mr. Millholland was telling me recently that we had two senior IT executives we wanted to hire, who were willing to come work for us, but were not willing to participate and wait for the several months it takes to be approved for government employment as a career employee, and also were not satisfied with the maximum compensation we could offer absent the critical pay aspect.

So presently we have people across the IT spectrum who are on critical pay. We have lost almost half of the people on critical pay when I began a year and a half ago because their term ran out. The three critical data, compliance data analytics people, including our expert in authentication, left the agency at the end of last year because his term ran out. We have not been able to replace him appropriately.

We hope that we will be able to get the authorization to resume the program which would allow us to recruit the kinds of people, a handful of them, that we need at the top of IT, that we need at the top of international tax administration.

Senator CARPER. Good. Thank you. I said this morning, Mr. Millholland—I do not know if you were in the audience when the Commissioner spoke before the Finance Committee, but I said in my life sometimes people ask me why I have had some success, modest as it is. And I always say because I picked the right parents, and the other thing is because I have always surrounded myself with people smarter than me. And if you look at some of the people that we are trying to attract and retain at IRS to help us deal with these cyber issues, they could make a whole lot more money in the private sector, as you know, and are, but the reason why they are serving where they are is because they are doing something for their country, and they feel a need to do that.

Mr. Millholland, just very briefly, there was some discussion earlier, I think in the first panel, about two-factor methods, and I think with respect to using stronger authentication technologies, and they talked about, for example, two-factor methods like sending a letter with a password or calling an individual's phone with a password. Facebook, Google, and Bank of America are just a few of the major names.

How are you moving forward in using the so-called two-factor authentication technology? And when will you have it fully implemented, please? Just very briefly. Thank you.

Mr. MILLHOLLAND. Sure. I want to distinguish between inside use and use of somebody connecting to the website. Inside use, we already use two-factor authentication, with variations of those, including personal identity verification (PIV) cards, for example—that is, the Homeland Security Presidential Directive 12 (HSPD–12) cards. And there are a number of ways to implement two-factor authentication.

For the external, we fundamentally have to decide are we going to set up accounts for taxpayers so that they can file directly. If we were to do that, and discussions have started with the Commissioner and others about should the IRS deal directly with taxpayers in the filing of their returns, we would want to set up accounts like you would have with a financial institution. If we were to do that, we would go with multifactor authentication; that is, certainly an ID, a verification that the person is who they say they are, with far more confidence than what we did with this particular Get Transcript application, perhaps use of biometrics, perhaps use of something like Connect.gov, something else that gives us that additional proof that the person is who they say they are.

Senator CARPER. OK. Thanks so much. My time has expired. Senator Ayotte.

Senator AYOTTE. Thank you so much.

Senator CARPER. Thank you.

Senator AYOTTE. I want to thank both of you for being here. Commissioner Koskinen, let me just thank you up front for your response to my letter of May 28, and I think this is really important that you are going to change the policy that you have in terms of providing tax returns to those who find themselves to be victims of identity theft. And what prompted me to write you that letter is I am sure many of my colleagues could share similar stories, but one was a woman, the Weeks family, and they learned last year, when they went to file their tax return, a month after their 7-year-old daughter had been killed in a car crash that, in fact, someone had claimed their deceased child as a dependent. In fact, what the IRS told Mrs. Weeks was that their deceased child's Social Security number had been used three times, and then she had a really hard time getting any more information. She could not get any information from the IRS, and, similarly, in terms of who used it, what happened, even getting copies of the returns and trying to understand what happened.

Another family I had, after having surgery and complications that prevented one of the members of the family from returning to work for 3 months, she filed their tax returns, this family did as soon as they could, and they really needed the return because they were in jeopardy of losing their home. And what they found out when they filed their return, the wife discovered that someone had already filed a tax return with using her Social Security number, and she was told that it would take her 4 to 6 months to process any kind of refund because of this identity theft. And they became delinquent on their home and faced foreclosure, and this was one where my staff was able to intervene and help them in time to save their home.

And I wanted to use these real stories because your response to me is very important. What we heard earlier today from Mr. Michael Kasper—and perhaps you had a chance to hear what he had to say as a victim of identity theft—who testified before this Committee is that the process of not being able to get a return or information, it makes these victims—obviously puts them in a worse position, because Mr. Kasper went through a long process, finally had to pay $50 and got information that allowed him to go to the bank and to try to protect himself and actually resulted in finding out who did this.

So what I wanted to understand is with this new procedure, how long do you think it will take to put this in place? And will all victims of tax-related identity fraud be able to request copies of their fraudulent returns? And can you give me a sense—I have constituents coming to my office. Do you have a sense of how big this problem would be in New Hampshire and across the country? And those are some of the first questions I have.

Mr. KOSKINEN. First of all, I appreciated your letter, and I was delighted that we were able to review the situation and remedy it.

We hope to in a very short period of time have the new process up where we can redact any information that might look like it would be a violation of the so-called 6103 and give taxpayers access to the false return so they can get an idea of exactly what it looked like and what they have to deal with, and we should be able, as I say, to have that system up and running within a matter of no more than 3 weeks, to be able to do that.

As I have said in other contexts, the access to Get Transcript is really just another form manifestation of identity theft. These are criminals who already knew and had enough information to file a false return. What they were trying to do was get more information so they could file a better false return. As noted, the reason we have stopped 3 million returns, suspicious returns at the door is because we keep improving the sophistication of our filters which detect anomalies. So if you can eliminate the anomalies, you are better off.

But we continue to try to do whatever we can to help taxpayers. For instance, as I said, the notification to the 104,000 who had data access, those letters are out. They should have those already in the next few days. But we need to, as quickly as we can, provide support to taxpayers. When the problem exploded 4 or 5 years ago, it would take us up to a year to be able to straighten out a taxpayer's account. We now have it down to an average of 120 days. Our goal really is to get it even shorter than that as we go.

It is a problem. We have IP PINs in the hands of about a million and a half taxpayers who have had fraudulent, false returns filed. They are spread across the country, and, again, it is an ongoing challenge for us. One of the issues we need to continue to do as much as we can is develop filters at the back end to stop returns, but increasingly do authentication of the front end, and that is why we have this partnership with the private sector and the States. When I pulled them together 3 months ago, H&R Block into it and others, I said, "The purpose of this meeting is not for me to tell you what to do. The purpose of this meeting is start a discussion where we can work together, the private sector, the States, and the IRS, to figure out how jointly we can do a better job of protecting taxpayers." Because as you know with your cases, there is nothing more traumatic to an individual than to feel that their data has been violated, has been stolen. And it is not only the difficulty of getting a refund—70 percent of people who file with us get refunds—that you may need immediately, but it is that lack of certainty of where else is this information available.

Senator AYOTTE. Right, and that is why I think it is important that the taxpayer be given as much information as possible to protect their own financial interests. And one of the things we heard from Mr. Kasper, who was here, but it is also a similar experience that I have heard a lot about—in fact, Nina Olson, the Taxpayer Advocate, noted in her annual report that victims often must "navigate a labyrinth of IRS operations" and recount their experience time and time again to different employees. And so Mr. Kasper's experience was four to five different people, waiting an hour or two on the phone for each. Has thought been given to assigning one person when someone becomes an identity theft victim to that individual rather than, calling back up again and being put back sort of in——

Mr. KOSKINEN. It is a problem that we have been focused on. When we started, ID theft was spread around various parts of the agency. We have now consolidated all ID theft issues, particularly for taxpayers, into one location so that they will actually be able to go one place and tell their story once. The Taxpayer Advocate, whom I work with closely and I have great admiration for, and I have a disagreement about whether there should be a single individual, because the problem with a single individual as opposed to a single entity is that if you call, they could be on vacation, they could be at lunch, they could be somewhere else. Most call centers, if you call any commercial enterprise and then call back, you do not get a name to talk to. What you do get when you call back is they know what your call is about. They have a record of what you said. And that is the system that we are building. So that a taxpayer can call a special number for ID theft. They do not have to battle through the lack of service we are able to provide generally. And when they call the second time, if they have to, they will not have to repeat the story. The record of what their situation is will be readily available to the next available operator for them. And I think our experience is and the private sector experience is that is a more efficient way to provide the service to taxpayers rather than for them to have to depend upon the location of a given individual.

But the point that the Taxpayer Advocate raised initially was extremely right, that we cannot have taxpayers have to themselves navigate the various aspects of the IRS operations, and we are working to, in fact, as I say, consolidate that to give taxpayers one-stop shopping, as it were.

Senator AYOTTE. Thank you. I know my time has expired, and I will stick around for another round when we get through our votes. But thank you.

Chairman JOHNSON [Presiding.] Thank you, Senator Ayotte.

Mr. Commissioner, we had Mr. Michael Kasper, and in his closing comments, he talked about a gentleman named John Valentine—I believe he must be working for the Utah Department of Revenue—that apparently contacted the IRS in February of this year, talking about seeing returns with prior years' information, very close, basically looked like fraudulent returns. Were you aware of that? Or were you, Mr. Millholland?

Mr. KOSKINEN. We were aware, obviously, of the difficulties with filings that basically took place in a number of States, including Utah and Wisconsin and others, in January, had a symptom identified with them, and that is that they had access to the prior year's returns, and those returns primarily were filed only at the State not at the Federal level. But it was out of that concern that I pulled together what is called the "Security Summit" in March to pull everybody together to say, OK, what is going on and, most importantly, what can we do together that we cannot do separately.

So we were aware of that situation, and we have been working with the States and with the private sector since then.

Chairman JOHNSON. You were aware of Mr. Kasper's situation then? I guess Krebs on Security had a blog posting on March 30.

Mr. KOSKINEN. Yes.

Chairman JOHNSON. You were aware of that personally as well as the IRS was.

Mr. KOSKINEN. Yes, we were. And, in fact, as we have been tracking back through everything, I am not allowed to talk about particular taxpayers, but as a general matter, let me just say that we took all of that information into consideration and were in the process in April of beginning to take a look at adjustments, made some adjustments already during the filing season to issues around Get Transcript, and, in fact, were developing and are developing with the States a protocol that will, in fact, improve the security significantly as we go forward. But we will not put the site back up until we are confident with its security.

Chairman JOHNSON. But you were aware at the end of March, but you decided not to make any changes at that point in time.

Mr. KOSKINEN. I know we made some changes, which I would be happy to talk to you about more privately, but we did not change the fundamental security aspect of Get Transcript. Our plan was to take a look at that and roll it out toward the middle or the end of June.

Chairman JOHNSON. You were made aware of the actual breach of a couple hundred thousand—well, 100,000, but an attempt on 200,000 different accounts on about May 18th. Is that correct?

Mr. KOSKINEN. Yes, it would have been about May 18, and it was mid-May when we thought it was a denial of service, and then on Thursday—someplace around here I know where that date is. I can tell you for sure.

Chairman JOHNSON. OK. But then about 2 weeks later, you decided to shut down——

Mr. KOSKINEN. Actually, we knew there was a denial of service attack on May 14th—or we suspected that. We then knew and I was advised by Thursday, May 21, that, in fact, there had been—less than a week ago, 10 days ago, I was advised that there had been a breach. We continued to investigate that. We had already notified Homeland Security and other security people, as well as the Inspector General. And then the following Tuesday, it was the Memorial Day weekend, as we got more details and knew what we were dealing with, we made an announcement to the public and started mailing out letters.

Chairman JOHNSON. OK. And you shut down the site then with how many——

Mr. KOSKINEN. We shut down the site probably on Tuesday or Wednesday——

Mr. MILLHOLLAND. It was Thursday morning.

Mr. KOSKINEN. I guess the Thursday morning before the meeting with me they had shut down the site.

Chairman JOHNSON. So within a week or so, something like that. OK.

Mr. KOSKINEN. From the time there was an indication of a problem until the time—which was originally thought to be a security problem, until the site was taken down was a week.

Chairman JOHNSON. OK. Mr. Kasper was talking about his frustration that he had contacted the IRS and could not get any information on this, that it would take about 6 months. And there are always privacy concerns. That was the reason why the IRS could not give him more information. Can you talk about, why would it take 6 months? What are those privacy laws you are dealing with that you could not communicate with the taxpayer whose identity had been stolen through an IRS system? Why the time lag? What are those privacy laws that prevent the IRS from——

Mr. KOSKINEN. Privacy laws that we are concerned about—and as Senator Ayotte raised issues with us, Section 6103 says we cannot reveal to anyone any taxpayer information. We cannot share it even with other government agencies unless there is a statutory exception that allows us to do that.

So the challenge we had when taxpayer information—fraudulent returns were filed, first you have to determine who is the fraudster and who is the legitimate taxpayer. Second, there was a concern that if we issued a copy even of a fraudulent return, it could have other taxpayer information that had been stolen in that return, and technically it is a criminal violation for us to reveal that.

I do not know why it took anybody 6 months. It should never take you 6 months to get through the system. But basically what we have set up is a situation where we can simply redact any third-party information in a return and give the taxpayer a copy of the fraudulent return so they will know exactly what was in there.

Chairman JOHNSON. And how long a time do you think that process should take then?

Mr. KOSKINEN. That process, we have a special hotline for identity theft, and if you get a notice that you have been returned, there is no reason you should not be able to get a copy of that return promptly.

Chairman JOHNSON. Promptly means?

Mr. KOSKINEN. Promptly within—if you call us, I do not know why you could not have that return within a week.

Chairman JOHNSON. OK. In Wisconsin the Guenterbergs had their identities stolen quite a few years ago. Again, the IRS could not—even though they knew they were fraudulent returns, they understood there was identity theft, they were prevented, again, under apparently the same privacy statute, from contacting the Guenterbergs, and as a result, they continued to have their identity being stolen and victims of that.

I have introduced a piece of legislation. It is called "The Social Security Identity Defense Act of 2015," to allow you to provide that information of identity theft. Is that a piece of legislation you will support?

Mr. KOSKINEN. We would be delighted to be able to. Our biggest problem, for instance, with law enforcement is when there has been identity theft, we cannot give the law enforcement authorities that information without the approval of the taxpayer involved. So to the extent that for law enforcement purposes, for protection against identity theft, we are allowed to provide information to either law enforcement authorities or others who need to know to prevent further identity theft, that would be helpful.

Chairman JOHNSON. Mr. Millholland, I am actually surprised that having noticed, found out about this breach on May 18, you already know that there have been 13,000 fraudulent returns filed from those same breached accounts and $39 million of tax refunds have been sent to those criminals. How did the IRS get that information so quickly?

Mr. MILLHOLLAND. Part of our analysis was to go in and look at every one of these attempts and see what they were doing and such. And, thus, the mapping process, the data analysis process of taking each one of these e-mails, tracking down what domains those e-mails were going to, determining how many Social Security numbers had different e-mail addresses, all that then were worked so we could block those particular Social Security numbers from getting any more information. But it also allowed us then to go dive into the IRS master file and associated systems to say, all right, how many of these people actually filed returns? How many of them did not file returns? The Commissioner provided some numbers on that. That has led us down to this approximate 13,000 that may or may not be fraudulent. We are not sure yet.

Chairman JOHNSON. As long as we are talking about those e-mails, so you have that two-step authentication that required the criminals to get another—a signal from or a text or an e-mail to that account. Did those have to be separate e-mail accounts?

Again, the 100,000 accounts that were successfully breached, that was a two-step process. Did those have to be separate e-mail accounts? Were they separate e-mail accounts?

Mr. MILLHOLLAND. They did not have to be. It was one of the design flaws.

Chairman JOHNSON. OK. So that is a design flaw.

Mr. MILLHOLLAND. Absolutely.

Chairman JOHNSON. OK.

Mr. KOSKINEN. But part of our problem is because we do not communicate with taxpayers yet electronically, so we never send e-mails back or forth because we have no security for them. If we could as part of our development and refinement of our systems be able to communicate electronically, it would accomplish a lot of goals, one of which would be the two-factor authentication then would be much more significant. Financial institutions and others, when you want to change your password, they send you a key to your e-mail address because they know it is your e-mail address.

Chairman JOHNSON. That is a relatively significant flaw and a pretty easy fix that, each e-mail, in terms of this authentication, has to be a unique e-mail. Correct?

Mr. MILLHOLLAND. That would be going forward, is absolutely correct.

Chairman JOHNSON. OK. So that is a corrective item that needs to be done almost immediately.

Mr. Millholland, knowing that this authentication process is being used by Healthcare.gov, the Social Security Administration, and other agencies in the Federal Government, have any of those agencies or departments been in contact with you to discuss what happened at the IRS? And are they considering shutting down their sites?

Mr. MILLHOLLAND. I cannot speak to whether they are shutting down or not, but we have had conversations, just most recently this last Friday, with the Social Security Administration on what do they do to authenticate. So that kind of conversation is going on there.

In addition, we have had, although it has been a bit of time, with the VA, again, how do they authenticate. So I will call it "best practices" amongst government is much better known.

Chairman JOHNSON. So Healthcare.gov, CMS, the U.S. Department of Health and Human Services (HHS) has not been in contact with you in terms of their authentication and their concern about similar type of breach of their system?

Mr. MILLHOLLAND. Not with me. Perhaps with other parts of the IRS, but not with me.

Chairman JOHNSON. OK. I would like to find out whether they have. I think that is pretty serious.

[Pause.]

I do know that, Mr. Commissioner, you did mention budget cuts as one of the potential problems, but this really had nothing to do with budget cuts. Correct?

Mr. KOSKINEN. In my testimony, as I have said, this issue was not a budget issue. I have tried to make that clear all along. I do not want anybody to think—while we have significant budget challenges, I do not want anybody to think that every problem we have is a budget problem. There are issues and challenges we have that are management questions. There are other issues. Our problem here for the budget is not fixing the authentication on this side. Our challenge for the budget is, in fact, upgrading and protecting our entire system, which is at this point secure, but under continual attack.

Chairman JOHNSON. Mr. Millholland, this knowledge-based authentication, you are using an outside vendor to provide you this type of information. Correct? That was from Healthcare.gov, but yours is very similar. Correct?

Mr. MILLHOLLAND. We use a third-party source for information beyond the type of questions that—if someone called, they are asked a series of questions. Then we go to these out-of-wallet questions to a credit scoring agency.

Chairman JOHNSON. Again, that taxpayer personally identifiable information, that is not held within the IRS anywhere. Correct? That is all held by an outside vendor?

Mr. MILLHOLLAND. That is correct.

Mr. KOSKINEN. That is correct.

Chairman JOHNSON. Is there any personal information that the IRS stores that is not obtained by the IRS directly from the taxpayer? Do you go to any outside vendor anywhere in the IRS and then store it within the IRS' system?

Mr. MILLHOLLAND. I do not believe so, but possibly Criminal Investigation (CI), maybe.

Mr. KOSKINEN. That is a good catch. As a general matter, we have no personal information from people that they have not provided us. The Criminal Investigation Division does in its investigations pursuing criminal cases accumulate data and information that they go after. If we do an audit of someone, an examination where we are actually examining their records, we may accumulate information about demonstrating whether they are following the tax laws. But even that is not in a database that the IRS is keeping on individuals. The only data we have in our major database is the information that comes from filing of taxes. And that is lot.

Chairman JOHNSON. Again, that is simply on a case-by-case basis, that information .

Mr. KOSKINEN. That is right. Both the investigations and the examination are just on case-by-case pursuit of particular issues.

Chairman JOHNSON. Is the IRS in any kind of analytics utilizing information from credit card companies, Mr. Millholland or Mr. Commissioner?

Mr. KOSKINEN. Yes. Under a statute provided by Congress, as individuals we all at the end of the year get a credit card summary of your expenses. We get on what is called the 1099–K, we get that information for all merchants. So for the first time in history, we have third-party information about what small and medium-sized, even larger businesses are doing as far as credit card receipts. So that comes in. Then we have to decide what to make of it because all it tells us is what the credit card receipts are.

Now, the really out of it small businesses are filing returns with less revenues than their credit card receipts, so those are sort of low-hanging fruit. But beyond that, we do not know what their expenses are. More importantly, we do not know what their cash receipts are. So that data needs to be analyzed. We need to try to figure out what do we know as a result of that data. How can we begin to model what an average business in a certain industry in a certain area ought to look like based on the data we are getting out of those credit cards? And we think the biggest part of the tax gap is an estimated $135 billion of underreporting by small and medium-sized, some large businesses, and this is the first time we have ever had third-party information. So there is a significant amount of data analytics around that information.

Chairman JOHNSON. Are you getting individual transaction information? Or are you just getting a summary of——

Mr. KOSKINEN. We are getting summary data. It is obviously voluminous. It is as a result of a year's transactions. We do not know what an individual bought, whether they bought, had their car washed or had it serviced or whatever else. What we are getting is, in fact, the receipts, this many credit cards, this many dollars in funding provided to that organization.

Chairman JOHNSON. So is this kind of akin to a 1099 then? You are using this—so you can trace the fact that if it is a small business who is obviously receiving revenue through credit cards, you are matching what that business has reported for income versus the——

Mr. KOSKINEN. The summary amount—exactly.

Chairman JOHNSON. So that is what this is being used for.

Mr. KOSKINEN. Yes, exactly.

Chairman JOHNSON. OK. Mr. Millholland, I see that you used to be chief technology officer at Visa International. Is there any government agency taking a look at individual transactions from the credit card companies that you are aware of?

Mr. MILLHOLLAND. Not that I am aware of, no.

Chairman JOHNSON. Because we do hear that the CFPB, is looking at individual transactions and trying to come up with, for some purpose.

Mr. MILLHOLLAND. Again, not to my knowledge, sir.

Chairman JOHNSON. OK. Senator Carper, do you have further questions? Thank you.

Senator CARPER. Mr. Millholland, do you feel up to one more? All right. We want to get our money's worth out of you today. Here is the chance to do it.

Again, thank you both for being here and for your hard work. We are lucky to have you serve our country. We are grateful.

It seems that there are some valuable lessons to be learned from this incident. We have talked about some of them this afternoon, and we certainly talked about them this morning before the Finance Committee with the Commissioner. But I would just ask you, Mr. Millholland, what are your plans for ensuring that breaches like this do not happen again or at least we reduce significantly the likelihood that they will happen again? And have you updated your security procedures in fraud prevention methods to account for this particular attack?

Mr. MILLHOLLAND. I call it a work in progress at the current point in time. As I say, the Commissioner pointed out the timeframes. It has only been a week since we shut the site down. We are completing our data analysis of what happened and when did it happen. Did the problem extend beyond this group of 200,000? So we can get basically all the facts and data in one place.

In addition, there are investigations outside of the IRS going on that we have to, let us just say, maintain the environment for.

But beyond that is then what could we have done differently? This particular application was designed the way that the phone system was designed; that is, we make a phone call. We designed it very much that same way in the sense of provide an easy way for the taxpayer to get a copy of their information. We extended it because it was electronic to these out-of-wallet questions as such. The debate inside was how many of those should we have. What degree of confidence would we have if, instead of asking 4 or 5, we asked 15 or 16? Each one of those questions that you ask can increase the confidence level that it really is the person who you think it is. I think if you ask 16, you are in the 99-percent range of confidence. But that is then a burden on the taxpayer and such. So the decision point inside is how easy do you make it versus the risk that you are wrong kind of thing.

