IRS Security and Summit Updates: Making Progress against Identity Theft
(edited transcript)

Good afternoon. Thank you for attending. The title of this seminar is IRS and Security Summit Updates; Making Progress Against Identity Theft. Can everyone hear me okay? In the back?

Okay. My name is Terri Parks-Thompson and I am a member of the Return Integrity and Compliance Services Organization, also known as RICS. RICS falls under the umbrella of the Wage and Investment Division. So, if you're not familiar with RICS, RICS is generally responsible for pre-refund compliance which includes the prevention, detection of identity theft returns as well as refund fraud. We also play a lead role within the Security Summit Group, if you're familiar with that.

So, our objectives for today is to review Security Summit efforts to help combat tax-related identity theft, to provide victim assistance, -

to outline some steps that you can take to help in this effort as well as give you a preview of our 2018 safeguards.

Identity theft presents a challenge nationwide for all businesses, organization, and governmental agencies including the IRS. So, it places a tremendous burden on its victims, on industry, and on our economy. This is not just not an IRS problem. This is not just a tax fraud problem. This is an international problem fueled by criminal enterprises here and abroad. It will take all of us collectively working together to combat it. I hope you've had an opportunity to sit in on two other seminars, identity theft seminars. One was hosted by a criminal investigation –

agent. It was called Data Compromises. The other was hosted by Larry Gray from NATP, also giving you tips on cyber security and the threats that you may face.

Unfortunately, for some people, the first time they learn that they are a victim of identity theft is from the IRS. They file a tax return electronically and it may be rejected because someone has filed a tax return using their name and their Social Security Number or they may receive a verification letter from the IRS asking if they filed a certain return because we stopped it because it looked suspicious. So, these letters will ask your clients to –

verify their identities in some way either by calling us or visiting a tax payer assistance center. The letters that you – I'm speaking of are the 4883 C Potential for Identity Theft

and the 5747 C letter. The 5747 C letter will absolutely ask your client to make an in-person visit to an IRS office to verify their identity. Or the client may receive a paper refund check in the mail that they know they didn't file a tax return for or they may receive a tax transcript in the mail for which they did not order. So, these two letter cases absolutely are indications that our identity theft filters are in fact working.

So, whatever the criminal was looking for, they didn't receive it because it went to the address of record. So, they did not benefit from receiving a refund in their mailbox or receiving transcripts at an address. So, the effort by criminals to quickly monetize stolen identities by filing fraudulent tax returns has put the IRS, the taxpayers, and you right in the middle of this fight. So, I would like to give a historical overview and then outline our new approach that we believe is making inroads against this crime. The problem of tax-related identity theft really exploded from 2010 to 2012 and, for a time, overwhelmed industry, -

law enforcement and us, the IRS.

So, over the next few years, we made steady progress within our reduced sources, resources, both in terms of protecting against fraudulent refund claims and prosecuting those engaged in this crime. Our strategy was prevention, detection, victim assistance, and criminal enforcement. So, from 2010 to 2015, the IRS took many steps to fight back and better protect taxpayers. We greatly improved our identity theft filters, we limited the number of direct deposits and we locked accounts of deceased taxpayers.

We also worked with the banks to get help to identify suspicious refunds. We created the Identity Protection PIN or IP PIN which you're familiar with, to –

prevent tax payers from being victimized repeatedly. We – also, our Criminal Investigation Division put more than 2,000 identity thieves behind bars. But all of these actions we put in place over a series of years, although we consider it real progress, there's much more work needed to be done.

So, initially, tax-related identity theft was a crime of opportunity. The thieves might have an insider working within a hospital or a college, having access to many names and Social Security Numbers. Excuse me. But as our identity theft filters become more sophisticated, criminals needed more information about a legitimate taxpayer in order to be successful. We evolved, so did the criminals. Identity theft –

shifted from relatively small-time thieves to national and international criminal enterprises. So, these sophisticated organized criminal syndicates had resources, technological know-how and, unbeknownst to us, tax savvy. This next generation of identity thief can now steal hundreds of thousands of Social Security Numbers and names and Social Security Numbers at a time. They roam the 21st Century version of the Wild West, also known as the Dark Net, that vast expanse of the World Wide Web that is unseen and uncatalogued by most search engines and invisible to you and I. So, on the Dark Net, criminals can buy and sell SSNs and people's –

personal identifiable information or PII on a huge scale and for little dollars. So, just as those of us in the tax community do our filing season, planning, and strategy, so do these criminals. They master stolen identities, they use clues, discussion forums on the Dark Net to plot strategy and trade information. They are constantly probing and testing our filters. So, if they're constantly probing and testing our filters, we know that they're doing the same to you.

We stopped the vast majority of the identity theft returns. We're very good at stopping the ones where the thief only has the name and Social Security Number. However, it becomes more difficult when they in fact have more information, additional information like the names and –

Social Security Numbers of your spouses, your dependents. They may know the information from your prior year tax returns. They may even have your prior year income.