The one aspect I would say that in hindsight I think we should have looked at a little bit better was the method of this particular attack. We sort of, as I say, built it the way the phone system was built, whereas if you want to get someone's tax return, you would call up and fake it and hopefully you would get through. An individual would do it. That is the mind-set we had with the electronic version. It would only be one person attempting to get it instead of what happened was, appears to be an organized criminal activity. That in hindsight one we had to—we should have thought better about. But, again, it is a hindsight question.

In addition, one could argue should we have put other authentication factors in like some other method that would provide the way we set up an e-mail account, for example, is to write a letter to the taxpayer instead to say, "This is your code for your e-mail address." That, of course, adds time and burden to people who want their transcripts very fast.

But it is those kind of debates that we had inside. A risk decision was made back in 2013 about the level of risk we were willing to take, and as I say, for a lot of people it has been very successful. I believe the Commissioner remarked it was some 23 million people who got their transcripts successfully. But then, again, we had this incident, and that is the dilemma.

Senator CARPER [Presiding.] All right. Thanks.

And the question I asked of the Commissioner this morning, he used the term "IP PIN," and I asked him just to drill down and explain to our Committee this morning what was the relevance of that and why was that important. Would you just tell us what you think? And we will compare answers. Go ahead, Mr. Millholland.

Mr. KOSKINEN. No pressure. [Laughter.]

Mr. MILLHOLLAND. The use of an IP PIN is an additional flag that we can provide to those who have demonstrated an ID theft issue. In that case, then, within the—I will just say the master file of the IRS, their account, their return, all the information about them has that flag on it to say this person had a theft and, therefore, needs to be treated differently. We would then look for returns that come in allegedly from that person that do not have that IP PIN with them.

This, of course, necessitates a lot more work from the point of view of, well, what do you do when the person loses the PIN? And then you have to have another validation procedure on top of the one you had to give them still another PIN. Thus, again, it complicates life, so to speak, but this is all part of the Digital Age where one has to think through all of those use cases. What will you do about it if something goes wrong? And then how do you provision it in a way that for the taxpayer is relatively easy but yet still maintains the security that you want to have around such a request?

Senator CARPER. OK. Good. Let me ask, Commissioner one last question, and it is kind of a wrap-up question for me, and you answered this this morning and this afternoon as well. I am going to ask you to do it again, and just tell us what can Congress, particularly this Committee, do to help prevent future breaches like the one we are talking about, both at the IRS but also at other organizations.

Repetition is good.

Mr. KOSKINEN. We need third-party information, particularly W–2s, earlier. We need to get them when the employees get them in January so we can match the taxpayer's return with third-party information.

We need legislation that allows us to mask or put hashtags, as they are called, on those W–2s and then limit the number of people who can prepare those by an appropriate competitive process, because criminals now are so creative, they are creating false corporations, false W–2s, and then filing false——

Senator CARPER. These guys are not stupid.

Mr. KOSKINEN. No. They have made enough money and have enough money that they are a multi-billion-dollar operation out there with an unbelievable amount of information on individuals across the world. So if we could get the W–2s earlier, if we could make sure the W–2s were accurate, if we could increase the penalties for identity theft and refund fraud——

Senator CARPER. By what magnitude? Any idea?

Mr. KOSKINEN. We have proposals in there to, not make it unreasonable, but make it unreasonable enough that it increases the penalties significantly. Those are in our proposals for this year for legislation that would be very helpful. And then ultimately, as we talked about earlier, reauthorizing streamlined critical pay. We always had it for 40. We never used it for more than 34. It would allow us to continue to recruit and retain directly the smartest, best people we can like Mr. Millholland.

Senator CARPER. So that you can continue to surround yourself, as I do, with people smarter than you?

Mr. KOSKINEN. Smarter than you are, yes.

Senator CARPER. There we go. All right. That is good. Senator Ayotte.

Senator AYOTTE. Thank you very much, Senator Carper.

I just wanted to followup, actually. I know that you were just discussing the IP PIN program, and I believe you also testified that over a million taxpayers already, as I understand it, are in this program. But I also, in looking at the TIGTA report, said that there is still a big gap in terms of at least for 2013 what we could see that when TIGTA had looked at it, there were still over a half million eligible taxpayers, looking at processing year 2013, that the IRS did not give the IP PIN to.

So can you help me understand, are you sort of overwhelmed at this point that everyone who wants one cannot have one? Or is there a reason for that?

Mr. KOSKINEN. No; there was a reason. At that point, those were returns a little like the 200,000 we have today—the 100,000 that did not have any access to their accounts, so they have not been victims of identity theft from the standpoint of the IRS. So we have indicators on a number of accounts where there is an indication that there may be an issue, and the IG raised in that report that we should for those—actually a total of about 1,700,000 people had some, sometimes minor, sometimes more significant, indications.

We have historically been careful about the IP PINs. As Mr. Millholland said earlier, when we issue them, if you lose it, then we have to go through validating you again, and it is a burden on the taxpayers. But we took the IG's recommendation to heart, as we often do, generally do with the IG recommendations, and this before this filing season we offered, besides mailing out a million and a half PINs to people who had them before and got them again, we offered the 1.7 million the opportunity to get a PIN.

We also have a pilot program that ran this year for the second year, in Florida, Georgia, and the District, which are the three major kind of hotbeds historically of ID theft, and offered taxpayers there, even if they did not have an indicator of tax identity theft, to apply for an IP PIN if they would like. And it is a pilot to see what the burden is on the taxpayers, what the burden is on the IRS, and how effective that can be.

Senator AYOTTE. Well, that was going to be my follow-up question. Is this something that we can offer opt-in for everyone?

Because I think there are definitely some of my constituents that would choose to opt in on this.

Mr. KOSKINEN. The reason we ran this pilot was to see how it would work if we offered people the PINs. One of the things we are looking at right now—if you get an IP PIN, the requirement is you have to get a new one every year, and you have to file forever with your IP PIN. One of the things we are looking at now as a result of evaluating the process is could we allow people after 3 or 4 years, if they wanted to, to drop their IP PIN and go back to their Social Security number if they feel that by this time it is all right?

The other thing is, can we give the IP PIN and have it last for more than a year? In other words, could we give it to you for 3 years so that we and the taxpayer do not have the burden of sending them back and forth? We started initially that way just to try to get control of them.

So as we get that refined, then we will take a look at is there a way we could offer more people IP PINs. As you can imagine, though, if we had 100 million people with IP PINs out there and they start losing them, which people inevitably do, we then suddenly have a major influx of calls and revalidations that go on that would be almost impossible for us in our present resource-constrained situation to handle.

But we are kind of gradually working into it because, for someone who has an IP PIN, it is added security. That is why the 104,000 who had data illegally obtained are being offered the opportunity to get an IP PIN if they would like.

Senator AYOTTE. And as I understand it, you cannot e-file with an IP PIN, too, so——

Mr. KOSKINEN. Pardon?

Senator AYOTTE. You cannot e-file when you have an IP PIN. Is that true?

Mr. KOSKINEN. No; you can. I e-filed this year. I actually live in the District of Columbia and thought, well, as the Commissioner, I ought to try the pilot program.

Senator AYOTTE. So you can do it with——

Mr. KOSKINEN. Yes. You can file. Our joint return with IP PINs for the two of us went through.

Senator AYOTTE. So one of the things I wanted to understand, too, is do you feel you have the legal authority today to contract with any fraud prevention tools that you might think are effective for the agency? Or is that authority that you need from us? Obviously, I know the resources need to be there, but——

Mr. KOSKINEN. Right. I have not been made aware of any legal restrictions on our ability to actually take advantage of external things. In fact, already, as Mr. Millholland said, for the out-of-wallet authentication, those questions come from a third party that we selected by route of a competitive contract. So at this point, nobody has told me that we are hamstrung in any way that way, and, in fact, we have spent a lot of time over the last 4 or 5 years in consultation with financial institutions and others about what their authentication is. And as I say, we just spent the last 3 months with States and with the private sector tax preparers and software developers sharing information about existing authentication regimes and what we can do among the three of us to deal with it better.

One of the things we can do, we are thinking about—that I have always been intrigued by is we could charge you $1 for your transcript, and then you would pay for it with a credit card, and that would be a multifactor verification because you would have to have the credit card handy. Now, of course, there is enough data out there, some criminals have your credit cards as well, but they would not necessarily know which one to use and which one was available. So there are different elements of that that we are looking into.

Senator AYOTTE. You think about the challenges that people are facing. Right now, on the refund issue, do you screen refunds for last known bank accounts or mailing addresses which are consistent with past returns before checks are mailed out?

Mr. KOSKINEN. We have a whole series of filters in our system that we generally do not talk a lot about for obvious reasons.

Senator AYOTTE. Sure.

Mr. KOSKINEN. One thing we have looked at, you have to understand with addresses, is we are little less mobile than we used to be. It used to be 20 percent of people moved every year. And, in fact, therefore, if we never got anybody moving with new addresses, we would be suspicious.

Senator AYOTTE. Well, and also if you have a multiple refund situation, it strikes me as being able to look at, where has there been some consistency on mailing address or bank accounts, because the multiple refund issue has to obviously raise a big flag.

Mr. KOSKINEN. And we cut that. It took us a little while to catch up with that, but this year, for instance, we would only send three refunds to a bank account. Beyond that, if whoever was collecting them, preparers or otherwise, we mailed the checks.

Senator AYOTTE. So one other thing that I wanted to ask about was what you tell victims, because it strikes me what we heard from Mr. Kasper who was here, but also have heard this from other of my constituents, that the IRS did not tell Mr. Kasper whether his case would be investigated, whether law enforcement would be notified, or whether there was any action taken on his case. So if I am a victim and I am trying to contact the IRS, what is the IRS taking in terms of telling me?

And then for this category of people that you have some kind of red flag, where there may be an indicator, are you affirmatively notifying anyone that we are seeing something on our end that should cause you to examine your financial records?

Mr. KOSKINEN. We are. That is one of the reasons we are writing letters to the 100,000 that did not lose any information, because we know that there are indications that criminals have at least some of their personal——

Senator AYOTTE. And if they do not use it now, they could use it in the future.

Mr. KOSKINEN. They could use it in the future. So we think it is important for that second group of 100,000 to get a notice from us to give them an opportunity to protect their data and their identity to the extent they can. And we have marked their accounts so that someone cannot file a fraudulent return on their behalf as we go forward.

But it is important for us—we have a whole series of people who have been delighted with their care. The people who handle dealing with ID theft victims, our call center people, are dedicated to helping them. They go out of their way to try to be as helpful as they can. There have been, and particularly early on when we were overwhelmed, 4 of 5 years ago, even up to maybe 3 years ago, people just did not have a lot of time. But we have tried to refine both single point of contact internally but try to make sure that we respond quickly, that refunds are issued, and that cases are resolved inside of 120 days, because while people sometimes have a hard time understanding it, we spend a lot of time trying to help taxpayers across the board figure out what they owe, how to pay it. And so anything we can do, particularly for taxpayers in this situation, to help them, we are going to.

We cannot tell them, because we do not know, whether anyone is going to actually be charged for that case. It is turned over to our criminal investigators. They do not prosecute. They then turn cases over——

Senator AYOTTE. Well, and I know my time is up, but one thing I wanted to understand fully is if you turn it over to your criminal—I was a prosecutor before this, so if someone came in to report a crime—and this is a crime, clearly.

Mr. KOSKINEN. Yes.

Senator AYOTTE. We could not tell them all the information on the ongoing investigation, but we could tell them that, yes, this is going to be referred to law enforcement, and here is the law enforcement agency that is going to be handling that. I have not gotten that sense that that is happening with the IRS, and is it or isn't it being—I know you have your own investigators, but does it end there, or does it get referred to—for example, Mr. Kasper was able to go to a local police agency.

Mr. KOSKINEN. Well, one of the things that we advise people, both on the website and when they call, is they should actually go immediately and report the case to their local law enforcement authorities, and they should report it to the Federal Trade Commission as well, as well as to us, and we report it—and TIGTA keeps track of all this. So we are delighted to have as many law enforcement or other people involved as possible.

So the taxpayers who are victims of identity theft, one of the pieces of information they should be getting is that they should themselves feel comfortable directly going and, in fact, should go—and, in fact, for authentication sometimes we need an affidavit that they have gone—to local law enforcement.

Senator AYOTTE. Well, this is obviously a really important issue. I want to thank the Chairman and Ranking Member for holding this hearing. I have a number of questions I am going to submit for the record, because this issue is one I hope obviously the Committee works on with you to get this right for taxpayers. So thank you both for being here.

Chairman JOHNSON [Presiding.] Thank you, Senator Ayotte.

I just have a couple closing questions, and then we will give you an opportunity to make some final comments.

Mr. Millholland, when you were setting this thing up, considering it in 2013 before you set it up in 2014, did you ever review and take a look at utilizing for that second step using a phone number or some identifier from an actual tax return?

Mr. MILLHOLLAND. There were a number of options we considered as we were looking at how do you know this is the person, if you like. Some of that information was considered. I cannot remember all the factors, so to speak, but we really came down to say let us use this out-of-wallet approach with a third party. That seemed to be where the energy was, and it was like more believable and such that these credit scoring agencies would have a lot more information about the individual than we would. And, thus, that is what we basically focused on.

Chairman JOHNSON. We did have Dr. Fu go through that list of questions and just pretty well show how incredibly easy it is to have that information, particularly in light of the fact that we know we have a billion people whose identities have been compromised and all that information with Social Security numbers is readily available. I mean, did you factor that in?

Mr. MILLHOLLAND. It was factored in in the following way: Yes, the ease of use of the system for the taxpayer versus our confidence level at least equivalent to the phone, if somebody had called in, that this is the person who they say it would be. I previously remarked that, of course, in hindsight we had not thought about the mass attack like this. We thought of individuals coming in to try to fake it, but not the mass. And, frankly speaking, that is one of the mistakes we made in this.

Chairman JOHNSON. I appreciate the fact that the IRS has taken the decision to shut this site down because of the danger, the risk to taxpayers of losing even more information. Are you surprised that none of the other government agencies that are using this have not made that same decision?

Mr. MILLHOLLAND. I really cannot comment on how they balance their risks. The whole cyberspace, so to speak, with these kind of applications, you always are making tradeoffs of risks, how risky is it versus the benefit you are getting from it. As I say, 23 million taxpayers got their transcripts successfully. That is a tremendous saving in productivity for them and, of course, a cost savings for the IRS.

Chairman JOHNSON. Yes, but the IRS has made a decision because of the risk to taxpayers. What about the Social Security Administration? What about CMS with Healthcare.gov? OK, I can understand decisions being made and thinking this will be secure enough. Now we know it is not secure enough. It is highly vulnerable. And I guess I will ask you, Mr. Commissioner, are you surprised that—have you been contacted by any of these other Secretaries or department heads or agency heads in terms of the decision you made? And are they mulling the same decision?

Mr. KOSKINEN. We have had enough visibility with this issue that I would assume that everybody is, but I have not been contacted. And as Mr. Millholland said, they are all dealing with a whole set of unique circumstances and challenges in their agencies, and I am confident they will continue to make the right decisions. And if they need information from us, we obviously communicate and provide security information across the government. So at this point, I do not know what they are doing, and there is no way I can second-guess what they should be doing or what they have been doing.

Chairman JOHNSON. So you have not been contacted by Sylvia Burwell or none of the other agencies that are using this have contacted you directly to just talk about your experience, asking you the questions I am asking, and talk about the decision you made?

Mr. KOSKINEN. None of them have, and none of them at the technical level either.

Chairman JOHNSON. OK. Well, if they are watching here, I would highly recommend that they get in touch with both of you gentleman and start thinking long and hard about whether or not they ought to be taking their websites down or changing this very quickly.

Mr. Millholland, how quickly would you be able to set up a new authentication system with multiple steps that would be more secure?

Mr. MILLHOLLAND. The question literally comes down to how should we extend the multifactor approach into this application and what level of confidence do we want to have that the person is who they say they are. This will range from work that we already have initiated. As I say, we are still doing the analysis of what happened and such. We have to settle these 13,000 taxpayers right now, but then present the options and debate it inside.

But I suspect that we will be bringing the decision to the Commissioner before the end of June of here are the investments we think we now want to make in hardening this, and then that will go through a process of decisionmaking. It probably will involve externals.

Chairman JOHNSON. How many months do you think it will take you to actually implement increased security and be up and running again? Do you have any kind of outside estimate? I am not going to hold you to it. I mean, is this months or is this going to be dragging to 2016?

Mr. MILLHOLLAND. The way I would answer it is to provide a reasonable level that the people are who they say they are. Reasonable is in the eye of the beholder, actually, in this beholder, that we think this person is who they say they are with this level of confidence. Here is what it will take to do that. It may involve things like, hey, if you are asking for a transcript, maybe we ought to have you use your credit card, another form of authentication, charge you $1 or whatever, so that at least we now have that additional piece of information about you. All those things can be done, I will say, in a straightforward way. Certainly we will do this before the next filing season.

Chairman JOHNSON. Through a third-party vendor, will you be able to access a beefed-up security system other than this? Or is this going to be something that you are going to have to use a third-party vendor and implement something within your own software system?

Mr. MILLHOLLAND. My leaning right now today is beef up the use of the tools that are already available from the out-of-wallet provider. There are a number of technology things we can do, like, for example, the IP address of the person that made the request. Are they now switching devices when they make a second request—that kind of information is known—and a number of other, I will just say, technology approaches that are available from that third party.

In addition, there are the other choices we have from a technology view. What kind of blocks do we want to put on this? As I said earlier, you only get one e-mail address with one Social Security number, if you like. That has consequences. As I say, well, suppose a person wants to change the address, how easy do we make that? And all those what-ifs unfortunately, Mr. Chairman, increases costs and the complexity of the solution we want to put out.

In any case, I think we will be able to make significant hardening of this particular application certainly before the next filing season.

Chairman JOHNSON. So were those capabilities to harden this security available from the third-party vendor when you were going through this in 2013? Are these new capabilities? Or was it primarily just a cost decision that it will harden our capability but it is going to cost too much?

Mr. MILLHOLLAND. I frankly do not remember all the technology capabilities that this particular third party had at the time. I do know that when we made considerations of the tradeoffs, the tradeoffs were keeping it easy like it was on the telephone versus adding this additional layer of questions and complexity. And that was a frank and vigorous exchange of views inside the agency about how we ought to do that.

Chairman JOHNSON. What is the cost of this outside vendor for this application?

Mr. MILLHOLLAND. I think it was around 10 cents per transaction to get per question. I am not 100 percent positive about that.

Chairman JOHNSON. It is a per question cost.

Mr. MILLHOLLAND. Right.

Chairman JOHNSON. So that thing right there costs 40 cents, and if you have 23 million accessing this——

Mr. MILLHOLLAND. It is clearly one of these things that is negotiable with the particular suppliers. You could say a bundle of questions could be X amount. All those go into the contract negotiations and such.

First is the cost of, well, suppose you just kept it the normal way and let us say we mailed you your tax return. That is 40 or 50 cents to do that. So all those go into those tradeoff decisions of benefit versus the risks, and that is going to be one of the things we have to weigh as we decide how hardened do we want this.

Chairman JOHNSON. Mr. Kasper in his testimony said that when he contacted the IRS and talked about the fact that somebody had already filed a tax return on that, the IRS did react by saying that there was something suspicious about the address being used by the criminal. Do you know what that was?

Mr. MILLHOLLAND. In Mr. Kasper's case, no, I do not.

Chairman JOHNSON. Those addresses used, were those easily identifiable as Russian, or were they addresses in the United States but somehow you were able——

Mr. MILLHOLLAND. They were—go ahead.

Mr. KOSKINEN. I am going to say the IG has asked us not to speculate in public about where the domains were set up. There were domains that were set up for this purpose relatively recently, and we would be delighted to give you that information off the record.

Chairman JOHNSON. OK. That is really all the questions I have. I am happy to give you gentlemen the opportunity to make a final comment before we close the hearing.

Mr. KOSKINEN. I appreciate that, Mr. Chairman. First, as I said to start my testimony, this is a serious issue. We take it seriously. Protecting taxpayers and their information is a high priority for us, in many ways the highest priority.

This is, as I said, in many ways a shot across the bow. The issue we are dealing with here, critical to the taxpayers whose accounts were accessed, is about a Web access, a Web program we have that does not have anything to do with our system. But as I say, we increasingly over the last 3 or 4 years have seen that more and more of the identity theft we are seeing, more and more of the attacks we are seeing are coming from organized crime and syndicates around the world. So it is, as I fondly say, no longer bean bag. We are actually in the middle of a war with very sophisticated, well-funded, intelligent enemies.

And so the challenge for us all—and it is not just a problem for the IRS, not just a problem for government agencies. It is obviously a problem for everyone in the financial services industry, everyone who has data, financial or otherwise, on people, to try to figure out how to battle this most effectively.

So to some extent, it is a question of funding for how do we make sure our system is secure across the board as we go. But it is not just a question of money. It is also a question of just a continual attempt to assess where you are and where you are going. So we should always assume that we have to get better, which means as we get better over time, we will always be better than we were in the past.

The system of out-of-wallet authentication, already 22 percent of taxpayers cannot answer their own questions. In some cases it means that the criminals are better able at answering the questions in some cases than the taxpayers. So to Mr. Millholland's point, you are always doing that balancing act: Do you make it inaccessible to taxpayers and increase the burden, and at what cost? Clearly, I think that with all of the breaches that have gone on, as I noted, I think—it is hard to remember what I have noted here and earlier today. The IRS was one breach out of 25 in the month of May across the world. So, clearly, we are dealing with unknown volumes of information out there that dwarf anything we could imagine.

So we are going to continue now, I think, to have to assume that we are at risk. It is what we assume in our normal day with our security for the overall cybersecurity issue of our system, is to assume that we are at risk. So even as we harden this program and put it back up—and we will not put it back up until we feel comfortable with it, even then we will run on the assumption that we are at risk. And we need to do that, and I think that is the only way we are going to be able to continue to make progress.

But it is not a simple problem. It is a complex one that is going to take the best efforts of everyone, and that is why we are delighted to have what I think is going to turn out to be a very successful partnership as a result of the Security Summit we put together with the private sector, because we all agreed we can do a lot more together working with various levels and layers of authentication and protection than any group, whether it is the private sector or the States or the IRS, by themselves can do, and that is what we are committed to doing going forward.

Chairman JOHNSON. Thank you, Mr. Commissioner. Mr. Millholland.

Mr. MILLHOLLAND. I have no closing remarks.

Chairman JOHNSON. OK.

Mr. MILLHOLLAND. Thank you, though.

Chairman JOHNSON. I would like to ask consent to enter into the record two articles,[1] Krebs on Security and Nextgov, “Other Agencies Use Same Log-on Procedures As Exploited IRS Site.” Without objection, so ordered.

I want to thank both of you for your thoughtful testimony and your answers to our questions.

Mr. Commissioner, I would ask that you take a serious look at the Social Security Identity Defense Act of 2015. I think it really would be a very helpful piece of legislation to allow, actually require the IRS, when you are made aware of the fact that identity theft has occurred, to notify the taxpayer as well as Federal authorities so they can track down the criminal, and we can, end those types of activities. So if you could look at that, I would appreciate you working with our staff, and hopefully you can be supportive of that.

With that, the hearing record will remain open for 15 days until June 17 at 5 p.m. for the submission of statements and questions for the record.

This hearing is adjourned.

[Whereupon, at 4:28 p.m., the Committee was adjourned.]

[1] The articles referenced by Senator Johnson appears in the Appendix on page 86.

APPENDIX

Opening Statement of Chairman Ron Johnson

"The IRS Data Breach: Steps to Protect Americans' Personal Information"

June 2, 2015

As prepared for delivery:

Good afternoon and welcome.

Last week, the IRS announced that, from February through mid-May this year, criminals accessed the past tax returns of 100,000 Americans using IRS' own website, and attempted to access the tax information of many more.

Using stolen information on taxpayers and public data sources, criminals created fraudulent accounts on IRS.gov in the names of real taxpayers. This allowed the criminals to obtain those taxpayers' previous tax returns directly from the IRS, including data such as adjusted gross income (AGI) that criminals can use to submit fraudulent returns to the IRS. In short, IRS.gov provided criminals with the information they needed to successfully defraud taxpayers.

These criminals' ability to defraud the American taxpayer was made possible, in part, by the IRS' decision to ignore the advice of a cybersecurity expert earlier this year. In late March, prominent cybersecurity journalist Brian Krebs published an article highlighting weaknesses in the way the IRS verified users' identities on its website. The article noted that IRS.gov relied on knowledge-based questions to authenticate users that can be answered using information easily obtained online — questions like, "When did you purchase your home?" or "When did you purchase your car?"

Although the IRS was made aware of the weaknesses in its authentication practices as early as March, according to Commissioner Koskinen the IRS made a conscious decision to not make any changes to its authentication practices. It was not until after IRS employees discovered the breach in late May that the IRS disabled the "Get Transcript" functionality of its website — nearly two months after these concerns were first brought to light. Professor Kevin Fu from the University of Michigan and Mr. Jeffrey Greene from cybersecurity firm Symantec, who have joined us here today, will speak to the weaknesses of knowledge-based authentication and will discuss alternatives that would provide more security.

The case of one victim of this data breach at the IRS, Michael Kasper, was highlighted in the article brought to the IRS' attention in March. Mr. Kasper is here with us today as well. Mr. Kasper attempted to file his tax return online in February, only to discover that criminals had already filed it for him. He soon learned that the thieves had also created an account in his name at IRS.gov, apparently to obtain his past tax information in order to make their fraudulent return look legitimate. In his testimony, Mr. Kasper will expand on the details of this difficult experience, and how he was forced to track down the criminals who impersonated him without the help of the IRS.

According to the IRS, about 13,000 questionable tax returns have already been filed in the names of victims of this breach. Through these likely fraudulent returns, the IRS has transferred up to $39 million to criminals. Further, the cost to taxpayers may rise as criminals file fraudulent returns in the names of other victims.

Unfortunately, the damage to taxpayers doesn't stop there. Although the IRS will provide taxpayer-financed credit monitoring to the 100,000 victims, many forms of identity theft — such as fraudulent applications for government benefits — do not appear on credit reports. As a result, credit monitoring will not detect that form of fraud and the ultimate cost of this breach is likely much higher.

The privacy implications of this breach are profound. In this time of vigorous debate about the privacy implications of the NSA's collection of telephone metadata — phone numbers and times and dates of calls — the IRS is conducting data-mining on Americans and has allowed foreign organized crime syndicates to access the financial histories of more than 100,000 Americans.

Just as concerning is the fact that other government websites, such as Healthcare.gov, suffer from the very same authentication weaknesses. This is an issue I intend to look at deeply in the coming weeks. Federal agencies must do a better job safeguarding the massive amount of data they collect from the American people.

IRS Commissioner John Koskinen and IRS Chief Technology Officer Terence V. Milholland will also testify today, and we appreciate their appearance. We look forward to their explanations of the timeline and decision-making process they followed in setting up and securing IRS data on millions of Americans.

###

Statement of Ranking Member Thomas R. Carper

"The IRS Data Breach: Steps to Protect Americans' Personal Information"
June 2, 2015

As prepared for delivery:

Nearly every day, we learn of another major cyber attack or data breach on an American company or organization. In many ways, we are dealing with an epidemic of online theft and fraud. That epidemic is growing at an alarming rate and continues to victimize and frustrate more and more of us.

Over the past several months, for example, we witnessed several companies in the healthcare sector suffer major data breaches. And, of course, we know that our government networks are under constant attack in cyberspace.

These attacks are growing ever more sophisticated, too. That's happening at least in part because our defenses are also getting better. Still, we must do more to stay ahead of those that would do us harm. And, we must learn from those instances when criminals have been successful in getting past the protections we put into place and create havoc.

Today, we will take a closer look at the recent cyber attack on the Internal Revenue Service (IRS). We will examine what went wrong, how the IRS is trying to repair the damage, and what we can do to reduce the likelihood to make sure that something like this doesn't happen again, either at the IRS or elsewhere.

From what we know so far, the attack on the IRS appears to have been an especially sophisticated one. We also know that the IRS had defenses and fraud prevention measures in place at the time of the attack. Yet despite the precautions that were taken, skilled criminals were able to use innovative tactics to trick the IRS system into releasing past tax returns.

Given the vast amounts of sensitive information the IRS possesses, it is critical that the agency continues to do more to protect the American taxpayer. In fact, all agencies need to step up their efforts and improve their cybersecurity posture. The wake-up call has been ringing for years now. We need an all-hands-on deck effort in responding to it.

As we know, cybersecurity is a shared responsibility. Those of us here in Congress have an obligation to ensure that agencies have the funding, the tools and the authority they need to adequately protect their systems from attack. Unfortunately, Congress has significantly reduced IRS funding in recent years, and we've done so while also tasking the agency with far greater responsibilities. In fact, the IRS is operating at its lowest level of funding since Fiscal Year 2008. These cuts have had real consequences for the agency and American taxpayers.

I look forward to hearing from the Commissioner today about what he needs to better protect his agency from fraud and cyber attacks. Here in the Committee, we've been working hard to address our country's cybersecurity challenges. Our efforts led last year to the enactment of four key pieces of cybersecurity legislation. One of these bills updated the Federal Information

Security Management Act or 'FISMA' to better protect federal agencies from cyber attacks. Another codified the DHS cyber operations center. The two others strengthened the cyber workforce at the Department of Homeland Security.

This year, I introduced an information sharing bill and have been working closely on this issue with our colleagues on the Senate Intelligence Committee. I have also been working closely with Senator Blunt on data breach legislation that will create a national standard for how we protect data and consumers. It is my hope that we can come together as a Congress to pass these two important pieces of legislation and provide our agencies with the resources they need to tackle the nation's growing cyber threat. With that, I would like to thank all of our witnesses for joining us here today. We look forward to your testimony.

###

Statement of Mike Kasper

June 2, 2015

Dear Members of the Committee:

On Friday, February 6, I filed my taxes by using the desktop version of Turbo Tax like I do every year. However, later that evening I got an email notice from Turbo Tax that the IRS had rejected my return because a federal tax return had already been filed by someone else using my social security number.

On Monday morning, February 9, I called the IRS identity theft hotline who confirmed my identity with tax related questions and then told me a direct deposit was being made for a tax refund filed with my social security number on that same day, into a bank account different than any that I had used before. Obviously, I knew and they agreed this was fraud, but they said it was too late to stop the deposit now. In addition, since I was alerting them this transaction was fraudulent, their privacy rules prevented them from giving me any more information, such as the routing number and account number of that deposit.

When I asked why, they all but admitted it was to protect the privacy of the criminal, not because they were going to investigate it right away. If I had played dumb and just asked what account my deposit was going into they probably would have told me. Yet because I was straightforward and told them it was fraud, they would not tell me, even in person at the IRS office. They were clear, my case would not be investigated further until a fraud affidavit and accompanying documentation were processed by mail. They said if I had filed a day earlier and called on Friday, they could have just stopped the deposit, but because it was being paid they could not tell me more, or call the bank, until it was fully investigated.

The most interesting thing to me about this rule is that the IRS itself refuses to look at the bank account data until it is fully investigated. Banks are required by law to report suspicious refund deposits, but the IRS does not even bother to contact banks to let them know a refund deposit was reported fraudulent, at least in the case of individual taxpayers who call, confirm their identity and report fraud, just like I did. The IRS told me it can take six months to investigate. Meanwhile, an unknown criminal has all my data.

Frustrated by not knowing who stole my identity, I then tried to get a transcript of the fraudulent return online using the Get Transcript function on IRS.gov on the same day, February 9, but I soon learned that someone else had already registered their email address for my social security number. When I called IRS eServices to fix this, and spent another hour on hold, they explained they could not tell me what the email address was either, due to privacy regulations, but something about the email address led them to believe that is was not me and it seemed suspicious. They said they could not change the email address, all they could do is ban access to eServices for my SSN. It was unclear if they would investigate further.

Regardless, I was able to successfully ask the IRS for a copy of the fraudulent tax transcript sent by mail, which I got a few weeks later. It did not show the deposit account number, but showed whoever filed it had access to my 2013 tax return, because the amounts were very similar and they knew a lot about me. Eventually, by looking around the IRS website, I discovered that I could submit Form 4506 and pay $50 for a photo copy of the fraudulent return, which I did. Just $50 and they would ignore the privacy rules.

On March 17, I obtained the photo copy of the fraudulent return in the mail which showed the bank account information and I saw the fraudulent return was submitted January 31, 2015, with a corrected W-2 that had increased the withholding by exactly $6,000 to increase their total refund due to $8,936.

On March 18, I contacted First National Bank of Pennsylvania whose routing number was listed, and reached their head of account security who called back and confirmed a direct deposit by the IRS for $8,936.00 was made on February 9, 2015 into someone else's checking account, but specifying my name and my social security number in the meta data with the deposit. She told me that she could also see that transactions were made at one or more branches in the city of Williamsport, PA to withdraw those funds and a substantial portion of the money was gone. She also told me that no one from the IRS had contacted her bank to raise any questions about that deposit, despite my fraud report filed February 9. She said she was required to report it to the IRS herself now, and would cooperate with local police too.

At this point, I finally had some progress, a chance to find my ID thief. So I called the Williamsport police and spoke to the Lieutenant who heard my story and sympathized with the lack of any investigation by the IRS. He asked me to write out my story in an email to his Captain, which I sent to them on March 19. About two hours later, I received a call from an investigator who had been assigned to work on my case. He followed up March 20 with the bank, then interviewed the person who held the account and told me the bank's fraud department was investigating it now too, and had asked the woman to return the cash.

It seemed like my case was basically solved. However, it turned out to be more complex. At least if you believe the story that the account holder is telling. According to her, she herself had been conned. She said she responded to a Craigslist ad about a money making opportunity. Money was deposited into her account, and she sent money to individuals in Nigeria through Western Union, keeping some as a profit, and apparently never suspecting that she might be doing something illegal. I'd like to believe her story, but wouldn't someone who could pull this off also have an explanation ready? Apparently she received the refund for someone from South Dakota as well and I believe that a warrant is out for her arrest now. Regardless, I believe that being able to get a copy of the return for $50 and contacting the bank did help to resolve my case. Just over 90 days after I filed, I got my full tax refund check in the mail on May 12. Several days later, I received a letter from the IRS stating that my identity theft case was confirmed and that I would receive an Identity PIN at the end of the year to use when filing my taxes next year in 2016.

The GAO found millions of people experience stolen ID refund fraud and $5.8 billion is lost each year. By contrast 5,000 banks are robbed and $6,000 lost on average. This fraud equals 1 million bank robberies. If the IRS cannot handle all of this fraud, redact any unrelated third party SSNs and mail taxpayers copies of returns to pursue it themselves with local law enforcement or banks, like I did successfully in my case. USPS is the preferred means of communication for the IRS so they need to use it more to help taxpayers.

Last but not least, why does the IRS rely on a few multiple choice questions to safeguard tax transcripts? E-filing PINs are even easier to get. It is so simple to file a false tax return for a refund it is actually giving criminals an incentive to attempt more data breaches, since they can trade SSNs for cash from the IRS. I understand putting government services online provides significant cost savings, but it needs to be done securely to avoid actually costing more to reverse all the damage done by criminals committing ID theft. Computer security requires a more advanced approach today than it did five years ago. It is no longer enough to put up strong filters and firewalls and depend on them holding. You have to assume criminals will find a way around them and actively monitor all systems like the immune system does in our bodies. I'm not an expert on fraud, but I believe a lot more can be done to protect taxpayers and to prevent this.

Sincerely yours,

Mike Kasper

STATEMENT OF PROF. KEVIN FU, PH.D.

DEPARTMENT OF
ELECTRICAL ENGINEERING & COMPUTER SCIENCE
UNIVERSITY OF MICHIGAN
ANN ARBOR, MI

KNOWLEDGE-BASED AUTHENTICATION (KBA)

SUBMITTED TO THE
U.S. SENATE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS

HEARING ON
THE IRS DATA BREACH:
STEPS TO PROTECT AMERICANS' PERSONAL
INFORMATION

TUESDAY, JUNE 2, 2015

1 Introduction

Good afternoon, Chairman Johnson, Ranking Member Carper, and distinguished members of the Committee. I am testifying before you today on the use of instant "secret questions" in knowledge-based authentication (KBA) related to the recent IRS breach. I will explain the key properties of instant KBA to give you a better understanding of current challenges and vulnerabilities. I will close with recommendations on what can be done in the future to avoid similar, large-scale breaches.

My name is Dr. Kevin Fu. I represent the cybersecurity research community. Cybersecurity researchers innovate technologies and principles to improve cybersecurity as well as break security systems to understand their weaknesses and limitations. I am Associate Professor of Computer Science & Engineering at the University of Michigan where I teach and carry out research on how to improve the trustworthiness of computer systems. My educational qualifications include a Ph.D., master's degree, and bachelor's degree from M.I.T.'s Department of Electrical Engineering and Computer Science. We teach programming to over 1,300 undergraduates each year, and we teach a rigorous course in computer security to 440 undergraduates each year.

I am speaking today as an individual. All opinions, findings, and conclusions are my own and do not necessarily reflect the views of any of my past or present sponsors or employers.

2 Authentication

Authentication is the process of verifying a claimed identity. For instance, the IRS web site attempted to verify the claimed identity of a user before disclosing transcripts of tax returns. There are three basic means to authenticate an identity:

- Inheritance-based: Something you are (e.g., biometrics, fingerprints, iris scans, signatures)
- Ownership-based: Something you have (e.g., ID cards, mobile phones, tokens)
- Knowledge-based: Something you know (e.g., **secret questions**, passwords, PINs)

Let me focus on "secret questions," which is a form of knowledge-based authentication (KBA).

3 Knowledge-Based Authentication (KBA) with Secret Questions

There are two popular ways of using secret questions to authenticate a user: static and instant. The recent IRS "get transcript" breach involved an attack on the instant KBA. To better understand instant KBA, let me first contrast it with static KBA.

Static KBA. Users will recognize that many financial web sites and cloud services ask for answers to "secret questions" during the initial creation of an account. The secret questions serve as a backup mechanism to reset lost or forgotten passwords. Static KBA would not be appropriate for establishing *initial* trust in an identity. IRS did not use static KBA, and that is an appropriate design choice for their situation. Common static KBA questions include:

- Where were you born?
- What is your favorite food?
- What is your favorite sports team?
- Where did you meet your spouse?

Instant KBA. Instant KBA (also known as dynamic KBA) also uses secret questions to authenticate a user. However, in instant KBA, the user does not file answers to secret questions beforehand. Instead, the web site presents personal questions with answers readily available or purchasable from credit reports and other financial sources. Thus, the site can verify that the user knows certain knowledge that is more difficult to obtain than publicly available data. The IRS "get transcript" service used instant KBA questions to authenticate tax payers downloading transcripts of their tax returns. The questions and answers were provided by a third party from the private sector.

To verify your identity, please select your previous address:

A. 52 Church St

B. 1600 Pennsylvania Ave

C. Gettysburg

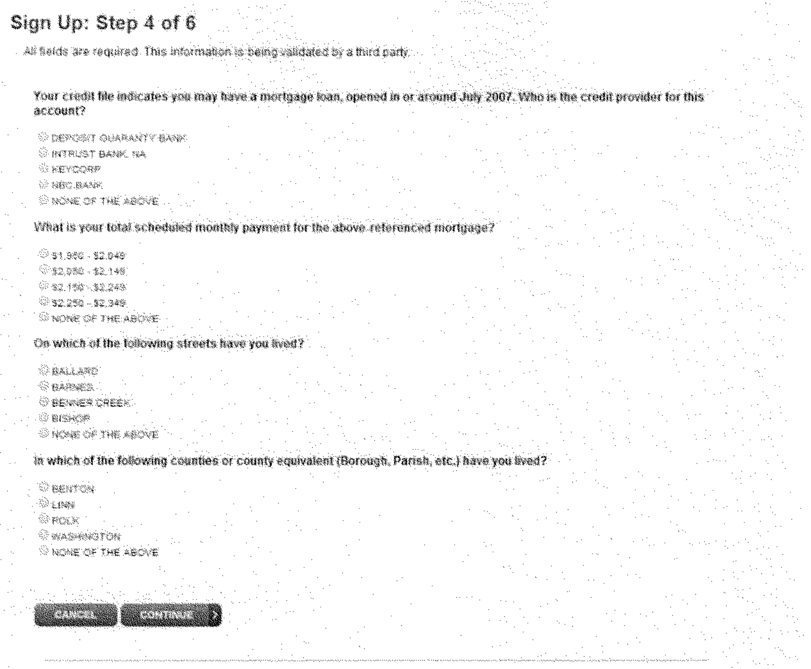
D. None of the above

Figure 1: An illustrative example of a hypothetical instant KBA question drawn from financial records to establish faith that a user is who they claim to be.

4 Anatomy of Instant KBA at IRS Get Transcript and SSA mySSA

My understanding is that multiple federal sites make use of private sector services for instant KBA secret questions to verify the authenticity of a claimed tax payer identity. For instance, the mySSA site[1] advertises that it uses Experian to verify claimed identities with four secret questions. I believe that IRS used a similar service.

[1] https://secure.ssa.gov/



Sign Up: Step 4 of 6

All fields are required. This information is being validated by a third party.

Your credit file indicates you may have a mortgage loan, opened in or around July 2007. Who is the credit provider for this account?

○ DEPOSIT GUARANTY BANK
○ INTRUST BANK, NA
○ KEYCORP
○ NBC BANK
○ NONE OF THE ABOVE

What is your total scheduled monthly payment for the above referenced mortgage?

○ $1,950 - $2,049
○ $2,050 - $2,149
○ $2,150 - $2,249
○ $2,250 - $2,349
○ NONE OF THE ABOVE

On which of the following streets have you lived?

○ BALLARD
○ BARNES
○ BENNER CREEK
○ BISHOP
○ NONE OF THE ABOVE

In which of the following counties or county equivalent (Borough, Parish, etc.) have you lived?

○ BENTON
○ LINN
○ POLK
○ WASHINGTON
○ NONE OF THE ABOVE

Figure 2: A screenshot of sample instant KBA secret questions at the IRS "get transcript" web site after having entered personal data and completed an email confirmation check from http://lpc.financialaidtv.com/cats/general_information#playlist-8075%3Avideo:video-5. It is believed that hackers answered these secret questions correctly by using personal data taken from any of the many breaches in the private sector.

5 KBA: Strengths and Limitations

No one system is perfect. Instant KBA does improve the security of identity verification by making it more difficult for an adversary to compromise a system, but sophisticated adversaries can nonetheless circumvent the protections at unprecedented scale, as demonstrated by the recent breach of 100,000 tax payer records at IRS. The root cause is that our supposedly independent systems are highly dependent on each other, and a seemingly unrelated compromise at one provider (e.g., Anthem, Target) can affect the security at a different service provider (IRS).

The main strength of instant KBA is ease of use. Most legitimate tax payers will be able to authenticate by answering multiple-choice questions about their personal, financial, and tax history. However, a major limitation is that the security of the system rests on assumption that the adversary does not have access to this information.

Instant KBA is designed under the threat model where an adversary may have stolen a tax payer's wallet. Using only the stolen wallet, it would be difficult for a criminal to answer four instant KBA questions successfully. Unfortunately, this threat model is no longer realistic as countless databases of such personal information have been compromised.

Opting out. Tax payers get no chance to opt out of the risks of instant KBA. As NIST explains in a technical report, "Instant KBA is not acceptable when transactions result in the release of sensitive or private information related to an individual." NIST researchers further explain:

> "In an Instant KBA authentication system, no matter how carefully the verifier treats the private personal authentication information, unless that information is known only to the verifier, the authentication system is somewhat at the mercy of third parties who may also have this information (and from whom the verifiers may have obtained it). But the user is initially not even a knowing party to the system, has given no consent, and has no obligation to treat every bit of personal private information that might be used in such a system as a secret, nor does the user know what personal private information may be used for authentication. It is inappropriate to involuntary expose the privacy of unknowing citizens to the risks of an instant KBA authentication scheme, unless the

> risks for any individual citizen is very close to zero, however much an adversary may desire the information about that particular user. The (involuntary) users whose information is to be accessed, whether movie stars, public figures, or average citizens, may be expressly targeted by capable, experienced, resourceful attackers such as investigative reporters, private investigators, or personal enemies, who may be motivated to do a great deal of research to learn more about their target. Viewed from that perspective, instant KBA, with its vulnerability to off-line research, is more than a little alarming."

A principle espoused by the security research community is that if a user does not know something is a secret, then it's not a good secret for authentication because the user is easily tricked into divulging such information. Static and instant KBA therefore can violate this principle of security. In the 1990s, cybersecurity researchers initially believed that secret questions would be more secure than passwords. However, subsequent research in social and behavioral studies have shown severe weaknesses in authentication based solely on secret questions.

Lack of instant audibility. When I log into my Apple iTunes account from a new device, Apple sends me an email warning because Apple already knows how to reach me. When I make a credit card purchase, I receive a text message warning from my bank because my bank already knows how to reach me. With instant KBA, a service provider like IRS has no effective way to quickly inform a tax payer that their data or account was accessed because IRS does not already know how to reach the tax payer electronically. Worse, it is difficult for a tax payer to repudiate a fraudulent transaction.

Static KBA as a single factor is unreliable and insecure. Researchers at Google analyzed hundreds of millions of static KBA questions and have come to the conclusion that secret questions have poor reliability and poor security.[2] For this reason, Google services prefer to pair KBA ques-

[2] "Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google" by Bonneau et al. in *Proceedings of the 24th International Conference on the World Wide Web*, May 2015. https://cdn.elie.net/publications/secrets-lies-and-account-recovery-lessons-from-the-use-of-personal-knowledge-questions-at-google.pdf

tions with second factors such as email or SMS messages to mobile phones. Note that the IRS *did* use email as a second factor; thus the adversary appears to have circumvented what Google recommends as a second factor. Their research paper lists a number of technical alternatives to personal knowledge questions in Section 6.2.