So, after a series of identity theft incidents in 2015, IRS Commissioner Koskinen convened a meeting in Washington, D.C. with representatives from the state tax agencies and the tax community. We agreed to find new ways to leverage our public/private partnership to help battle identity theft refund fraud against these organized criminal syndicates. So, motivating us was the understanding that no single organization could fight this type of fraud alone. This meeting led to the development of the Security Summit –

Group. So, it's an unprecedented group that has focused our joint efforts on making sure that the tax filing experience would be a safer and more secure experience for the taxpayer, and that includes you and I.

Our emphasis quickly centered on what steps we could take to better authenticate the identity of the taxpayer and the validity of the tax return at the time of filing. Thanks to a lot of hard work by our partners, we put in place a series of safeguards for 2016. Our focus was on the do-it-yourself tax returns. Here are a few actions that we took. So, we

identified data elements from both state and federal tax returns to improve the fight against fraud.

What that means is that we looked at the time that it took to complete a tax return so that we could quickly identify those rapid computer-generated returns. Tax software providers, they strengthened password protocols for users to better protect and prevent account takeovers. Anyone been a victim of account takeovers? No? It's a good thing. Summit Group members also agreed on the need to create a Tax Administration, Information Sharing and Analysis Center or ISAC to share actionable data information about identity theft schemes. So, we believe that ISAC will in fact – has great potential to be our early warning system that will allow us to rapidly respond to identity theft threats.

Okay. All security partners agreed to align under a stronger cyber security framework. We also agreed to expand the number of work groups including a tax professional work group to focus on your issues specifically. The IRS also took steps to better protect its online tools creating a robust, secure, access identification/verification – identity verification process. So, this relies on a two-factor process including a secure code being sent via text and that would be for returning users. So, having a big risk e-authentication system is –

critical as the IRS moves towards adding more self-help tools in account information on the IRS.gov website.

Let's talk results. The results of the Security Summit initiatives for 2016, we believe, were impressive. So, the number of identity theft returns entering the processing pot blind dropped dramatically, and that's a good thing. Because we stopped more returns at the door, there was a cascading effect. So, here are some numbers. During 2016, the IRS stopped 969,000 confirmed identity theft returns. That resulted in a 30 percent decline.

The number of suspect refunds stopped by banks and returned to the IRS dropped by 50 percent. So, that was 124,000 returned refunds. The number of people who reported to the IRS that they were victims of a tax-related identity theft, that dropped by 46 percent. That number translates to 376,000 taxpayers. Despite those incredible numbers, we're not even close to declaring victory.

Okay, so for 2017 filing season, our emphasis remained on what we call trusted customer requirements. So, what this means is that with a great deal of certainty, we are certain, we are sure that the person filing the tax return is –

who he or she say they are. So, we expanded our focus from do-it-yourself filers to include safeguards involving tax professionals and business returns. Here are a few steps that we took. So, we identified more new data elements that we will be receiving from the e-file return. For the first time, we agreed to collect and share – because you know the IRS doesn't like sharing so much – to collect and share data elements from business returns, extending identity theft protections to Form 1120 and 1041 filers. More than 20 states are working together with the financial services industry to create their own version of a program that allows financial services to flag suspicious refunds preventing –

them being deposited into taxpayers' account.

Our financial services partners are also enhancing their efforts in relation to our ultimate bank account initiative. The goal here is to do a better job at identifying not only fraudulent refunds but also legitimate ones. This is, of course, to help minimize refund delays to the taxpayer. Thanks to the help from the payroll community and the software industry, we expanded the W2 verification code initiative to about 50 million W2s in 2017. So, are we – anyone here familiar with the W2 initiative?

Okay. So, those of you not familiar, the W2 initiative was a unique password – I'm sorry – a unique code that we assigned to some payroll providers and they would insert this unique code to the left of box 10 on the W2. But as we go forward in this seminar, I'll share our plans for 2018. The software industry expanded strong password requirements to tax professionals as well as taxpayers which helped prevent account takeovers by identity thieves. So, taken together, these trusted customer requirements will help the IRS and states do a better job of protecting taxpayers of detected –

fraudulent tax returns and protecting the taxpayers. Now in January, we also launched the initial stages of ISAC, which is the Information Sharing and Analysis Center. This will help us identify emerging identity threats – identity theft schemes. I'm sorry. We'll be able to quickly share this information among some partners. This way, we can move faster to shore up our defenses against these emerging threats. We believe ISAC will also help enhance law enforcement efforts to investigate and prosecute these identity thieves. This will be an important new, long-term defense for the nation's tax system. It will eventually become a cornerstone in our fight against identity theft. For example, -

if a tax professional suffers a data breach, the states and the IRS can quickly share SSN data to adjust their filters and help block any fraudulent returns, which helps your clients.

Congress also gave IRS some new tools for 2017. We all know what they were. They probably created a little bit of a headache for you guys. One, they accelerated the deadline for the filing of W2s and information returns so that we can quickly verify

income and thus protect the taxpayer. The other tool was holding refunds that contained EITC, earned income tax credit, and the additional child tax credit, holding those refunds until February 15th.