Static KBA questions are predictable. In 2009, researchers from Microsoft and Carnegie Mellon University (CMU) conducted a human subjects study of guessability of secret questions from static KBA. The study found that some secret questions had a 15% chance of guessability within five tries without knowing anything about the victim. In fact, the research foreshadowed the IRS breach with their warning that, "While most well publicized attacks on personal questions have been targeted at individuals, our results show that large scale attacks are also possible."[3] The authors recommend eliminating questions that are statistically guessable more than 10% of the time, and flagging questions that exceed a certain threshold of popularity.

6 Alternative Approaches

Let me highlight a few approaches that might improve the effectiveness of the authentication systems at IRS and other federal agencies.

Second-Factor Authentication (2FA). Use of a second factor can make it more difficult for an adversary to impersonate a tax payer online by slowing down or deterring attacks. A second factor should come from the "something you have" or "something you are" categories to be a genuine and independent second factor to "something you know." A popular second factor is a mobile phone. For example, DuoSecurity.com provides a suite of 2FA tools to combat credential theft and breaches. Federal service providers such as IRS could send a text message to a mobile phone to make it more difficult for a single adversary to impersonate 100,000 tax payers. However, no system is fool proof. It merely reduces risk. The threat landscape can change quickly.

[3] "It's No Secret. Measuring the Security and Reliability of Authentication via 'Secret' Questions" by Schechter et al. in *IEEE Symposium on Security and Privacy*, May 2009. http://research.microsoft.com/pubs/79594/oakland09.pdf

Notification warnings. One could imagine the IRS notifying a tax payer when someone attempts to access tax transcripts electronically. For instance, IRS could use contact information in tax returns to reach out to the tax payer or accountant to warn of the attempted download before allowing the download. But such systems are subject to phishing attacks, and would remove the instant gratification of quickly downloading tax returns.

NSTIC. The National Institute of Standards and Technology (NIST) launched the National Strategy for Trusted Identities in Cyberspace (NSTIC) for a ten-year goal of improving authentication of identities. The NSTIC roadmap set guiding principles for federal agencies to improve authentication by partnering with industry service providers. NIST published a report on its NSTIC interactions with IRS.[4]

In April 2015, NIST researchers involved with the NSTIC explained that, "While KBA is widely used today, there is no performance standard for KBA solutions—something that many of the NSTIC pilots have flagged as a significant challenge."[5]

Voice-Based Fraud Detection. The financial sector has been subject to widespread fraud by callers who attempt to engage in identity theft. One novel approach is to analyze the subtle cues in the audio conversation to identify known fraudsters. For instance, one might be asked to respond to instant KBA by phone rather than by typing. The subtle cadence and mannerisms of the speaker as well as the fundamental characteristics of the phone line makes it harder for an adversary to impersonate 100,000 people at once. The machine learning and security analytics are sufficiently effective that service providers can identify when a single fraudster calls back attempting to impersonate yet another consumer. This research was published in 2010, and later commercialized as a company called PinDrop.[6] There is also other research on speaker identification that may help with fraud detection.

[4] http://www.nist.gov/director/planning/upload/report13-2.pdf

[5] http://nstic.blogs.govdelivery.com/2015/04/09/a-retrospective-look-advancing-standards-for-strong-identity-and-authentication-in-the-identity-ecosystem/

[6] "PinDr0p: Using Single-Ended Audio Features To Determine Call Provenance" by Balasubramaniyan et al. in *ACM CCS*, 2010. http://www.cc.gatech.edu/ traynor/papers/traynor-ccs10.pdf and http://www.pindropsecurity.com/

7 Summary and Recommendations

The IRS used instant knowledge-based authentication in an attempt to verify identities seeking transcripts of tax returns. Unfortunately, the threat landscape is changing quickly as attackers adapt to newly fortified defenses. There will always be fraud, but a reasonable goal is to make it difficult for a single adversary to commit wide-scale, automated fraud. A major challenge in identity theft prevention is maintaining low false-positives (that would deny legitimate requests) and low false-negatives (that would allow identity theft) while serving the technologically diverse, tax paying U.S. population.

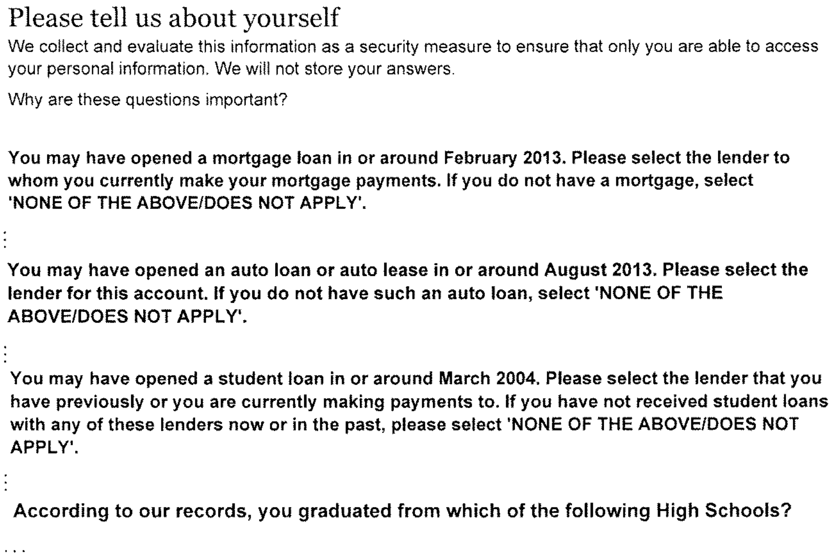
Technical recommendations include:

- Develop KBA performance standards and security metrics so that service providers such as IRS can more meaningfully decide acceptable risk of different kinds of KBA questions.
- Stop using SSNs or financial records as secrets for single-factor authentication because personal data are widely available in underground markets of stolen databases. Such data is effective only against unsophisticated adversaries.
- Consider enhancing KBA with a second factor of authentication from the "what you are" and "what you have" categories such as SMS messages or voice-based fraud detection.
- Leverage the existing cybersecurity expertise within the NIST's National Cybersecurity Center of Excellence (CCoE), National Strategy for Trusted Identities in Cyberspace (NSTIC), and Information Security and Privacy Advisory Board (ISPAB).
- Encourage research collaboration between cybersecurity experts and social and behavioral science to carry out human subjects experiments that measure the risks and benefits of knowledge-based authentication.

We are likely to see more compromises of this nature because of systems depend on each other in subtle ways. What is most interesting is the advanced nature of the threat in the case of the IRS breach. Most cybersecurity research on the limits of secret questions does not consider the case when the adversary has a copy of the answers. Knowledge-based authentication systems are often built to protect against simple guessing attacks, but are not able to withstand an adversary with a complete cheat sheet of all the answers.

Let me end with an anecdote of an acquaintance affected by identity theft of their tax records in a previous incident. In April, an orthodontist received a notice via his CPA that someone had filed a fraudulent tax refund. To reclaim his identity, he had to fill out rather tedious affidavits. He now worries about the process he will have to follow for potentially the rest of his life to simply file a tax return. The identity theft protection does not make up for this orthodontist's significant time lost. Worse, his four-year-old child who was on one of the compromised tax returns may have to cope with the consequences of identity theft for the next hundred years of tax returns.

Thank you. I am happy to answer any questions you may have.



Please tell us about yourself

We collect and evaluate this information as a security measure to ensure that only you are able to access your personal information. We will not store your answers.

Why are these questions important?

You may have opened a mortgage loan in or around February 2013. Please select the lender to whom you currently make your mortgage payments. If you do not have a mortgage, select 'NONE OF THE ABOVE/DOES NOT APPLY'.

⋮

You may have opened an auto loan or auto lease in or around August 2013. Please select the lender for this account. If you do not have such an auto loan, select 'NONE OF THE ABOVE/DOES NOT APPLY'.

⋮

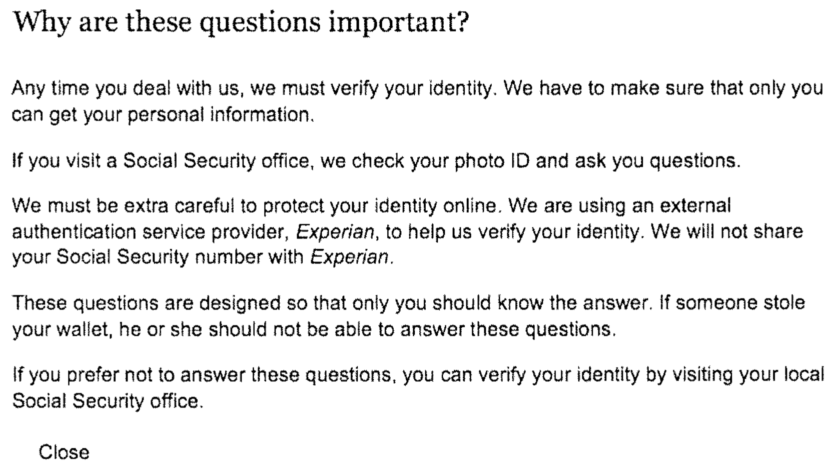
You may have opened a student loan in or around March 2004. Please select the lender that you have previously or you are currently making payments to. If you have not received student loans with any of these lenders now or in the past, please select 'NONE OF THE ABOVE/DOES NOT APPLY'.

⋮

According to our records, you graduated from which of the following High Schools?

. . .

Figure 3: A screenshot of sample instant KBA secret questions at the MySSA web site after having entered basic information such as a tax payer name, SSN, birthdate, and address. For each of the four questions, the user would select one of four multiple choices, often including an option of "None of the Above."



Why are these questions important?

Any time you deal with us, we must verify your identity. We have to make sure that only you can get your personal information.

If you visit a Social Security office, we check your photo ID and ask you questions.

We must be extra careful to protect your identity online. We are using an external authentication service provider, *Experian*, to help us verify your identity. We will not share your Social Security number with *Experian*.

These questions are designed so that only you should know the answer. If someone stole your wallet, he or she should not be able to answer these questions.

If you prefer not to answer these questions, you can verify your identity by visiting your local Social Security office.

Figure 4: A screenshot of the MySSA web site that accurately explains their threat model. Unfortunately, the threats are changing quickly.

Symantec.

Prepared Testimony and
Statement for the Record of

Jeffrey E. Greene
Director of Government Affairs, North America & Senior Policy Counsel
Symantec Corporation

Hearing on

"The IRS Data Breach: Steps to Protect Americans' Personal Information"

Before the

United States Senate
Committee on Homeland Security and Governmental Affairs

June 2, 2015

Chairman Johnson, Ranking Member Carper, my name is Jeff Greene, and I am the Director of Government Affairs for North America and Senior Policy Counsel at Symantec, where I focus on cybersecurity, the Internet of Things, and privacy issues. Prior to joining Symantec, I was Senior Counsel with the U.S. Senate Homeland Security and Governmental Affairs Committee, where I focused on cybersecurity and Homeland Defense issues. I have also worked on the Committee on Homeland Security in the House of Representatives as a subcommittee staff director and as counsel to the Senate's Special Investigation into Hurricane Katrina. I recently served as the staff co-chair of the "Internet of Things" research subcommittee of the President's National Security Telecommunications Advisory Committee, and am a Senior Fellow at The George Washington University Center for Cyber & Homeland Security and a Senior Advisor at the Truman National Security Project. I also co-chair the Homeland Security Committee of the American Bar Association's Section of Science & Technology Law.

Symantec protects much of the world's information, and is a global leader in security, backup and availability solutions. We are the largest security software company in the world, with 33 years of experience developing Internet security technology and helping consumers, businesses and governments secure and manage their information and identities. Our products and services protect people's information and their privacy across platforms – from the smallest mobile device, to the enterprise data center, to cloud-based systems. We have established some of the most comprehensive sources of Internet threat data in the world through our Global Intelligence Network, which is comprised of millions of attack sensors recording thousands of events per second, and we maintain 10 Security Response Centers around the globe. In addition, every day we process billions of e-mail messages and web requests across our 14 global data centers. All of these resources allow us to capture worldwide security data that give our analysts a unique view of the entire Internet threat landscape.

The hearing today not only is timely – given the recent high profile data breaches and other cyber attacks – but also is a critically important discussion that will help focus attention on what government, businesses, and individuals can do to protect themselves from similar attacks. In my testimony today, I will discuss:

- The current cyber threat landscape;
- Some common types of attacks;
- How breaches are happening, including the methods criminals are using to steal data; and
- Security measures to protect data and prevent breaches.

The Current Cyber Threat Landscape

Many of the recent headlines about cyber attacks have focused on data breaches across the spectrum of industries. Breaches impact individuals whose identities have been stolen, the organizations that were compromised, and governments that are seeking ways to set data breach policies and to apprehend the perpetrators. Some of the organizations that suffered significant breaches over the past few years include Anthem Inc., the Internal Revenue Service, the State of South Carolina, Target, Neiman Marcus, Michael's, Home Depot, and Sony, just to name a few.

The recent theft of personally identifiable information (PII) is unprecedented – over just the past three years alone, the number of identities exposed through breaches approached *one billion*. And this is just from known breaches, as many go unreported or undetected. Recent data breaches have touched all parts of society and across the globe, from governments and businesses to celebrities and individuals' households.

While many assume that breaches are the result of sophisticated malware or a well-resourced state actor, the reality is much more troubling. According to a recent report from the Online Trust Alliance, 90 percent of last year's breaches could have been prevented if organizations implemented basic cybersecurity best practices.[1] Moreover, some breaches are actually second generation activity – criminals leverage previously stolen personal information to compromise an individual's account.

Statistics from our 2015 Internet Security Threat Report demonstrate that the cyber threats we are facing on a day-to-day basis are growing. More than 348 million identities were exposed in 2014, a number that seems extraordinary until one considers that 550 million identities were exposed in 2013. Over the past two years, twelve breaches exposed more than 10 million identities each – and this does not include some of the major breaches we have heard about in 2015. These breaches expose PII such as names, birth dates, and government ID numbers. Some breaches also exposed other highly sensitive data, such as medical records or financial information.

While the focus on data breaches and the identities put at risk is certainly warranted, we also must not lose sight of the other types of cyber attacks that are equally concerning and can have damaging consequences. There are a wide set of tools available to the cyber attacker, and the incidents we see today range from basic confidence schemes to massive denial of service attacks to sophisticated (and potentially destructive) intrusions into critical infrastructure systems. The economic impact can be immediate with the theft of money, or more long term and structural, such as through the theft of intellectual property. It can ruin a company or individual's reputation or finances, and it can impact citizens' trust in the Internet and their government.

The attackers run the gamut and include highly organized criminal enterprises, disgruntled employees, individual cybercriminals, so-called "hacktivists," and state-sponsored groups. The motivations vary – the criminals generally are looking for some type of financial gain, the hacktivists are seeking to promote or advance some cause, and the state actors can be engaged in espionage (traditional spycraft or economic) or infiltrating critical infrastructure systems. These lines, however, are not set in stone, as criminals and even state actors might pose as hacktivists, and criminals often offer their skills to the highest bidder. Attribution has always been difficult in cyberspace, and is further complicated by the ability of cyber actors to mask their motives and objectives through misdirection and obfuscation.

Common Types of Attacks

Distributed Denial of Service ("DDoS")

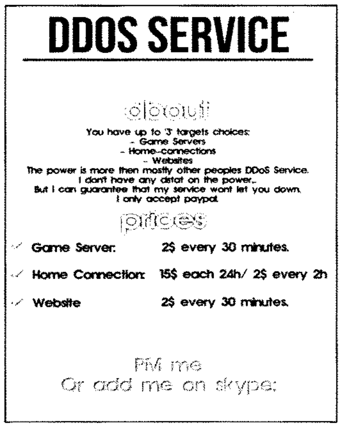
Distributed denial-of-service (DDoS) attacks attempt to deny service to legitimate users by overwhelming the target with activity. The most common method is to flood a server with network traffic from multiple sources (hence "distributed"). These attacks are often conducted through

[1] https://www.otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented

"botnets" – armies of compromised computers that are made up of victim machines that stretch across the globe and are controlled by "bot herders" or "bot masters."[2]

DDoS attacks have grown larger year over year and in 2014 some attacks reached 400 gigabits per second, a previously unimaginable volume of data. This is roughly equivalent to blasting a network every second with the data stored on more than 10 DVDs. In the past few years we have seen attacks go from the equivalent of a garden hose to a fire hose to the outflow pipes of the Hoover dam. Even the most prepared networks can buckle under that volume of data the first time it is directed at them, which is why even some of our biggest financial institutions initially suffered outages when they were victims of a DDoS campaign. In addition to increasing in volume, the attacks are getting more sophisticated and varying the methods used, which makes them harder to mitigate. In 2014, attackers used new techniques to amplify the strength of an attack which made it easier for even the "average" attack to reach levels of volume that were unthinkable just years before.[3]

According to a survey by Neustar, 60 percent of companies were impacted by a DDoS attack in 2013 and 87 percent were hit more than once.[4] The most affected sectors were the gaming, media, and software industries. The purpose of most attacks is to disrupt, not to destroy. Cybercriminals can rent DDoS attack services on the black market for as little as $5, allowing them to conduct a short, minutes-long DDoS attack against any chosen target (fig. 1).[5] If successful, even such a short attack is enough to garner attention – or to distract an organization's security team, as another recent use of DDoS attacks has been to provide cover for other, more sophisticated attacks. Organized crime groups have been known to launch DDoS attacks against banks to divert the attention and resources of the bank's security team while the main attack is launched, which can include draining customer accounts or stealing credit card information.



DDOS SERVICE

about

You have up to '3' targets choices:
- Game Servers
- Home-connections
- Websites
The power is more then mostly other peoples DDoS Service.
I dont have any detat on the power..
But I can guarantee that my service wont let you down.
I only accept paypal.

prices

✓	Game Server:	2$ every 30 minutes.
✓	Home Connection:	15$ each 24h/ 2$ every 2h
✓	Website	2$ every 30 minutes.

PM me
Or add me on skype:

Fig. 1. Example of a DDoS service for hire – this one is directed at online gamers.

[2] "Bots and Botnets – A Growing Threat," *Symantec,* http://us.norton.com/botnet/
[3] Symantec, *"Security Response: The Continued Rise of DDoS Attacks,"* October 21, 2014, Pg. 25.
[4] Neustar, *"2014, The Danger Deepens: Neustar Annual DDoS Attacks and Impact Report,"* June 2014, Pg. 3.
[5] Symantec, *"Security Response: The Continued Rise of DDoS Attacks,"* October 21, 2014, Pg. 12.

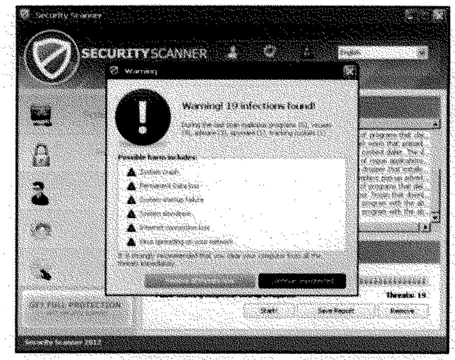
Targeted Attacks

Targeted attacks are another tool in the cybercriminal's tool box, and the attached graphic illustrates some common attack methods as well as the economics of cybercrime (see *Path of A Cybercriminal*, attached on page 12). Some attacks are directed at a company's servers and systems, where attackers search for unpatched vulnerabilities on websites or undefended connections to the internet. But most rely on social engineering, tricking people into clicking on a link, opening a file, or taking some other action that will allow an attacker to compromise their device. They can be targeted at almost any level, even at an entire sector of the economy or a group of similar organizations or companies. They also can target a particular company or a unit within the company (*e.g.*, research and development or finance) or even a specific person.

Most of the data breaches and other attacks that have been in the news were the result of a targeted attack, but the goal of the attacker can vary greatly. One constant is that after attackers select a target they will set out to gain access to the systems they want to compromise and once inside there are few limits on what they can do if the system is not well-protected. The malware used today is largely commoditized, and while we still see some that is custom-crafted, most of the attacks rely on attack kits that are sold on the cyber black market. But even these commodity attack kits are highly sophisticated and are designed to avoid detection – some even come with guarantees from the criminal seller that they will not be stopped by common security measures. This makes it all the more important – but also more challenging – to stay ahead of them.

Scams, Blackmail, and other Cyber Theft

Like most crime, cyber attacks are often financially motivated, and some of the most common (and most successful) involve getting victims to pay out money, whether through trickery or direct threats. One early and widely successful attack of this type was known as "scareware" (fig. 2). Scareware is a form of malware that will open a window on your device that claims your system is infected, and offer to "clean" it for a fee. Some forms of scareware open pop-ups falsely claiming to be from major security companies (including Symantec), and if a user clicks in the window they are taken to a fake website that can look very much like that of the real company. Of course, in most cases the only infection on your computer is the scareware itself. Victims who fall for the scam are lucky if they only lose the $20 or $30 "cost" for the fake software, but most are out much more as they typically provide credit card information to pay the scammer in the mistaken belief they are purchasing legitimate security software. Not only did they authorize a payment to the scammer, but they also provided financial information that could then be sold on the criminal underground. And by allowing the scammer to install the supposed cleaning software on their device, they give the criminal the ability to install additional malware and potentially steal more financial information or turn their system into a zombie soldier in a botnet.



Security Scanner

SECURITYSCANNER

Warning

Warning! 19 infections found!

During the last scan malicious programs (5), viruses (3), adware (3), spyware (2), tracking cookies (1)

Possible harm includes:

- System crash
- Permanent data loss
- System startup failure
- System slowdown
- Internet connection loss
- Virus spreading on your network

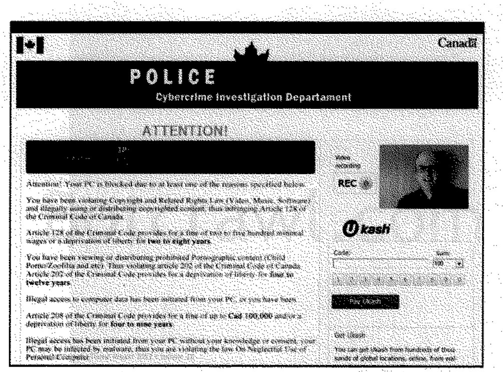
It is strongly recommended that you clear your computer from all the threats immediately.

Threats: 19

Fig. 2. An example of Scareware. The pop-ups proclaim that the victim's computer is infected, and often cannot be closed.

First widely seen in 2007, scareware began to diminish in 2011 after users became alerted to the scams and they became much less effective. Nevertheless, criminals have made millions from this type of scam.

Once scareware began to be less effective, criminals turned to "ransomware," which has grown significantly since 2012. Ransomware is another type of deception where the malware locks the victim's device and displays a screen that purports to be from a law enforcement entity local to the user. The lock screen states that there is illegal content on the computer – everything from pirated movies to child pornography – and instructs the victim to pay a "fine" for their "crime" (fig. 3). The criminals claim that the victim's device will be unlocked once the "fine" is paid, but in reality the device frequently remains locked. Both of these types of attacks can be removed from your computer and we offer instructions and free tools on our Norton.com website to assist victims in doing so. Unfortunately, some of the more sophisticated variants can require some expertise to remediate.



Canada

POLICE

Cybercrime Investigation Departament

ATTENTION!

[redacted]

Attention! Your PC is blocked due to at least one of the reasons specified below.

You have been violating Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing Article 128 of the Criminal Code of Canada.

Article 128 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for **two to eight years**.

You have been viewing or distributing prohibited Pornographic content (Child Porno/Zoofilia and etc). Thus violating article 202 of the Criminal Code of Canada. Article 202 of the Criminal Code provides for a deprivation of liberty for **four to twelve years**.

Illegal access to computer data has been initiated from your PC, or you have been

Article 208 of the Criminal Code provides for a fine of up to **Cad 100,000** and/or a deprivation of liberty for **four to nine years**.

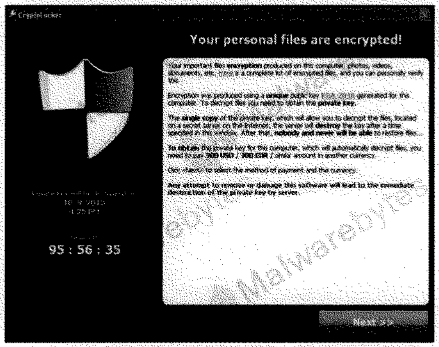
Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law On Neglectful Use of Personal Computer

Get Ukash

You can get Ukash from hundreds of thousands of global locations, online, from wal

Fig. 3. This ransomware targeted victims in Canada; victims in other countries would see logos of law enforcement local to them._ It used built-in webcams to take a victim's picture to further frighten them.

Criminals have now moved beyond even ransomware and are using a more insidious and harmful form of malware known as "ransomcrypt." While scareware and ransomware are more classic confidence schemes, ransomcrypt is straight-up blackmail: pay a ransom or your computer will be erased (fig. 4). And unlike scareware and ransomware, there is often no easy way to get rid of it – the criminals use high-grade encryption technology to scramble the victim's computer, and only they have the key to unlock it. Unless the system is backed up, the victim faces the difficult choice of paying the criminals or losing all the data, and earlier this year a police department in Maine paid a ransom in order to regain control of its data.[6] The police chief said "[w]e needed our programs to get back online."[7]



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Fig. 4. This is a screenshot of Cryptolocker, a sophisticated piece of ransomcrypt that was disrupted in summer 2014 by an international takedown effort, in which Symantec participated.

This is not meant to suggest that the criminals are unstoppable; in fact, in June 2014 we were part of a team that helped take down Cryptolocker, a prevalent form of ransomcrypt. Symantec assisted the FBI and several other international law enforcement agencies to mount a major operation during which authorities seized a large portion of the infrastructure that had been used by the cybercriminals. As a result of Symantec's research into the threat, we were able to provide technical insights into their operation and impact. Since the operation, the Cryptolocker infection rate has dropped to near zero. But other forms are still out there, and the fight goes on.

Threats to Critical Infrastructure

Critical infrastructure such as the power grid, water systems, and mass transit are also at risk. As more of these devices become connected and are controlled remotely, attackers have more opportunities to try to exploit them. In June 2014, we notified and provided detailed Indicators of Compromise (IoC) to more than 40 national computer security incident response teams around the world about a new threat

[6] Stephanie Mlot, "Maine Police Pay Ransomware Demand in Bitcoin," *PCmag*, April 14, 2015, http://www.pcmag.com/article2/0,2817,2481356,00.asp

[7] *Id.*

we named *DragonFly*.[8] This was an ongoing cyber espionage campaign against a range of targets, mainly in the energy sector, which gave attackers control over computers that they could have used to damage or destroy critical machinery and disrupt energy supplies in affected countries. Among the targets of *Dragonfly* were energy grid operators, electricity generation firms, petroleum pipeline operators, and industrial equipment providers – the majority of which were located in the U.S., Spain, France, Italy, Germany, Turkey, and Poland. Quick and detailed notification was critical in mitigating the threat.

This was not the first campaign targeted at the energy sector. In 2012, cyber attackers mounted a campaign against Saudi Arabia's national oil firm Saudi Aramco, which destroyed approximately 30,000 computers and took its network off line for days. The infected computers were rendered unusable and displayed the image of a burning American flag. Though operations were not impacted, there was speculation in the press that oil production was the ultimate target. Shortly after the Saudi Aramco attack, a Qatari producer of liquefied natural gas, RasGas, suffered a similar attack which damaged its networks and took down its website. Other sectors have seen attacks too. In the manufacturing sector, late last year the German Government disclosed that a cyber attack on a steel plant had resulted in the failure of multiple components and, according to one report, "massive physical damage."[9]

In the U.S. we have yet to see major destructive attacks on critical infrastructure. However, there have been widespread reports that foreign actors have sought to gain a foothold on the networks of U.S. critical infrastructure providers.[10] And we have seen the actual compromise of one water treatment facility in South Houston, Texas (fig. 5), though the attacker did not alter any controls or settings and claimed to be trying to bring attention to the vulnerabilities that exist in critical infrastructure. This particular facility was not following security best practices and was still using default passwords that were widely known. There are undoubtedly many other critical systems that are similarly exposed.

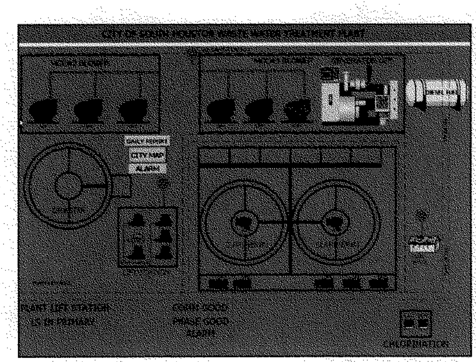


Fig. 5. Screenshot a hacker posted of the graphical user interface of the South Houston Waste Water Treatment Plant. He accessed this through use of an unchanged default user name and password.

[8] Symantec, *"Security Response: Dragonfly: Western Energy Companies under Sabotage,"* June 30, 2014. http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

[9] SANS Industrial Control Systems (ICS), *"German Steel Mill Cyber Attack,"* December 30, 2014, Pg.1.

[10] Pierluigi Paganini, "The US energy industry is constantly under cyber attacks," *Security* Affairs, November 14, 2014 http://securityaffairs.co/wordpress/30328/cyber-crime/cyber-attacks-energy-industry.html

Methods Attackers Use to Compromise Systems - Inside the Attacker's Tool Kit

All of the attacks outlined above started with a common factor – a compromised device. From this one computer, attackers often are able to move within a system until they achieve their ultimate goal. But the threshold question is how do they get that foothold – how do they make that initial compromise that allows them to infiltrate a system?

We frequently hear about the sophistication of various attackers and about "Advance Persistent Threats" or "APTs," but the discussion of cyber attacks – and of cyber defense – often ignores the psychology of the exploit. Most attacks rely on social engineering – in the simplest of terms, trying to trick people into doing something that they would never do if fully cognizant of their actions. For this reason, we often say that the most successful attacks are as much psychology as they are technology.

Spear phishing, or customized, targeted emails containing malware, is the most common form of attack. Attackers harvest publicly available information and use it to craft an email designed to dupe a specific victim or group of victims. The goal is to get victims to open a document or click on a link to a website that will then try to infect their computers. While good security will stop most of these attacks – which often seek to exploit older, known vulnerabilities – many organizations and individuals do not have up-to-date security or properly patched operating systems or software. And many of these attacks are extremely well-crafted; in the case of one major attack, the spear phishing email was so convincing that even though the victim's system automatically routed it to junk mail, he retrieved it and opened it – and exposed his company to a major breach.

Social media is an increasingly valuable tool for cyber criminals in two different ways. First, it is particularly effective in direct attacks, as people tend to trust links and postings that appear to come from a friend's social media feed and rarely stop to wonder if that feed may have been compromised or spoofed. Thus, attackers target social media accounts and then use them to "like" or otherwise promote a posting that contains a malicious link. But social media is also widely used to conduct reconnaissance for spear phishing or other highly targeted attacks as it often provides just the kind of personal details that a skilled attacker can use to get a victim to let his or her guard down. The old cliché is true when it comes to cyber attacks: we have to get it right 100 percent of the time while the attacker only has to do so once.

Beginning in 2012, we saw the rapid growth of a new type of targeted web-based attack, known as a "watering hole" attack. Like the lion in the wild who stalks a watering hole for unsuspecting prey, cybercriminals have become adept at lying in wait on legitimate websites and using them to try to infect visitors' computers. They do so by compromising legitimate websites that their victims are likely to visit and modifying them so that they will surreptitiously try to infect visitors. For example, one attacker targeted mobile application developers by compromising a site that was popular with them. In another case, we saw employees from 500 different companies in the same industry visit one compromised site in just 24 hours, each running the risk of infection.[11] Cybercriminals gained control of these websites through many of the same tactics described above – spear phishing and other social engineering attacks on the site managers, developers, or owners. Many of these websites were compromised through known attack vectors, meaning that good security practices could have prevented them from being compromised.

[11] Symantec, *"Internet Security Threat Report, Volume XVIII,"* April 16, 2013, Pg. 21.

We are also seeing an increasing number of "second generation" compromises – where attackers use personal information that was previously stolen or harvested off the internet to access data or even establish new online accounts. Twenty or more years ago criminals would use stolen social security numbers or other information to open fraudulent credit cards; today that same information can be used to verify – fraudulently – a person's identity to access information held by companies or governments. As the personal information of more people is stolen and sometimes coupled with other information posted on social media or elsewhere, systems that use Knowledge Based Authentication (KBA) are increasingly under attack. This is particularly true with static KBA – which uses fixed questions and information provided by a user, and is often drawn from a set of queries that have become well-known to attackers.

Dynamic KBA, which connects some identifying information with data drawn from a wider data-set that is not supplied by a user, provides a higher level of security. However, it is still most effective when paired with additional authentication, which can include behavioral analytics or additional factors such as a text message, a smart card, biometrics, or a token or mobile application with a changing numeric password. To make it even more secure, some systems require an out-of-band communication such as a phone call or even standard mail before allowing an account to be opened. Of course, additional security measures can also slow the verification process, which can frustrate users.

The information that is stolen through these types of attacks can be used for immediate gain, though it is often used in more sophisticated criminal scams such as tax fraud. But the lesson is plain: no matter how innocuous a piece of data may seem to you, criminals are constantly devising new ways to monetize it once it is stolen.

Security Measures

Cybersecurity is about managing risk, whether at the individual or the organizational level. Assessing one's risk and developing a plan is essential. For the individual, the Federal Trade Commission's website is an excellent starting point for doing so.[12] The website provides educational resources for how to better protect your identity and privacy online as well as helpful tools to help you report and recover if your personal information is ever stolen. Similarly, we offer many tools and reference materials on our Norton.com website.

For organizations of any size, the National Institute of Standards and Technology's Cyber Security Framework[13], developed by industry and government in 2014 and in which Symantec was an active contributor, provides a solid structure for risk management. It lays out five core cybersecurity functions (Identify, Protect, Detect, Respond and Recover) that all organizations can use to plan for managing cyber events and protecting against data breaches, as well as useful references to international standards. As detailed below, good security starts with the basics and includes measures specific to one's needs.

- *Basic Security Steps*

Poor basic computer hygiene practices are a major cause of breaches. While good practices will stop most attacks – which often exploit known vulnerabilities – too many organizations do not keep their

[12] http://www.consumer.ftc.gov/topics/privacy-identity
[13] http://www.nist.gov/cyberframework/

systems updated. Indeed, security starts with the basics. Though criminals' tactics are continually evolving, good cyber hygiene is still the simplest and most cost-effective first step. Strong passwords remain the foundation of good security – on home and work devices, email, social media accounts, or whatever you use to communicate (or really anything you log into). And these passwords must be different, because using a single password means that a breach of one account exposes all of your accounts. Using two factor authentication significantly increases the security of a login.

Patch management is also vital. Individuals and organizations should not delay installing patches, or software or hardware updates, because the same patch that closes a vulnerability can be a roadmap for a criminal to exploit and compromise any unpatched devices. The reality is that a large percentage of computers around the world, including some in large organizations, do not get patched regularly, and cybercriminals count on this. While so-called "zero day exploits" – previously unknown critical vulnerabilities – get the most press, it is older, unpatched vulnerabilities that cause most systems to get compromised.

Additionally, we all need to exercise caution on social media. Cybercriminals target the places where we "live and play" online in order to get at sensitive personal data, and are increasingly using social media to launch attacks. It is particularly effective in direct attacks, as people tend to trust things that appear to come from a friend's social media feed. But social media is also widely used to conduct reconnaissance for spear phishing or other targeted attacks. Exercising some care in how we use social media can make the attacker's job harder.

- *Modern Security Software*

Poor or insufficiently deployed security can also lead to a breach, and a modern security suite that is being fully utilized is also essential. While most people still commonly refer to security software as "anti-virus" or AV, advanced security protection is much more than that. In the past, the same piece of malware would be delivered to thousands or even millions of computers. Today, cybercriminals can take the same malware and create unlimited unique variants that can slip past basic AV software. If all your security software does is check for signatures (or digital fingerprints) of known malware, you are by definition not protected against even moderately sophisticated attacks. Put differently, a check-the-box security program that only includes installation of basic AV software may give you piece of mind – but that is about all it will give you.

Modern security software does much more than look for known malware: it monitors your system, watching for unusual internet traffic, activity, or system processes that could be indicative of malicious activity. At Symantec we also use what we call *Insight* and *SONAR*, which are reputation-based and behavior-based heuristic security technologies. Insight is a reputation-based technology that uses our Global Intelligence Network to put files in context, using their age, frequency, location and other characteristics to expose emerging threats that might otherwise be missed. If a computer is trying to execute a file that we have never seen anywhere in the world and that comes from an unknown source, there is a high probability that it is malicious – and Insight will either warn the user or block it. SONAR is behavior-based protection that uses proactive local monitoring to identify and block suspicious processes on computers.

- *Tailoring Security to the Device*

Security should also be specific to the device being protected. For example, modern Point of Sale (PoS) systems, which were linked to a number of major data breaches, are at their core just computers running mainstream operating systems. Because a user on such a device typically does not browse the web, send emails, or open shared drives, the functionally of the machine and the files that actually need to be on it are limited. This allows businesses to reduce the attack surface by locking down the system and using application control tools, as well as controlling which devices and applications are allowed to access the network. Doing so can render many strains of malware useless because they would not be allowed to run on the devices. In addition, payment card system infrastructure is highly complex and threats can be introduced at any number of points within the system. Last year we released a report, *Attacks on Point of Sale Systems*, that provides an overview of the methods that attackers may use to gain entry into a system.[14] It also describes the steps that retailers and other organizations can use to protect PoS systems and mitigate the risk of an attack.

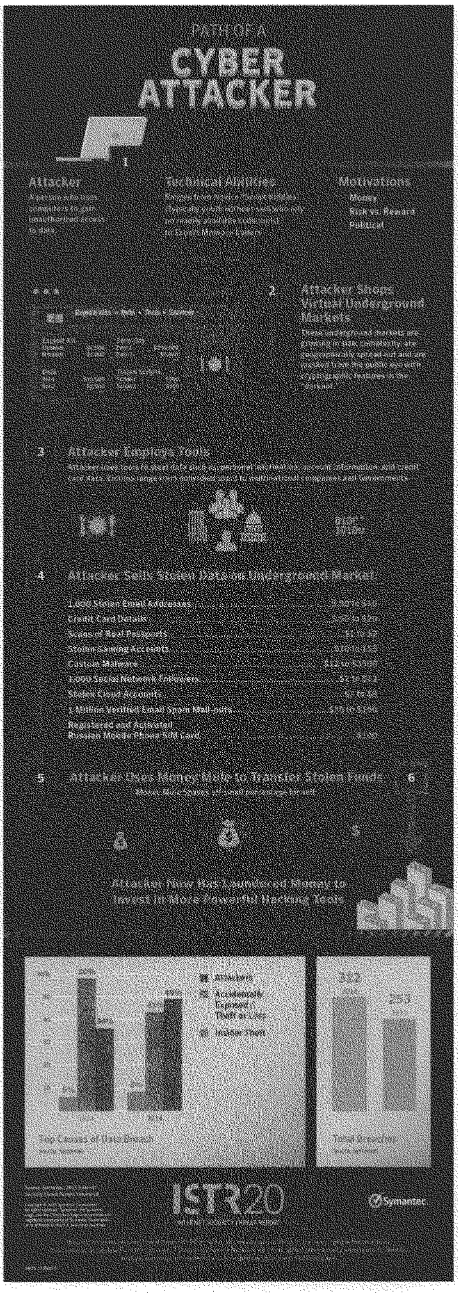
- *Encrypting and Monitoring Data*

Encryption also is key to protecting your most valuable data. Even the best security will not stop a determined attacker, and encrypting your sensitive data provides defense in breadth, or across many platforms. Encryption ensures that any data stolen will be useless to virtually all cybercriminals. The bottom line in computer security is no different from physical security – nothing is perfect. We can make it hard, indeed very hard, for an attacker, but if well-resourced and persistent criminals want to compromise a particular company or site, with time they are probably going to find a way to do it. Good security means not just doing the utmost to keep them out, but also to recognize that you must take steps to limit any damage they can do should they get in. Data loss prevention (DLP) tools are also important in keeping your most valuable data safe on your system. The latest DLP technology allows the user to monitor, protect and manage confidential data wherever it is stored and used – across endpoints, mobile devices, networks, and storage systems. It can help stop the theft of sensitive data by alerting the system manager before the data is exfiltrated.

Conclusion

Citizens are increasingly aware of the cyber risk and the need to take precautions to secure their data and protect their privacy. While we cannot prevent every cyber attack or every data breach, applying cybersecurity best practices and using risk management principles to protect data appropriately can significantly reduce the attack surface and the impacts we see today. Every time someone patches their a computer or mobile device, changes a password, or utilizes a modern security suite, he or she is making it more difficult for cybercriminals to operate. Like any other illicit activity, cybercrime will never be completely eliminated, but it can be fought. For example, the criminals did not stop using the scareware described above because they wanted to – they quit when it stopped working. At Symantec, we are committed to improving online security and we look forward to continuing to work with government and industry on ways to do so. Thank you again for the opportunity to testify, and I will be happy to answer any questions you may have.

[14] *Special Report on Attacks on Point of Sale Systems*, Symantec Security Response (February 2014). http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/attacks_on_point_of_sale_systems.pdf



PATH OF A

CYBER ATTACKER

1

Attacker
A person who uses computers to gain unauthorized access to data.

Technical Abilities
Ranges from Novice "Script Kiddies" (Typically youth without skill who rely on readily available code tools) to Expert Malware Coders

Motivations
- Money
- Risk vs. Reward
- Political

2 **Attacker Shops Virtual Underground Markets**

These underground markets are growing in size, complexity, are geographically spread out and are masked from the public eye with cryptographic features in the "darknet".

3 **Attacker Employs Tools**

Attacker uses tools to steal data such as: personal information, account information, and credit card data. Victims range from individual users to multinational companies and Governments.

4 **Attacker Sells Stolen Data on Underground Market:**

1,000 Stolen Email Addresses	$.50 to $10
Credit Card Details	$.50 to $20
Scans of Real Passports	$1 to $2
Stolen Gaming Accounts	$10 to $15
Custom Malware	$12 to $3500
1,000 Social Network Followers	$2 to $12
Stolen Cloud Accounts	$7 to $8
1 Million Verified Email Spam Mail-outs	$70 to $150
Registered and Activated Russian Mobile Phone SIM Card	$100

5 **Attacker Uses Money Mule to Transfer Stolen Funds**

Money Mule Shaves off small percentage for self

6

Attacker Now Has Laundered Money to Invest in More Powerful Hacking Tools

Top Causes of Data Breach
Source: Symantec

Total Breaches
Source: Symantec

ISTR20
INTERNET SECURITY THREAT REPORT

Symantec

WRITTEN TESTIMONY OF
JOHN A. KOSKINEN
COMMISSIONER
INTERNAL REVENUE SERVICE
BEFORE THE
SENATE COMMITTEE ON HOMELAND SECURITY & GOVERNMENTAL AFFAIRS
ON UNAUTHORIZED ATTEMPTS TO ACCESS TAXPAYER DATA
JUNE 2, 2015

Chairman Johnson, Ranking Member Carper and Members of the Committee, thank you for the opportunity to appear before you today to provide information on the recent unauthorized attempts to obtain taxpayer data through the IRS's "Get Transcript" online application.

While we are continuing our in-depth analysis of what happened, the analysis thus far has found that the unauthorized attempts to request information from the Get Transcript application were complex and sophisticated in nature. These attempts were made using taxpayers' personal information already obtained from sources outside the IRS – meaning the parties making the attempts had enough information to clear the Get Transcript application's multi-step authentication process.

For now, our biggest concern is for the affected taxpayers, to make sure they are protected against fraud in the future. We recognize the severity of the situation for these taxpayers, and we are doing everything we can to help them.

Securing our systems and protecting taxpayers' information is a top priority for the IRS. Even with our constrained resources as a result of cuts to our budget totaling $1.2 billion since 2010, we continue to devote significant time and attention to this challenge. At the same time, it is clear that criminals have been able to gather increasing amounts of personal data as the result of data breaches at sources outside the IRS, which makes protecting taxpayers increasingly challenging and difficult.

The problem of personal data being stolen from sources outside the IRS to perpetrate tax refund fraud exploded from 2010 to 2012, and for a time overwhelmed law enforcement and the IRS. Since then, we have been making steady progress, both in terms of protecting against fraudulent refund claims and prosecuting those who engage in this crime. Over the past few years, almost 2,000 individuals were convicted in connection with refund fraud related to identity theft. The average prison sentence for identity theft-related tax refund fraud grew to 43 months in Fiscal Year (FY) 2014 from 38 months in FY 2013, with the longest sentence being 27 years.

Additionally, as our processing filters have improved, we have also been able to stop more suspicious returns at the door, rather than accepting them for processing. This past filing season, our fraud filters stopped almost 3 million fraudulent returns before processing them, an increase of over 700,000 from the year before. But, even though we have been effective at stopping individuals perpetrating these crimes, we find that we are dealing more and more with organized crime syndicates here and around the world.

At the same time, over the last several years, the IRS has been working to meet taxpayers' increasing demand for self-service and electronic service options by providing them with more web-based tools, to make their interactions with us simpler and easier. As part of that effort, we launched the Get Transcript online application in January 2014. Get Transcript allows taxpayers to view and print a copy of their prior-year tax information, also known as a transcript, in a matter of minutes. Prior to the introduction of this online tool, taxpayers had to wait five to seven days after placing an order by phone or by mail to receive a paper transcript by mail. Taxpayers use tax transcript information for a variety of financial activities, such as verifying income when applying for a mortgage or student loan.

To access Get Transcript, taxpayers must go through a multi-step authentication process to prove their identity, consistent with many organizations in the financial services industry. They must first submit personal information such as their Social Security number (SSN), date of birth, tax filing status, and home address, as well as an email address. The taxpayer then receives an email from the Get Transcript system containing a confirmation code that they enter to access the application and request a transcript. Before the request is processed, the taxpayer must respond to several "out-of-wallet" questions – a customer authentication method that is standard within the financial services industry. The questions are designed to elicit information that only the taxpayer would normally know, such as the amount of their monthly mortgage or car payment.

During the 2015 filing season, taxpayers used the Get Transcript application to successfully obtain approximately 23 million copies of their recently filed tax information. If this application had not existed and these taxpayers had to call or write us to order a transcript, it would have stretched our limited resources even further. That is important to note, given our limitations during the past filing season. We would have been much less efficient in providing taxpayer service, not to mention the additional burden placed on taxpayers.

During the middle of May, our cybersecurity team noticed unusual activity on the Get Transcript application. At the time, our team thought this might be a "denial of service" attack, where hackers try to disrupt a website's normal functioning. Our teams worked aggressively to look deeper into the situation during the following days, and ultimately uncovered questionable attempts to access the Get Transcript application.

As a result, the IRS shut down the Get Transcript application on May 21. The application will remain disabled until the IRS makes modifications and further strengthens security for the application. It should be noted that the third parties who made these unauthorized attempts to obtain tax account information did not attempt to gain access to the main IRS computer system that handles tax filing submissions. The main IRS computer system remains secure, as do other online IRS applications such as "Where's My Refund?" Unlike Get Transcript, the other online applications do not allow taxpayers to access their personal tax data.

As they continued to investigate, our team determined that a total of approximately 200,000 suspicious attempts to gain access to taxpayer information on the Get Transcript application had been made between mid-February and mid-May. About 100,000 of the attempts were unsuccessful, with the parties making these attempts unable to work their way through the protections in place.

But we know that the other 100,000 or so attempts to request information from the Get Transcript application between mid-February and mid-May were successful. We are analyzing what, if anything, was done with the personal information of these taxpayers obtained using the Get Transcript application, and have discovered the following:

- About 35,000 taxpayers had already filed their 2014 income tax returns before the unauthorized attempts at access. This means that these taxpayers' 2014 returns and refund claims were not affected by this fraudulent activity, because any fraudulent return subsequently filed in their names would be automatically rejected by our systems;
- For another 33,000, there is no record of any return having been filed in 2015. This could be the case for a number of reasons. For example, the SSNs associated with these individuals may belong to those who have no obligation to file, such as children, or anyone below the tax filing threshold;
- Unsuccessful attempts were made to file approximately 23,500 returns. These 23,500 returns were flagged by our fraud filters and stopped by our processing systems before refunds were issued; and
- Since this activity occurred, about 13,000 suspect returns were filed for tax year 2014 for which the IRS issued refunds. Refunds issued for these 13,000 suspect returns totaled about $39 million, and the average refund was approximately $3,000 per return. We are still determining how many of these returns were filed by the actual taxpayers and which were filed using stolen identities. We will work with any of these affected taxpayers who had fraudulent returns filed in their name.

As I mentioned at the outset, our analysis thus far has found that the unauthorized attempts to access information using the Get Transcript application were complex and sophisticated in nature. These attempts were made using personal information already obtained from sources outside the IRS – meaning the parties making the attempts had enough information to clear the Get Transcript application's multi-step authentication process, including answers to the out-of-wallet questions.

We believe it is possible that some of the attempts to access tax transcripts were made with an eye toward using the information to file fraudulent tax returns next year. For example, any prior-year return information criminals obtain would help them more easily craft seemingly authentic returns, making it more difficult for our filters to detect the fraudulent nature of the returns.

As noted above, since we have already disabled Get Transcript, our biggest concern right now is for the affected taxpayers, to make sure they are protected against fraud in the future. We recognize the severity of the situation for these taxpayers, and have taken a number of immediate steps to assist the affected taxpayers in protecting their data against fraud that might be perpetrated against them. First, we have placed an identifier on the accounts of the roughly 200,000 affected taxpayers on our core tax account system to prevent someone else from filing a tax return in their name – both now and in future years.

Second, we are in the process of writing to all 200,000 taxpayers to let them know that third parties appear to have gained access from outside the IRS to personal information such as their SSNs, in an attempt to obtain their tax information from the IRS. Although half of this group did not actually have their transcript accessed because those who were trying to gain this information failed the authentication tests, the IRS believes it is important to make these taxpayers aware that someone else has their personal data. We want them to be able to take steps to safeguard their data.

Letters have already been sent to all of the approximately 100,000 taxpayers whose tax information was successfully obtained by unauthorized third parties. We are offering credit monitoring, at our expense, to this group of taxpayers. We strongly encourage people who receive this letter to take advantage of this offer. We are also giving them the opportunity to provide us with the authentication documentation necessary to obtain an Identity Protection Personal Identification Number (IP PIN). This will further safeguard their IRS accounts and help them avoid any problems filing returns in future years.

As further analysis is done, we may uncover evidence that personal information of others, such as spouses and dependents of the taxpayers already identified, was also compromised, and we will take similar steps to protect those individuals.

More broadly, the IRS continues to work to help taxpayers who have been victims of identity theft. For example, for the 2015 filing season, the IRS has issued IP PINs to 1.5 million taxpayers previously identified by the IRS as victims of identity theft. Also during this period, the IRS notified another 1.7 million taxpayers that they were eligible to visit IRS.gov and opt in to the IP PIN program. Meanwhile, taxpayers living in Florida, Georgia and Washington, D.C. – three areas where there have been particularly high concentrations of identity-theft related refund fraud – are eligible to participate in a pilot where they can receive an IP PIN upon request, regardless of whether the IRS has identified them as a victim of identity theft.

In terms of our investigative work on identity theft, it is important to note that our Criminal Investigation (CI) division has seen an increase in identity theft crime being perpetrated by organized crime syndicates. The IRS is working closely with law enforcement agencies in the U.S. and around the world to prosecute these criminals and protect taxpayers. But the fact remains that these cyber criminals are increasingly sophisticated enemies, with access to substantial volumes of data on millions of people.

For that reason, we recently held a sit-down meeting with the leaders of the tax software and payroll industries and state tax administrators, and agreed to build on our cooperative efforts of the past and find new ways to leverage this public-private partnership to help battle identity theft. The working groups that were formed out of this meeting have continued to meet, and later this month we expect to announce an agreement on short-term solutions to help better protect personal information in the upcoming tax filing season, and to continue to work on longer-term efforts to protect the integrity of the nation's tax system.

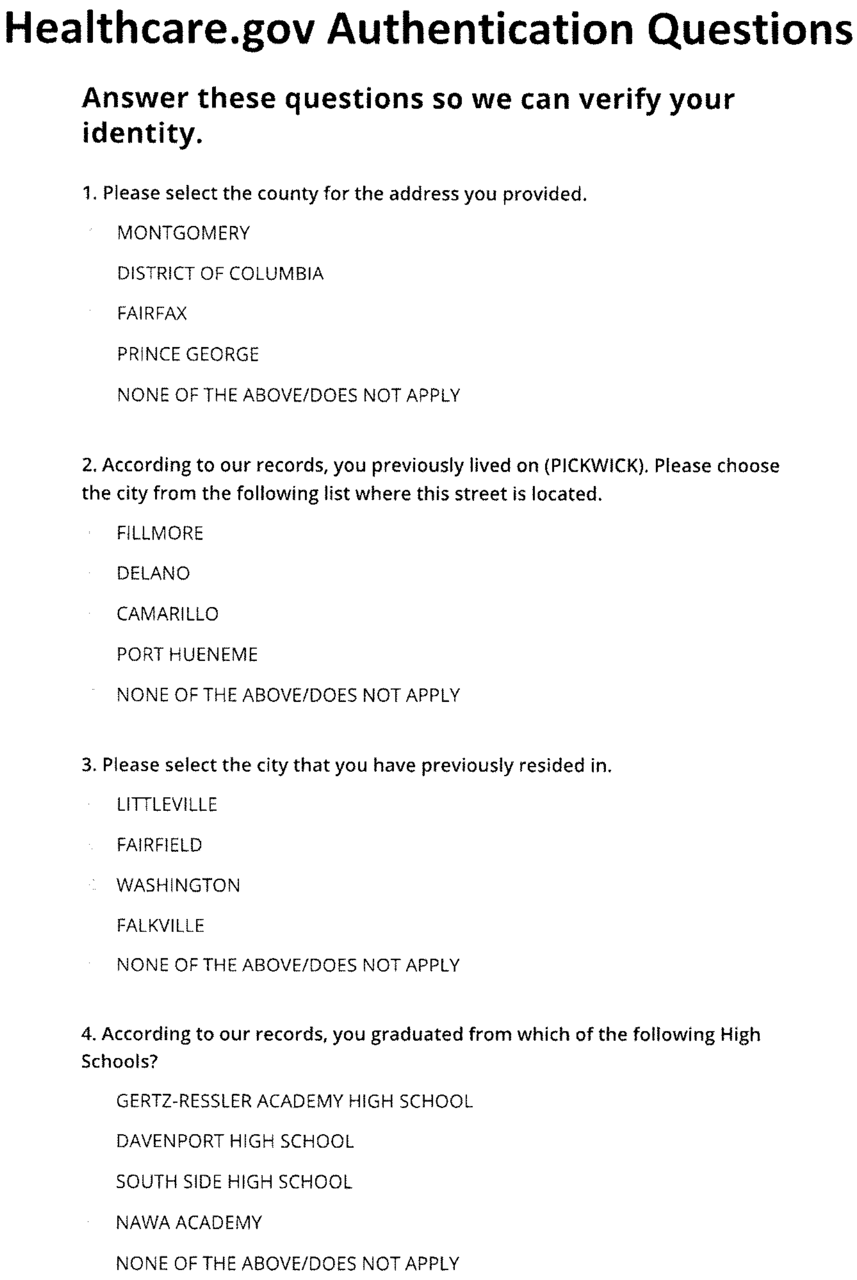
One of the three working groups formed out of this meeting focuses on authentication. As criminals obtain more personal information, authentication protocols need to become more sophisticated, moving beyond information that used to be known only to individuals but now, in many cases, is readily available to criminal organizations from various sources. We must balance the strongest possible authentication processes with the ability of taxpayers to legitimately access their data and use IRS services online. The challenge will always be to keep up with, if not get ahead of, our enemies in this area.

Congress has an important role to play here. Congress can help by approving the President's FY 2016 Budget request, which includes $101 million specifically devoted to identity theft and refund fraud, plus $188 million for critical information technology infrastructure. Along with providing adequate funding, lawmakers can help the IRS in the fight against refund fraud and identity theft by passing several important legislative proposals in the President's FY 2016 Budget proposal. A key item on this list is a proposal to accelerate information return filing dates.

Under current law, most information returns, including Forms 1099 and 1098, must be filed with the IRS by February 28 of the year following the year for which the information is being reported, while Form W-2 must be filed with the Social Security Administration (SSA) by the last day of February. The due date for filing information returns with the IRS or SSA is generally extended until March 31 if the returns are filed electronically. The Budget proposal would require these information returns to be filed when copies of this information are provided to the taxpayers, generally by January 31 of the year following the year for which the information is being reported, which would assist the IRS in identifying fraudulent returns and reduce refund fraud related to identity theft.

There are a number of other legislative proposals in the Administration's FY 2016 Budget that would also assist the IRS in its efforts to combat identity theft, including: giving Treasury and the IRS authority to require or permit employers to mask a portion of an employee's SSN on W-2s, which would make it more difficult for identity thieves to steal SSNs; adding tax-related offenses to the list of crimes in the Aggravated Identity Theft Statute, which would subject criminals convicted of tax-related identity theft crimes to longer sentences than those that apply under current law; and adding a $5,000 civil penalty to the Internal Revenue Code for tax-related identity theft cases, to provide an additional enforcement tool that could be used in conjunction with criminal prosecutions.

Chairman Johnson, Ranking Member Carper and Members of the Committee, thank you again for the opportunity to provide information on the recent unauthorized attempts to obtain taxpayer data through the IRS' Get Transcript online application. This concludes my statement, and I would be happy to take your questions.



Healthcare.gov Authentication Questions

Answer these questions so we can verify your identity.

1. Please select the county for the address you provided.

MONTGOMERY

DISTRICT OF COLUMBIA

FAIRFAX

PRINCE GEORGE

NONE OF THE ABOVE/DOES NOT APPLY

2. According to our records, you previously lived on (PICKWICK). Please choose the city from the following list where this street is located.

FILLMORE

DELANO

CAMARILLO

PORT HUENEME

NONE OF THE ABOVE/DOES NOT APPLY

3. Please select the city that you have previously resided in.

LITTLEVILLE

FAIRFIELD

WASHINGTON

FALKVILLE

NONE OF THE ABOVE/DOES NOT APPLY

4. According to our records, you graduated from which of the following High Schools?

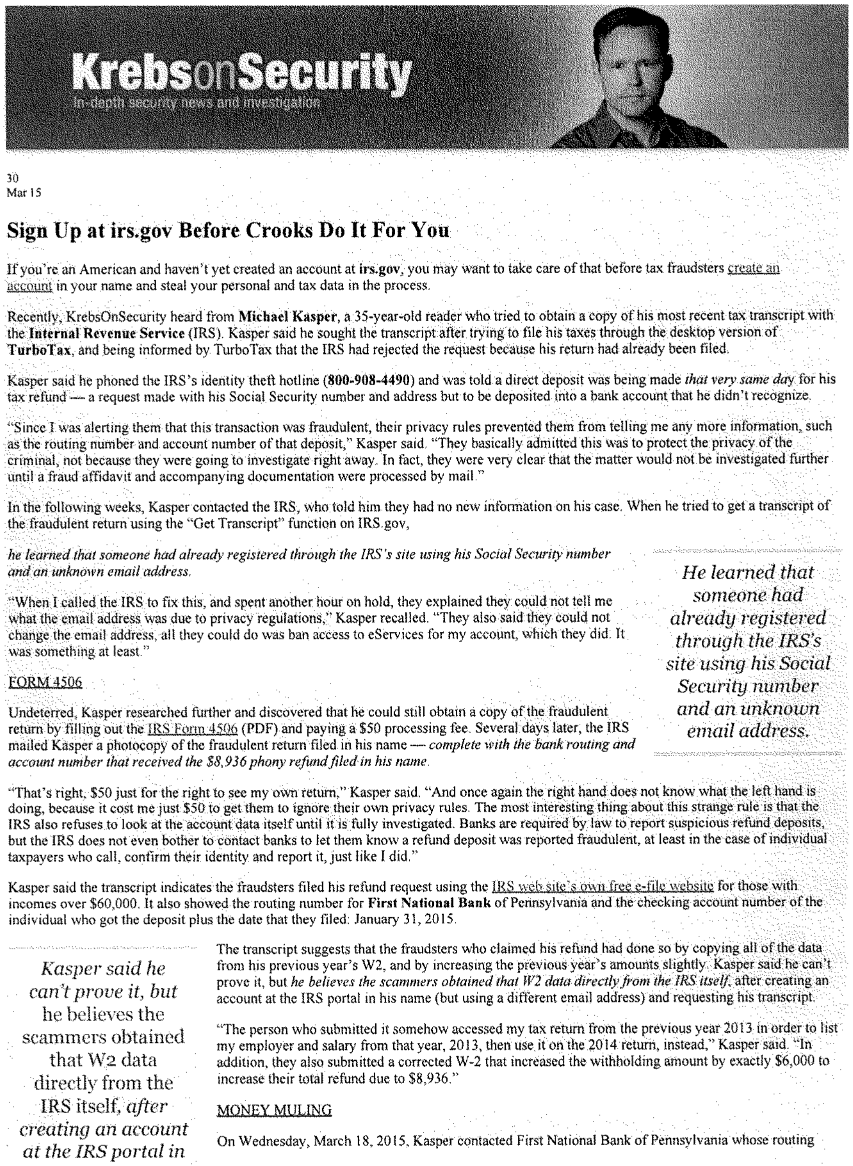
GERTZ-RESSLER ACADEMY HIGH SCHOOL

DAVENPORT HIGH SCHOOL

SOUTH SIDE HIGH SCHOOL

NAWA ACADEMY

NONE OF THE ABOVE/DOES NOT APPLY



KrebsonSecurity
In-depth security news and investigation

30
Mar 15

Sign Up at irs.gov Before Crooks Do It For You

If you're an American and haven't yet created an account at **irs.gov**, you may want to take care of that before tax fraudsters create an account in your name and steal your personal and tax data in the process.

Recently, KrebsOnSecurity heard from **Michael Kasper**, a 35-year-old reader who tried to obtain a copy of his most recent tax transcript with the **Internal Revenue Service** (IRS). Kasper said he sought the transcript after trying to file his taxes through the desktop version of **TurboTax**, and being informed by TurboTax that the IRS had rejected the request because his return had already been filed.

Kasper said he phoned the IRS's identity theft hotline (**800-908-4490**) and was told a direct deposit was being made *that very same day* for his tax refund — a request made with his Social Security number and address but to be deposited into a bank account that he didn't recognize.

"Since I was alerting them that this transaction was fraudulent, their privacy rules prevented them from telling me any more information, such as the routing number and account number of that deposit," Kasper said. "They basically admitted this was to protect the privacy of the criminal, not because they were going to investigate right away. In fact, they were very clear that the matter would not be investigated further until a fraud affidavit and accompanying documentation were processed by mail."

In the following weeks, Kasper contacted the IRS, who told him they had no new information on his case. When he tried to get a transcript of the fraudulent return using the "Get Transcript" function on IRS.gov,

he learned that someone had already registered through the IRS's site using his Social Security number and an unknown email address.

"When I called the IRS to fix this, and spent another hour on hold, they explained they could not tell me what the email address was due to privacy regulations," Kasper recalled. "They also said they could not change the email address, all they could do was ban access to eServices for my account, which they did. It was something at least."

FORM 4506

Undeterred, Kasper researched further and discovered that he could still obtain a copy of the fraudulent return by filling out the IRS Form 4506 (PDF) and paying a $50 processing fee. Several days later, the IRS mailed Kasper a photocopy of the fraudulent return filed in his name — *complete with the bank routing and account number that received the $8,936 phony refund filed in his name.*

He learned that someone had already registered through the IRS's site using his Social Security number and an unknown email address.

"That's right, $50 just for the right to see my own return," Kasper said. "And once again the right hand does not know what the left hand is doing, because it cost me just $50 to get them to ignore their own privacy rules. The most interesting thing about this strange rule is that the IRS also refuses to look at the account data itself until it is fully investigated. Banks are required by law to report suspicious refund deposits, but the IRS does not even bother to contact banks to let them know a refund deposit was reported fraudulent, at least in the case of individual taxpayers who call, confirm their identity and report it, just like I did."

Kasper said the transcript indicates the fraudsters filed his refund request using the IRS web site's own free e-file website for those with incomes over $60,000. It also showed the routing number for **First National Bank** of Pennsylvania and the checking account number of the individual who got the deposit plus the date that they filed: January 31, 2015.

Kasper said he can't prove it, but he believes the scammers obtained that W2 data directly from the IRS itself, *after creating an account at the IRS portal in*

The transcript suggests that the fraudsters who claimed his refund had done so by copying all of the data from his previous year's W2, and by increasing the previous year's amounts slightly. Kasper said he can't prove it, but *he believes the scammers obtained that W2 data directly from the IRS itself,* after creating an account at the IRS portal in his name (but using a different email address) and requesting his transcript.

"The person who submitted it somehow accessed my tax return from the previous year 2013 in order to list my employer and salary from that year, 2013, then use it on the 2014 return, instead," Kasper said. "In addition, they also submitted a corrected W-2 that increased the withholding amount by exactly $6,000 to increase their total refund due to $8,936."

MONEY MULING

On Wednesday, March 18, 2015, Kasper contacted First National Bank of Pennsylvania whose routing number was listed in the phony tax refund request, and reached their head of account security. That person confirmed a direct deposit by the IRS for $8,936.00 was made on February 9, 2015 into an individual checking account specifying Kasper's full name and SSN in the metadata with the deposit.

"She told me that she could also see transactions were made at one or more branches in the city of Williamsport, PA to disburse or withdraw those funds and that several purchases were made by debit card in the city of Williamsport as well, so that at this point a substantial portion of the funds were gone," Kasper said. "She further told me that no one from the IRS had contacted her bank to raise any questions about this account, despite my fraud report filed February 9, 2015."

his name (but using a different email address) and requesting his transcript.

The head of account security at the bank stated that she would be glad to cooperate with the Williamsport Police if they provided the required legal request to allow her to release the name, address, and account details. The bank officer offered Kasper her office phone number and cell phone to share with the cops. The First National employee also mentioned that the suspect lived in the city of Williamsport, PA, and that this individual seemed to still be using the account.

Kasper said the local police in his New York hometown hadn't bothered to respond to his request for assistance, but that the lieutenant at the Williamsport police department who heard his story took pity on him and asked him to write an email about the incident to his captain, which Kasper said he sent later that morning.

Just two hours later, he received a call from an investigator who had been assigned to the case. The detective then interviewed the individual who held the account the same day and told Kasper that the bank's fraud department was investigating and had asked the person to return the cash.

"My tax refund fraud case had gone from stuck in the mud to an open case, almost overnight," Kasper sad. "Or at least it seemed to be that simple. It turned out to be much more complex."

For starters, the woman who owned the bank account that received his phony refund — a student at a local Pennsylvania university — said she got the transfer after responding to a Craigslist ad for a moneymaking opportunity.

Kasper said the detective learned that money was deposited into her account, and that she sent the money out to locations in Nigeria via Western Union wire transfer, keeping some as a profit, and apparently never suspecting that she might be doing something illegal.

"She has so far provided a significant amount of information, and I'm inclined to believe her story," Kasper said. "Who would be crazy enough to deposit a fraudulent tax refund in their own checking account, as opposed to an untraceable debit card they could get at a convenience store. At the same time, wouldn't somebody who could pull this off also have an explanation like this ready?"

The woman in question, whose name is being withheld from this story, declined multiple requests to speak with KrebsOnSecurity, threatening to file harassment claims if I didn't stop trying to contact her. Nevertheless, she appears to have been an unwitting — if not unwilling — money mule in a scam that seeks to recruit the unwary for moneymaking schemes.

ANALYSIS

The IRS's process for verifying people requesting transcripts is vulnerable to exploitation by fraudsters because it relies on static identifiers and so-called "knowledge-based authentication" (KBA) — i.e., challenge questions that can be easily defeated with information widely available for sale in the cybercrime underground and/or with a small amount of searching online.

To obtain a copy of your most recent tax transcript, the IRS requires the following information: The applicant's name, date of birth, Social Security number and filing status. After that data is successfully supplied, the IRS uses a service from credit bureau **Equifax** that asks four KBA questions. Anyone who succeeds in supplying the correct answers can see the applicant's full tax transcript, including prior W2s, current W2s and more or less everything one would need to fraudulently file for a tax refund.

The KBA questions — which involve multiple choice, "out of wallet" questions such as previous address, loan amounts and dates — can be successfully enumerated with random guessing. But in practice it is far easier, said **Nicholas Weaver**, a researcher at the **International Computer Science Institute** (ICSI) and at the **University of California, Berkeley**.

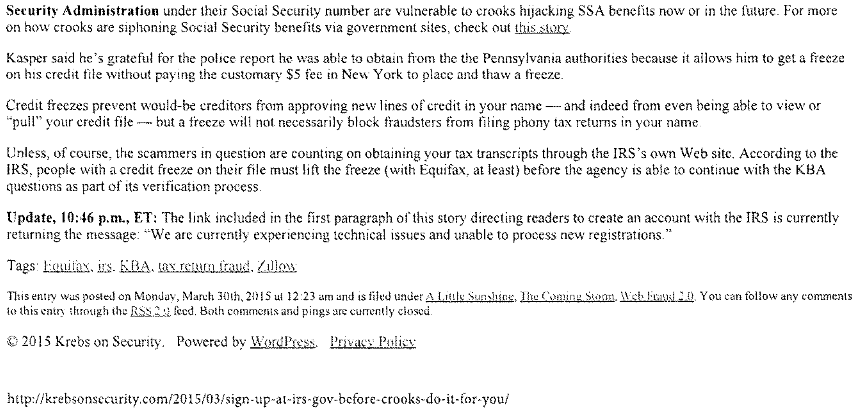
"I did it twice, and the first time it was related to my current address, one old address question, and one 'which credit card did you get' question," Weaver said. "The second time it was two questions related to my current address, and two related to a car loan I paid off in 2007."

The second time round, Weaver said a few minutes on Zillow.com gave him all the answers he needed for the KBA questions. Spokeo solved the "old address" questions for him with 100% accuracy.

"Zillow with my address answered all four of them, if you just assume 'moved when I bought the house'," he said. "In fact, I NEEDED to use Zillow the second time around, because damned if I remember when my house was built. So with Zillow and Spokeo data, it isn't even 1 in 256, it's 1 in 4 the first time around and 1 in 16 the second, and you don't need to guess blind either with a bit more Google searching."

If any readers here doubt how easy it is to buy personal data on just about anyone, check out the story I wrote in December 2014, wherein I was able to find the name, address, Social Security number, previous address and phone number on all current members of the **U.S. Senate Commerce Committee**. This information is no longer secret (nor are the answers to KBA-based questions), and we are all made vulnerable to identity theft as long as institutions continue to rely on static information as authenticators. See my recent story on Apple Pay for another reminder of this fact.

Unfortunately, the IRS is not the only government agency whose reliance on static identifiers actually makes them complicit in facilitating identity theft against Americans The same process described to obtain a tax transcript at irs.gov works to obtain a free credit report from **annualcreditreport.com**, a Web site mandated by Congress. In addition, Americans who have not already created an account at the **Social**



Security Administration under their Social Security number are vulnerable to crooks hijacking SSA benefits now or in the future. For more on how crooks are siphoning Social Security benefits via government sites, check out this story.

Kasper said he's grateful for the police report he was able to obtain from the the Pennsylvania authorities because it allows him to get a freeze on his credit file without paying the customary $5 fee in New York to place and thaw a freeze.

Credit freezes prevent would-be creditors from approving new lines of credit in your name — and indeed from even being able to view or "pull" your credit file — but a freeze will not necessarily block fraudsters from filing phony tax returns in your name.

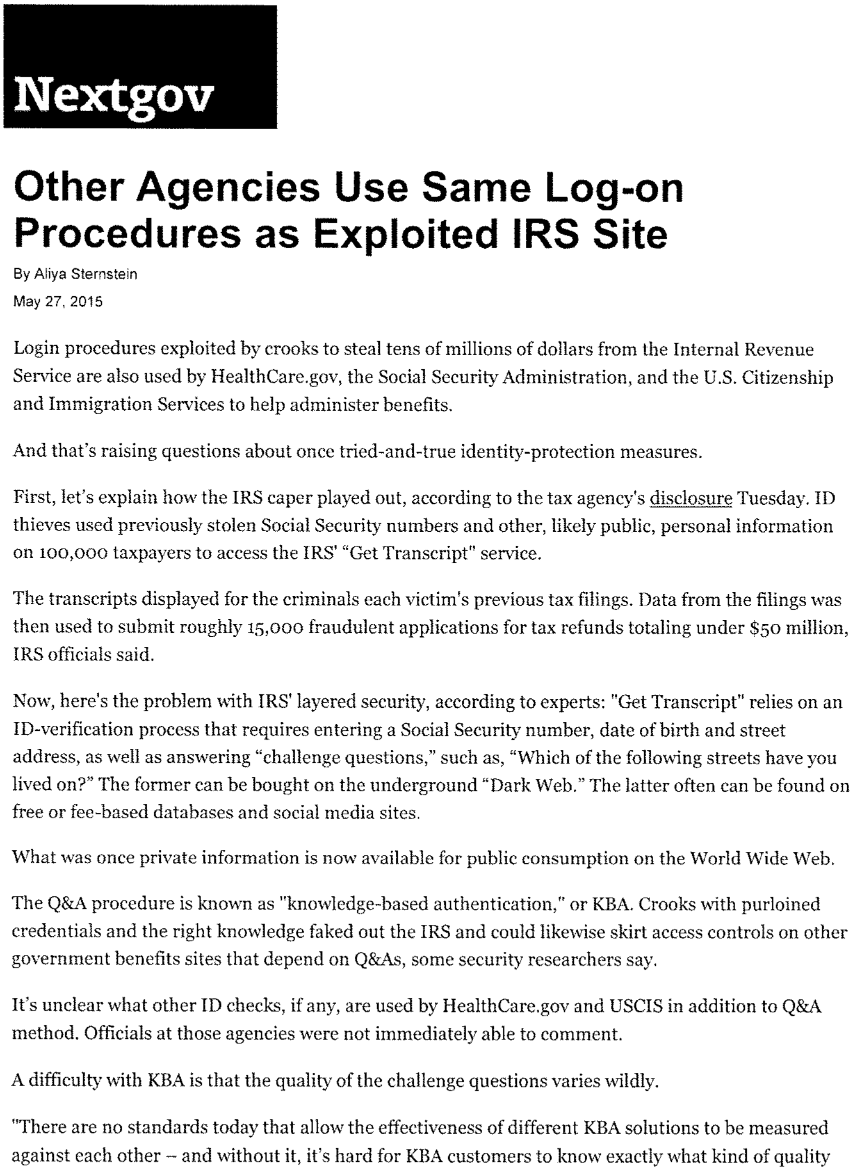
Unless, of course, the scammers in question are counting on obtaining your tax transcripts through the IRS's own Web site. According to the IRS, people with a credit freeze on their file must lift the freeze (with Equifax, at least) before the agency is able to continue with the KBA questions as part of its verification process.

Update, 10:46 p.m., ET: The link included in the first paragraph of this story directing readers to create an account with the IRS is currently returning the message: "We are currently experiencing technical issues and unable to process new registrations."

Tags: Equifax, irs, KBA, tax return fraud, Zillow

This entry was posted on Monday, March 30th, 2015 at 12:23 am and is filed under A Little Sunshine, The Coming Storm, Web Fraud 2.0. You can follow any comments to this entry through the RSS 2.0 feed. Both comments and pings are currently closed.

http://krebsonsecurity.com/2015/03/sign-up-at-irs-gov-before-crooks-do-it-for-you/



Nextgov

Other Agencies Use Same Log-on Procedures as Exploited IRS Site

By Aliya Sternstein

May 27, 2015

Login procedures exploited by crooks to steal tens of millions of dollars from the Internal Revenue Service are also used by HealthCare.gov, the Social Security Administration, and the U.S. Citizenship and Immigration Services to help administer benefits.

And that's raising questions about once tried-and-true identity-protection measures.

First, let's explain how the IRS caper played out, according to the tax agency's disclosure Tuesday. ID thieves used previously stolen Social Security numbers and other, likely public, personal information on 100,000 taxpayers to access the IRS' "Get Transcript" service.

The transcripts displayed for the criminals each victim's previous tax filings. Data from the filings was then used to submit roughly 15,000 fraudulent applications for tax refunds totaling under $50 million, IRS officials said.

Now, here's the problem with IRS' layered security, according to experts: "Get Transcript" relies on an ID-verification process that requires entering a Social Security number, date of birth and street address, as well as answering "challenge questions," such as, "Which of the following streets have you lived on?" The former can be bought on the underground "Dark Web." The latter often can be found on free or fee-based databases and social media sites.

What was once private information is now available for public consumption on the World Wide Web.

The Q&A procedure is known as "knowledge-based authentication," or KBA. Crooks with purloined credentials and the right knowledge faked out the IRS and could likewise skirt access controls on other government benefits sites that depend on Q&As, some security researchers say.

It's unclear what other ID checks, if any, are used by HealthCare.gov and USCIS in addition to Q&A method. Officials at those agencies were not immediately able to comment.

A difficulty with KBA is that the quality of the challenge questions varies wildly.

"There are no standards today that allow the effectiveness of different KBA solutions to be measured against each other – and without it, it's hard for KBA customers to know exactly what kind of quality they are buying," said Jeremy Grant, the recently departed senior executive adviser for identity management at the National Institute of Standards and Technology.

"KBA is not perfect, but, to date, it's been the best the market has had to offer when it comes to remote identity proofing – meaning solutions that give people the ability to prove their identity without the hassle of having to show up in person someplace," said Grant, who stepped down one month ago.

This sort of authentication is used on HealthCare.gov, mySSA and USCIS.gov to file for health insurance subsidies, access one's Social Security history and legal immigrant status, respectively.

A criminal can buy user IDs, passwords and KBA answers on the underground black market, said Chenxi Wang, a vice president at security firm CipherCloud. The puzzle pieces needed to put together a personality "are often available as a bundle," she said.

IRS officials said that's likely what happened with the "Get Transcript" breach. The tax refund crooks already had taken, from "non-IRS sources," the Social Security numbers, dates of birth and street addresses necessary to access the online feature. The bad guys also exploited "an outside source" to gain enough information to answer "several personal verification questions that typically are only known by the taxpayer."

Over the past few years, there have been many data breaches that compromised individuals' Social Security numbers and other personal details. They include attacks on, among other organizations, hospitals nationwide, several health care insurers, Lexis Nexis and Sony.

A safer mechanism for taxpayer registration would have been a two-step sign-on process that also required, for instance, a one-time pass code sent to the user's smartphone, many analysts said. Two-factor authentication "is more secure than KBA, but is also more cumbersome a user experience," Wang said.

On Thursday, Social Security officials said KBA questions are utilized in conjunction with personal records to confirm users are who they claim to be, but the agency also offers people optional two-factor authentication.

"We use knowledge-based questions as another layer of protection and work regularly with an external service provider to enhance our approach for using these types of out-of-wallet questions," Social Security spokeswoman Nicole Tiggemann said. "We work hard to ensure our online services are safe and the public's privacy is protected."

The IRS had the opportunity to switch to a more secure authentication arrangement but decided against it. A 2013 study that IRS officials helped author with NIST illustrated that using outside, governmentwide ID-check services, like those offered by Verizon or Symantec, could have saved them up to $305 million a year compared with the cost of maintaining their own in-house ID-proofing system.

The governmentwide ID companies also use KBA, but those providers must undergo a stringent certification process before they can sell to agencies.

"Even without considering any reduction in fraud from improved authentication of taxpayers, the adoption of improved online identity management would result in a net benefit of $74 million to $305 million annually, relative to continuing current operations," NIST National Strategy for Trusted Identities in Cyberspace officials said in July 2013.

The savings would come "primarily from eliminating the need for the IRS to pay to identity proof all users individually. Under an NSTIC-aligned authentication system, the IRS could instead accept third-party trusted credentials already strengthened by identity proofing. These third parties would be able to spread out the identity proofing costs across many relying parties at which the credential would be accepted."

The IRS decided not to make this ID security change.

Alternatively, the study recommended expanding the number of challenge questions and requiring every taxpayer to have a PIN number.

(Image via wk1003mike/ Shutterstock.com)

By Aliya Sternstein

May 27, 2015

http://www.nextgov.com/cybersecurity/2015/05/how-breach-government-benefits-site/113869/

Senator Ayotte QFRs June 2, 2015 Hearing Senate HSGAC
The IRS Data Breach: Steps to Protect Americans' Personal Information

<u>Question #1:</u>

If a tax-fraud victim calls the IRS to report that a fraudulent return has been filed in his/her name, is the IRS able to stop fraudulent refunds by either cancelling a paper check or informing a recipient bank for fraudulent direct deposit refunds?

If not, what authority would the IRS need to be able to stop fraudulent refunds that are in process?

Would the Social Security Identity Defense Act of 2015 (S. 1323), which I cosponsored with Senators Johnson and Warner, provide you with sufficient authority to do so?

Would authority to stop fraudulent refunds that are in process be beneficial to the IRS?

Response:

Most often, by the time the taxpayer warns the IRS they did not file the return in question, the refund has already been issued and the funds withdrawn from the account. If, however, the refund has not been issued, then the IRS can stop the refund from being released.

During criminal investigations, we coordinate efforts for revenue recovery from financial institutions directly or through the Bureau of Fiscal Services (BFS). Through the External Leads Program, we currently work with nearly 500 financial institutions that voluntarily provide IRS information regarding questionable refunds that the financial institution has received either from a direct deposit refund or a Treasury check being deposited. The IRS reviews the lead information and works with the financial institution to return the available funds.

There are currently no regulations that mandate a financial institution provide IRS leads or questionable refunds. We work with internal and external groups such as the Electronic Payments Association (NACHA), Network Branded Pre-paid Card Association (NBPCA), American Coalition for Taxpayer Rights (ACTR), and Financial Services Roundtable (FSR BITS) to conduct outreach to increase participation in the External Leads Program and share strategies for revenue protection.

As mentioned above, it is largely a matter of timing (not a lack of authority) that hinders our efforts to stop some refunds. However, we look forward to working with you to address any issues of authority in this area.

<u>Question #2:</u>

Since taxpayers are able to request their tax transcripts by filing Form 4506, has the IRS considered creating an opt-out mechanism for taxpayers that wish to not participate in the "Get Transcript" application?

Senator Ayotte QFRs June 2, 2015 Hearing Senate HSGAC
The IRS Data Breach: Steps to Protect Americans' Personal Information

While taxpayers would have to sacrifice the convenience of using the "Get Transcript" application, some taxpayers may forego the convenience to keep their personal information offline and to reduce potential access points to that information.

Response:

Although the "Get Transcript" application is shut down while the IRS works to strengthen the system, taxpayers have the option of contacting the IRS if they have concerns about their online account and can request that it be disabled (after completing the identity proofing process). In addition, we are developing automated disable and enable capabilities for all taxpayers. This will allow the taxpayer to disable or enable all online activity for their SSN after completing the identity proofing process.

Question #3:

I understand that there is a $50 charge to obtain tax transcripts using Form 4506. Would it be possible to waive this fee for tax fraud victims?

Response:

There is no cost to obtain a tax return transcript. Transcripts can be ordered using Get Transcript by Mail on IRS.gov; by calling the toll-free line, 1-800-908-9946; or by completing, and mailing or faxing Form 4506-T, *Request for Transcript of Tax Return*, or Form 4506-EZ, *Short Form Request for Individual Tax Return Transcript*.

The $50 fee is only required for requests to receive an exact photocopy of a tax return, with all attachments, using Form 4506, *Request for Copy of Tax Return*.

In most cases, the free transcript is all a taxpayer will need. For instance, taxpayers would request this transcript to verify income and marital status to a lender for student loans or a mortgage. Taxpayers would request an exact photocopy of a tax return from the IRS in limited circumstance, for instance if the taxpayer did not retain a copy of the return they filed.

Question #4:

How is the IRS going to create a secure, trusted ecosystem that protects all taxpayers, including the most vulnerable such as the poor, elderly, and the non-taxed (minors) when we know that those individuals are not included in the data the IRS obtains from the credit bureaus?

Response:

The IRS is working to protect the data of all taxpayers, including those with little to no credit history. One of the ways the IRS protects this data is through authentication and identity verification policies across channels (e.g., phone, correspondence, online via e-

Authentication, in-person) using internal IRS and third party data. Credit reporting questions include both credit and non-credit related questions so that individuals with limited credit histories may be able to pass our e-Authentication identity verification.

For taxpayers with no credit history, the IRS provides multiple channels for obtaining services such as tax transcripts, which do not rely on data from credit bureaus. Taxpayers can have a transcript mailed to their address of record by using Get Transcript by Mail on IRS.gov; by calling the toll-free line, 1-800-908-9946; or by completing, and mailing or faxing Form 4506-T, *Request for Transcript of Tax Return*, or Form 4506-EZ, *Short Form Request for Individual Tax Return Transcript*.

The IRS is considering additional enhancements to the e-authentication eco-system. These include increasing the level of assurance on all on-line services. Additionally, IRS is reviewing e-authentication options which will strengthen our systems while allowing wider use by more demographic groups, including individuals with limited credit history.

The IRS continually analyzes and implements technology solutions to improve authentication and the early identification of potentially fraudulent returns. As criminals obtain more personal information, authentication protocols need to become more sophisticated, moving beyond information that used to be known only to individuals and credit bureaus but now, in many cases, is readily available to criminal organizations from various sources. We must balance the ability of taxpayers to legitimately access their data and use IRS services online with the strongest possible authentication processes.

Realizing that the IRS is only one stakeholder in the battle against identity theft, we organized a Security Summit that was held in March 2015 with state tax administrators, tax software leaders, and payroll processing agents. During the Summit, we identified numerous new data elements that can be shared at the time of filing to help authenticate a taxpayer and detect identity theft refund fraud. The data will be submitted to the IRS and states with the tax return transmission for the 2016 filing season.

Question #5:

I understand that the IRS is currently running a pilot IP PIN program for taxpayers that reside in Florida, Georgia and DC, if they choose to opt in.

How long has this pilot program been running?

Response:

In 2014, the IRS piloted a program to provide an Identity Protection Personal Identification Number (IP PIN) to taxpayers who filed their prior year tax return in Florida, Georgia, or Washington, DC, and successfully obtained an Electronic Filing PIN (EFP) using the online application. Those states were chosen because they were the areas with the highest per-capita rate of identity theft.

Senator Ayotte QFRs June 2, 2015 Hearing Senate HSGAC
The IRS Data Breach: Steps to Protect Americans' Personal Information

In 2015, all taxpayers who filed their tax year 2013 return in Florida, Georgia or Washington, DC, are eligible to get an IP PIN. There is no longer any connection between getting an IP PIN and an EFP.

Are there any plans to expand the program to allow more taxpayers to opt into the IP PIN program?

If so, when does the IRS plan to expand this program?

Response:

We continue to analyze the benefits of the IP PIN program, the possibilities for future use, and the cost involved in expanding the program. In addition to taxpayers who filed tax year 2013 returns in Florida, Georgia, or Washington, D.C., we currently offer IP PINs to taxpayers with indications of stolen identity tax refund fraud, rather than to those who have received notice of unauthorized access to their personal data. With our present resource constraints, it is not possible for us to routinely offer an IP PIN to everyone who has been a victim of identity theft through breaches at other agencies or in the private sector.

The IP PIN is one tool in our identity protection strategy. We are also exploring other tools and solutions to increase security of taxpayer data available to a wider cross section of taxpayers. For example, as a result of the recent Security Summit we are looking at strengthening authentication at the point of filing through collaboration with state tax administrators, tax software leaders, and payroll processing agents. During the Summit, we identified numerous new data elements that can be shared at the time of filing to help authenticate a taxpayer and detect identity theft tax refund fraud. The data will be submitted to the IRS and states with the tax return transmission for the 2016 filing season.

Question #6:

Has the IRS sought input from states on how they are battling tax fraud?

Response:

The IRS and state tax administrators communicate regularly and share best practices in the battle against tax fraud. In March 2015, the IRS convened a Security Summit with state tax administrators, chief executive officers of tax preparation and software firms, and tax financial product processors to discuss emerging identity theft threats and expand existing collaborative efforts to stop fraud.

As a result of this summit, an agreement was reached to identify new steps to validate taxpayer and tax return information at the time of filing. The tax industry will increase the information it shares with government regarding suspected identity fraud, including analytics used to identify fraud schemes and locate indicators of fraud patterns . More information is available on our website at http://www.irs.gov/uac/Newsroom/IRS-and-

Industry-and-States-Take-New-Steps-Together-to-Fight-Identity-Theft-and-Protect-Taxpayers"

The groups agreed to expand sharing of fraud leads with the IRS. Currently, the IRS obtains this analytical information from some groups, but not all. For the first time, the entire tax community will share aggregated analytical information about their filings with the IRS to help identify fraud. This post-return filing process has produced valuable fraud information because trends are easier to identify with aggregated data. The expanded effort will ensure a level playing field so everyone approaches fraud from the same perspective, making it more difficult for the perpetration of fraud schemes.

In addition to continuing cooperative efforts, the groups will look at establishing a formalized Refund Fraud Information Sharing and Assessment Center (ISAC) to more aggressively and efficiently share information between the public and private sectors to help stop the proliferation of fraud schemes and reduce the risk to taxpayers. This would help in many ways, including providing better data to law enforcement to improve the investigations and prosecution of identity thieves.

Participants from the tax industry agreed to align with the IRS and the states under the National Institute of Standards and Technology (NIST) cybersecurity framework to promote the protection of information technology (IT) infrastructure. The IRS and the states currently operate under this standard, as do many in the tax industry.

The IRS, industry, and states agreed that more can be done to inform taxpayers and raise awareness about the protection of sensitive personal, tax, and financial data to help prevent refund fraud and identity theft. These efforts have already started, and will increase through the year and expand in conjunction with the 2016 filing season.

Question #7:

Has the IRS fully assessed the costs and benefits of accelerating W-2 deadlines?

In November 2014, the IRS reported that it convened a working group of internal stakeholders and subject-matter experts to identify the costs and benefits of accelerating Form W-2, Wage and Tax Statement, deadlines.

Has the working group identified and considered the potential impacts on internal and external stakeholders? If so, please provide my office with a copy of the report.

In addition, please provide my office information on the IRS systems and work processes that will need to be adjusted to accommodate earlier, pre-refund matching of W-2s and identify timeframes for when these changes could be made.

Response:

The IRS convened a working group of internal stakeholders and subject matter experts to identify the costs and benefits of accelerating Form W-2 deadlines in November

2014. The core activities of the subject matter experts began in January 2015, following the completion of the filing season start up, and resulted in a June 2015 assessment. When finalized, the report will address your questions and will serve as the response to a recent GAO recommendation surrounding this issue.

Accelerating information return filing due dates would greatly enhance the IRS's ability to verify suspicious returns earlier in the return filing process and help us do a better job of stopping improper payments. The IRS has partnered with key stakeholder groups to explore the impacts of accelerating third party information return deadlines. The majority of stakeholder groups conceptually agree that accelerating information reporting would benefit tax administration. Potential impacts are being considered for the following stakeholders: taxpayers; tax professionals and payroll organizations; software providers; and government entities. The IRS is in the process of drafting the report in response to the recommendation in GAO-14-633, *Identity Theft, Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud.* (See attachment)

In addition to this working group, the IRS issued temporary and proposed regulations in August, 2015, that would remove the automatic 30-day extension of time to file certain information returns and instead allow only a single non-automatic extension of time to file, beginning with forms in the W-2 series (except Form W-2G) that are due after December 31, 2016. The IRS is seeking comments on the proposed regulations by November 12, 2015.

Question #8:

How many financial institutions and other government agencies participate in the External Leads program?

In August 2014, TIGTA recommended that the "IRS establish more consistent time frames to verify leads based on analysis of current and historical lead verification data and, once established, communicate these verification time frames with external partners; develop a process to ensure that leads are verified within established time frames; and consolidate the current four lead inventory tracking systems into a single tracking system and ensure that key information is captured as to how each lead is resolved."

What changes has the IRS made on these recommendations? Is any congressional action needed to help the IRS make the most of this program?

Response:

The IRS revised the processing timeframes related to the External Leads Program and the updates will be reflected by October 2015 in the Internal Revenue Manual (IRM) Section 25.25.8, *Revenue Protection External Lead Procedures.*

Through the External Leads Program, the IRS receives leads on questionable tax refunds identified by partner institutions, including financial institutions, government and law enforcement agencies, state agencies, tax return preparation entities, and other sources. We currently receive referrals from 495 sources. A consolidated database was created to track the status of each lead to ensure timely processing and information sharing session meetings have been scheduled with external sources to discuss results from the leads that they had provided to ensure new and emerging fraud trends are being identified and refunds stopped.

The IRS is also in the process of updating the Publication 5033, *IRS External Leads Program: Fact Sheet on Submitting Leads*. This document provides our external stakeholders with guidance on how to submit leads, as well as the applicable IRS timeframes for response. The publication indicates that the IRS will contact the financial institution within 10 business days of the original lead and inform them of the total amount of funds that should be returned to the IRS along with an indemnification letter prior to transmittal of funds. The publication provides external sources a response for their account holders if they inquire about their refund after the financial institution returned the funds to the IRS, providing a 6-8 week timeframe for their account to have information readily available.

We continue working to increase participation in the External Leads Program and are analyzing options for recommendations. We don't believe additional statutory authority is needed at this time.

Attachment to Response to Sen. Ayotte Question 7

Date: September 22, 2015

Subject: IRS comments on recommendation #1 in GAO-14-633, *Identity Theft – Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud*

Responsible Function: Director, Business Modernization Office, Wage and Investment Division (W&I)

GAO-14-633: The Government Accountability Office (GAO) recommended that IRS fully assess the costs and benefits of accelerating Form W-2, *Wage and Tax Statement* deadlines and provide information to Congress on:

- The IRS systems and work processes that will need to be adjusted to accommodate earlier, pre-refund matching of Forms W-2 and then identify timeframes for when these changes could be made;
- Potential impacts on taxpayers, IRS, Social Security Administration (SSA), and third parties; and
- What other changes will be needed (such as delaying the start of the filing season or delaying refunds) to ensure IRS can match tax returns to Form W-2 data before issuing refunds.

Title: Accelerating Form W-2, *Wage and Tax Statement* Deadlines

Scope: GAO-14-633 indicated that certain characteristics of the current tax processing system hamper IRS' ability to effectively verify taxpayer information, specifically Form W-2 data, prior to issuing refunds. IRS convened a working group of internal stakeholders and subject matter experts to identify the costs and benefits of accelerating Form W-2 deadlines. The scope of the working group was to:

- Address the current state of IRS systems and work processes and the requisite adjustments or enhancements that will be necessary to meet the objective of using accelerated Form W-2 information;
- Identify and consider the potential impacts on internal and external stakeholders;
- Identify and evaluate other changes that may be necessary in order to match Form W-2 data to tax returns prior to issuing refunds.

Executive Summary: Stopping identity theft and refund fraud is a top priority for the Internal Revenue Service. The IRS is continually reviewing and updating processes and policies to minimize the incidence of identity theft and refund fraud. As a result of aggressive efforts to combat identity theft, the IRS has stopped 19 million suspicious returns and protected more than $63 billion in fraudulent refunds from 2011 through October 2014. For the 2015 filing season, IRS assigned more than 3,000 IRS employees to work on identity theft-related issues - more than twice the number of people working on these cases in 2011. These employees are working to prevent refund fraud, investigate identity theft-related crimes and help taxpayers who have been victimized by identity thieves. While the IRS has made considerable progress in this area, more work remains. Fighting identity theft is an ongoing battle as identity thieves continue to create new ways of stealing personal information and using it for their gain[1].

[1] http://www.irs.gov/uac/Newsroom/IRS-Combats-Identity-Theft-and-Refund-Fraud-on-Many-Fronts-2015

Third party information returns, including Form W-2, can serve an increasingly important role in preventing tax return based identity theft and refund fraud in the pre-refund environment. The IRS supports accelerating the filing deadline of Form W-2 to January 31. The introduction of more Form W-2 data into our tax return screening strategy, earlier in the filing season, would enhance IRS' ability to perform risk-based analysis of tax returns to identify cases of potential identity theft and refund fraud before refunds are issued, further strengthening pre-refund processing defenses.

Accelerating the filing deadlines of Forms W-2 alone will not permit IRS to meet all of the objectives associated with this strategy. The individual components of a systems-based approach, along with supporting legislative, regulatory and policy changes, as well as IRS adjustments or enhancements to systems, business processes and staffing requirements, would permit IRS to maximize the benefits of using the accelerated W-2 data. Earlier information return and W-2 data provides immediate benefits through expansion of the use of W-2 data in the Return Review Program (RRP)[2]. However, the following components in Table 1, in whole or in part, could allow the IRS to fully maximize the benefits of receiving information returns earlier.

Table 1: Components of a Systems-Based Approach to Maximizing the Benefits of Form W-2 Acceleration

Component	Is legislative or regulatory change required?	Timeframe
Accelerate the due date for filing Form W-2 with SSA to January 31[3]	Yes	One year after legislative proposal is adopted
Eliminate the extensions to file Form W-2, regardless of filing method[4]	Yes	One year after legislative proposal is adopted
Reduce requirement to electronically file Form W-2 from 250 to five[5]	Yes	One year after legislative proposal is adopted
Provide IRS with greater flexibility to address correctable errors[6]	Yes	One year after legislative proposal is adopted
Delay the processing of tax returns until W-2 information return data becomes available	No	Filing season following adoption of legislative proposal to accelerate the Form W-2 due date
Expand the use of W-2 data as a component of risk-based tax return assessments with identity theft and fraud filters, delaying refund issuance for certain suspicious tax returns	No	Filing season following adoption of legislative proposal

[2] The RRP is a major IRS project under development that in Filing Season 2015 has already become a major contributor in pre-refund identity theft fraud detection. The RRP is being designed to replace the EFDS analytics with powerful 'next generation' analytics and processing power, enhancing many aspects of IRS compliance activity through being able to evaluate and assign a non-compliance probability score on millions of tax returns each day. The RRP, if provided adequate funding, is envisioned to perform historical filing consistency and linked-return analysis combined with advanced analytics and rapid processing speed to review massive amounts of returns for potential noncompliance and fraud, including identity theft and other types of non-compliant filings. All potential non-compliant or fraudulent returns will be sent downstream for case management and the appropriate treatment, depending on the type and level of non-compliance.

[3] From the General Explanations of the Administration's Fiscal Year 2016 Revenue Proposals (Green Book): Rationalize Tax Return Filing Due Dates So They Are Staggered.

[4] Disaster extension requests will continue to be considered.

[5] From the General Explanations of the Administration's Fiscal Year 2016 Revenue Proposals (Green Book): Enhance Electronic Filing of Returns.

[6] From the General Explanations of the Administration's Fiscal Year 2016 Revenue Proposals (Green Book): Provide the IRS with Greater Flexibility to Address Correctable Errors.

Accelerating Form W-2, *Wage and Tax Statement* Deadlines

A. Current State: Form W-2, unlike most other types of information returns which are filed directly with IRS, is currently[7] mandated to be filed with the SSA in accordance with the timeframes identified in Table 2.

Table 2: Current Form W-2 Filing Deadlines

	Paper	Electronic
Form W-2 Due Date	Last day of February	March 31
First Extension[8]	March 31	April 30
Second Extension[9]	April 30	May 31

For Tax Year 2013, over 232M Forms W-2 were filed with SSA, 88.7 percent electronically and 11.3 percent by paper. Form W-2 filers that file 250 or more Forms W-2 are required to file electronically; however, there are no restrictions on electronic filing for lower volumes. The SSA requires significantly longer processing times to process paper filed Forms W-2, sometimes as late as August or September, well after filing season.

The SSA processes Forms W-2 and transmits the data elements to the IRS for purposes of tax administration. The IRS' Form W-2 data processing flow generally consists of three major milestones: intake, processing and posting. Due to system limitations, key processing steps in the IRS treatment of Form W-2 data rely on batch versus daily processing, affecting the capacity and speed in which the data can be posted to the Information Returns Master File (IRMF)[10]. Once the Form W-2 data is posted to the IRMF, it generally becomes available for pre-refund fraud detection immediately. Table 3 illustrates the typical delay in the W-2 data becoming available to IRS systems following receipt from SSA. This condition is largely caused by the current Form W-2 filing deadlines and IRS systems limitations, which combine to result in the Form W-2 data not being available to IRS until well into the filing season, after the majority of refunds have been disbursed.

Table 3: Accumulated Total of Forms W-2 that were Posted to IRMF per Tax Year (TY):

	Cycle 6	**Cycle 9**	**Cycle 14**	**Cycle 17**
TY2014	20,501,061	59,578,345	197,607,675	205,213,454
TY2013	0	228,113	138,562,744	199,204,184
TY2012	15,900,154	30,910,321	175,794,451	192,285,199
TY2011	0	0	127,604,873	181,926,210

Notes:

- TY2013 W-2s were delayed by Government Shutdown until Cycle 8.
- TY2011 W-2s were not processed by IRS until Cycle 12.
- Cycle 6 is around 1st to 2nd week of February.
- Cycle 9 is around 1st week of March.
- Cycle 14 is around 1st week of April.
- Cycle 17 is around 1st week of May.

[7] IRS issued temporary regulations in August 2015 that will remove the automatic extension of time to file information returns on forms in the W-2 series (except Form W-2G). The temporary regulations, if adopted, will allow only a single 30-day non-automatic extension of time to file these information returns, effective for filing season 2017.

[8] Filers do not need to provide cause for this request.

[9] Filers must provide cause for this request (i.e. disaster).

[10] The IRMF is the IRS database for information returns. The IRS' Information Technology organization has initiated a multi-year strategy to modernize Information Return processing to address existing processing limitations. The modernization will consolidate intake technologies and processes, leverage new data formats, and store data in a relational database, increasing the IRS' ability to use the information collected to support compliance activities. Tentatively, the Form W-2 processing flow will shift from legacy processing to the modernized platform in Processing Year (PY) 2018 or 2019.

To address the lag time in receiving third party information returns, including Form W-2 data, due to current filing deadlines, the IRS' pre-refund identity theft program has evolved along with the increase in identity theft, and IRS has increased its screening of returns for identity theft and fraud at multiple points in the processing cycle. The Return Integrity and Compliance Services (RICS) organization is responsible for key components of IRS' pre-refund defenses. All refund returns flow through the Electronic Fraud Detection System (EFDS), Dependent Database (DDb) and the RRP, which contain sophisticated fraud models and filters developed from historical fraud characteristics used to identify questionable income, withholding, refundable credits and taxpayer identity. In addition to these systemic fraud checks, the IRS performs manual analysis of tax returns with characteristics that indicate refund schemes. If detected, processing holds are placed on certain suspicious refunds until they can be validated with Form W-2 and/or other third party information. These traditional fraud detection/revenue protection methods address millions of questionable returns each year.

B. Requisite Adjustments or Enhancements to IRS Systems and Work Processes: An IRS working group concluded that the most efficient start-up strategy to expand the use of Form W-2 data in the pre-refund environment is to leverage the capabilities of the RICS RRP. In its present version, the RRP receives and loads information returns, to include available Form W-2 data, from the IRMF on a weekly basis and stores the data in an integrated data warehouse that combines the information with taxpayer data for data mining, runtime scoring, and research. As a component of its analysis, the RRP systemically flags returns with potential identify theft for treatment that results in identity theft indicators being placed on the account (in conjunction with EFDS and DDb), freezing further processing and the issuance of refunds.

Accelerating Form W-2 deadlines would allow RICS to feed more data, earlier, into the RRP and EFDS which, in turn, would accelerate the incorporation of Form W-2 data into risk-based analysis of tax returns in the pre-refund environment. Sending the data earlier to the RRP would likely reduce false positives passed downstream to the EFDS that require manual processing to reconcile. The RRP/EFDS/DDb systems can accommodate the accelerated W-2 data with limited enhancements, but may increase RICS staffing requirements for manual review of flagged returns.

The following adjustments or enhancements must be made to IRS systems and work processes to meet the objective of using accelerated Form W-2 data:

IRS Systems

- Improve access to W-2 data processed by the SSA – $2.579M in Information Technology (IT) funds and 18 Full Time Equivalent staff years[11] to:
    - Fund additional IT equipment and programming support to provide the IRS with improved access to W-2 data processed by the SSA, specifically Forms W-2 and W-3, *Transmittal of Wage and Tax Statement,* more quickly.
    - Accelerate the posting cycles of Form W-2 data to the IRMF to make the data available to downstream systems[12].

[11] IRS FY 2016 President's Budget

[12] IRS typically begins processing Form W-2 data around February 16. Without any changes, IRS is seeking to begin processing on January 27, 2016, for TY 2015. In PY 2017/TY 2016, provided with adequate resources, the IRS is aiming to begin processing Form W-2 data around January 4th (pending final IRS/SSA agreement).

- Modify the IRMF programming to ensure that the correct tax year indicator is applied to the accelerated Form W-2 data for downstream processing (estimated cost $200K).

Work Processes

- Expand pre-refund treatment streams for those tax returns with W-2 discrepancies related to identity theft, refund fraud and non-compliance. To alleviate some of the burden this would put on IRS resources, new policies, processes and guidelines would have to be implemented, including a change to math error authority[13], which must be legislated.
- Assess related staffing requirements to address potential increase in volume of cases requiring manual review prior to refund issuance. When identity theft or fraud filters identify Form W-2-related discrepancies, the wage information attached to the return must be manually verified. Having more Form W-2 data upfront could potentially lead to a larger volume of returns requiring income verification and reconciliation prior to releasing refunds, thus requiring additional resources[14].
- Assess customer service needs for taxpayers whose refunds are delayed. When the IRS takes an action on a taxpayer's account to delay a refund, they are provided with a method to contact the IRS to address the discrepancies so the refund can be released.

C. Stakeholder Impact: The IRS has partnered with key stakeholder groups to explore the impacts of accelerating third party information return deadlines. The majority of stakeholder groups conceptually agree that accelerating information reporting would benefit tax administration. Potential impacts were considered for the following stakeholders:

- Taxpayers
- Tax Professionals and Payroll Organizations
- Software Providers
- Government Entities: IRS; SSA; National Taxpayer Advocate Service (TAS); GAO; Treasury Inspector General for Tax Administration (TIGTA)

Taxpayers: The IRS typically issues more than nine out of ten refunds in less than 21 days and taxpayers have grown accustomed to this efficiency. A delay in the processing of tax returns until W-2 information return data becomes available would result in a corresponding delay in issuing refunds, primarily impacting those taxpayers who file prior to mid-February. Taxpayers relying on refunds earlier in the year may incur a financial hardship; however, the impact could be expected to normalize in subsequent years, as taxpayers adjust to the new filing season processing timeframe. Additionally, taxpayers who do not have consistent income and withholding information may be required to interact with the IRS before their refunds are released, extending normal processing times.

Tax Professionals and Payroll Organizations: Generally, the third party tax professional community has communicated that they recognize the benefits of accelerating the Form W-2 deadline to prevent identity theft and refund fraud; however, they believe the change would also impact their current operating models. Table 4 identifies issues that are representative of their concerns with Form W-2 due date acceleration. Many of these concerns would be applicable to employers as well.

[13] From the General Explanations of the Administration's Fiscal Year 2016 Revenue Proposals (Green Book): Provide the IRS with Greater Flexibility to Address Correctable Errors.

[14] The President's fiscal 2016 budget request includes $101 million specifically devoted to identity theft and refund fraud.

Table 4: Illustrative Summary of Tax Professional Concerns with Accelerated W-2 Filing Deadlines

Concern	Impact
Incomplete Information	Form W-2 information may be inaccurate due to the lack of complete information for items such as third-party sick pay and state disability pay information which is not due to employers until January 15 for inclusion on an employee's Form W-2.
Accuracy	Information reported on the Form W-2 comes from a variety of sources. Accelerating the reporting date increases the potential for errors. Some industry groups estimate six to eight percent[15] of employers would have to adjust the Form W-2 data after the original submission on January 31 (the current adjustment rate is approximately one to two percent)[16].
Condensed Time Frames	With only 31 calendar days to gather and process payroll records after the year-end, some employers may experience strain in gathering the Form W-2 data elements, as well as performing year-end adjustments and reconciliation.
Increase In Corrections Or Amended Returns	Inaccuracies or incomplete Form W-2 information may result in increased filing (two to six percent) of Form 941-X, *Adjusted Employer's Quarterly Federal Tax Return or Claim for Refund*, Form W2C, *Statement of Corrected Income and Tax Amounts* (adjusted Forms W-2) and Form 1040X, *Amended U.S. Individual Income Tax Return.*

Software Providers: Software providers may need to modify or update their software packages and programs, requiring sufficient lead time to meet the new requirements. Adequate time must also be provided for testing and IRS approval of the modifications.

Government Entities:
IRS: Accelerating the Form W-2 filing deadline to January 31 would compress the time required for the IRS to receive and process Form W-2 data. This would occur at a time of year (the beginning of filing season), when IRS systems and personnel are fully engaged in filing season preparation and kick-off.

A delay in the processing of tax returns until W-2 information return data becomes available could potentially impact the IRS by:

- Compressing the timeline for tax return processing.
- Stressing the Modernized e-File (MeF)[17] system due to increased start-up volumes after the delay.
- Shortening seasonal employee employment periods, adversely impacting IRS hiring, retention and quality of work.

SSA: The SSA has invested to improve Form W-2 service delivery through modernized systems and processes. Even with these investments, accelerating the deadline could be expected to:

- Increase Form W-2 customer service contacts; any change in filing timeframes or methods may increase the volume of requests for information that the SSA receives.
- Require the acceleration of annual systems testing; the SSA and IRS would need to shift annual systems testing from late October/November to September, to allow time for any needed adjustments or fixes.

[15] IRS Oversight Board Public Forum: Focus Forward – The Next Five Years in Tax Administration, Real Time Tax Initiative Implications for Information Reporting: National Payroll Reporting Consortium, May 1, 2013.

[16] National Payroll Reporting Consortium, May 1, 2013: "6% - 8% of employers" may equate to a larger percentage of employees and Forms W-2, because large employers have more complex compensation and benefits offerings, and make up much of the population with adjustments.

[17] The MeF is a web-based system that allows electronic filing of corporate, individual, partnership, exempt organization and excise tax returns through the Internet.

TAS/GAO/TIGTA: The National Taxpayer Advocate has espoused the benefits of accelerated third party information reporting to taxpayers and tax administration in her 2009, 2011 and 2012 annual reports. In more recent testimony[18], the Advocate supported enabling IRS to receive and process Forms W-2 before releasing refunds as an important step in deterring perpetrators from committing fraud and identity theft. GAO and TIGTA have also recommended that IRS expedite access to W-2 data for similar reasons.

D. Benefits: Accelerating the IRS' receipt of third party Form W-2 information can be expected to yield significant benefits in tax administration:

Reduced Taxpayer Burden:

- Increases the probability of preventing fraudulent activity on taxpayer accounts that may require interaction with the IRS to resolve.
- Allows the IRS to accelerate the release of some legitimate tax returns suspended by identity theft filters or other processes.
- Reduces the need for the IRS and employer interactions to verify Form W-2 data for employees whose returns are identified as high-risk by identity theft filters or other processes. A typical IRS/employer interaction to verify Form W-2 data can take up to 30 minutes.

Government Savings: For Government, the potential for billions of dollars in net revenue protection and the ability to redirect resources may result from pre-refund identity theft and fraud detection on tax returns being filed with the IRS:

- Accelerated Form W-2 data will help strengthen IRS efforts to reduce the occurrence of pre and post-refund identity theft and refund fraud, as well as the category of refund fraud that is undetected by the IRS each year.
- For each case of identity theft where the real taxpayer files a return after an identity thief has already filed a fraudulent return, the IRS must manually work the case to investigate the identity theft and ensure the legitimate taxpayer receives a refund. Identifying and stopping fraudulently filed returns earlier would reduce the need for this manual processing by IRS employees.

Improved Compliance:

- Substantially mitigates vulnerabilities to identity theft related refund fraud earlier in the filing season and allows the IRS to address identity theft and refund fraud more effectively before refunds are paid.
- Allows the IRS, over time, to direct resources to other issues.

[18] Written Statement of Nina E. Olson-National Taxpayer Advocate. Hearing on "Tax Fraud, Tax ID Theft and Tax Reform: Moving Forward with Solutions" Before the Committee on Finance: United States Senate, April 16, 2013.

E. Summary: Congress can help the IRS to continue to make progress combating identity theft and refund fraud by providing the legislative authority and resources required to expand the use of Form W-2 data in our tax return screening strategy earlier, enhancing the IRS' ability to perform risk-based assessments of tax returns. The IRS' systems-based approach to maximizing the benefits of Form W-2 acceleration will:

- Support the acceleration of the due date for filing Forms W-2 to January 31, providing IRS with earlier access to Form W-2 data to help identify cases of potential identity theft and refund fraud before refunds are issued, strengthening our pre-refund defenses and furthering our evolution from a "look back" compliance model.

- Ensure that the IRS has access to the vast majority of Forms W-2 prior to the processing of tax returns by eliminating the extensions to file Form W-2, regardless of filing method, and reducing the threshold for required electronic filing from 250 to five Forms W-2.

- Streamline tax return processing where identifiable errors can be quickly resolved by granting IRS greater flexibility to address correctable errors.

- Advance revenue protection by permitting the IRS to leverage more of its tax return screening technology and processes in the pre-refund environment.

Successful acceleration of Form W-2 filing deadlines will require inter-governmental and public/private industry partnerships to meet the objectives of leveraging accelerated Form W-2 data while minimizing unnecessary burden during the implementation. The IRS is committed to working closely with key stakeholder groups during all phases of the transition to ensure the needs of stakeholders are understood and addressed.