I'm almost certain your clients did not like that. But these were two tools that Congress did give us and we're happy about it in the fight against identity theft and fraud, refund fraud. We don't have the results for 2017 filing season, but preliminary numbers show that we're on the right path and making progress.

Okay, so let's turn to victim assistance. So, there's two ways your clients may learn that they are a victim of identity theft. Either they report it to us or we report it to them. As you know, our systems are only –

set up to accept unique Social Security Numbers for all persons listed on a tax return. So, if you are unable to submit your client's return electronically because of a duplicate SSN reject, you should double-check a few things. One, of course, be sure that the Social Security Numbers you entered is correct. Then second is to check dependents, check that they're not being claimed twice. We see it often. Young adults enter the workforce – excuse me – and they claim themselves. They file a tax return and they claim themselves when in fact their parents are still claiming them. The other is so, if you rule out those types of errors and the return rejects again, we all know what that means. That means that you must file your client's tax return via paper.

So, if you have to file a paper tax return for your client, we ask that you also file a Form 14039 which is the identity theft affidavit. Check box one, which is for tax administration impact. Once we receive the paper tax return and the 14039, we'll begin working the case to identify the legitimate taxpayer and set aside the fraudulent one.

So, at this point, we know it can be frustrating for you, for your client, but it takes time to resolve these cases. It takes time; however, we're resolving them within 120 days or less and all of that is dependent upon our resources, the volumes –

that we see, staffing, and also the complexity of the case. When I mentioned complexity of the case, some taxpayers are unaware that they've been a victim for years and they think it's just for that particular filing season when, in fact, they've been a victim for years and we have to undo all of that.

The other way taxpayers learn they are victims of identity theft is if they receive a notice from the IRS about a suspicious tax return. So, this is a part of our Taxpayer Protection Program. This is when we identify and halt a suspicious return. We issue a letter to the taxpayer who must tell us if they did or did not file a return in question. The most common notice –

would be the letter 4883 C, Potential for Identity Theft. This letter is sent when a return sets off our filters. So, it will instruct the taxpayer to call a telephone number within 30 days and inform us if they did or did not file. We worked very hard this year to staff our Taxpayer Protection Program phone lines to reduce wait time and to provide a better level of service.

The other letter, the 5747 C is sent to taxpayers who we absolutely know have been a part of a larger breach. Matter of fact, -

a lot of the data breaches that you hear in the media, we get that data and we know the taxpayer is involved and we will issue those particular taxpayers a 5747 C letter, just precautionary to protect them. So, they've been a part of a larger data breach. An identity thief may have enough information about them that they could pass our telephone authentication process. Scary. So, an in-person verification process is the only way we can be certain that we're dealing with the legitimate taxpayer. We have clarified in the 5747 C, since it asked them to go to –

an IRS office, we have clarified that if they're calling to report that they did not file the tax return in question, they do not have to go to an IRS office.

We make every effort used in various data elements to identify the legitimate taxpayer and exclude them from the 5747 C requirement. So, if your client receives either of these letters, the 4883 C or the 5747 C, they should respond immediately. If they did file the tax return, we will not release the – if they did file the tax return, we will not release the refund until their identity is verified either on the phone or that in-person visit. Starting January 2017, IRS also began notifying –

tax-payers when a valid Social Security Number appears on a Form W2 and the IRS determines that the W2 does not belong to the SSN owner. In this situation, there is no impact to the taxpayer's ability to file a tax return or receive a refund. Why? The W2 may be an error or it may be the result of a misused Social Security Number. Because there is a risk to the taxpayer, we send them a CP01E. Anyone see that this past filing season? So, the E just means it's employment related. This proactive notification allows taxpayers to check and protect other –

financial accounts and make sure that there's no other impact. So, as a tax professional, I'm sure you want to do all you can to help ease the burden of your clients and we don't want to add to that burden. Hard to believe, but we do not want to add to that burden, unnecessarily. But these are often cases in which we must deal directly with the filer. So, we may confirm their identity and ensure that we are dealing with a legitimate taxpayer.

With that being said, we did make one change this year that many of you tax professionals requested previously. If a client had an identity theft indicator on their account and you wanted to access their tax transcripts via the TDS service, Transcript Delivery Service, you were not able to.

Anyone? Yes. So, even if you had a power of attorney on file, it didn't matter. So, we have modified that procedure. You may now access those client transcripts for the tax years in which there is no identity theft issue. However, for the tax year in which there is an identity theft issue, only the tax-payer will have access.

How can you help? So, glad you asked. So, because the IRS and the states and industry are making progress, it means these cyber criminals need even more data they can use to impersonate taxpayers. That means there's been a major shift to targeting you, the tax professionals, payroll professionals, -

and others that hold a great deal of financial data. There are a few simple steps that you can take as a professional, tax professional to help protect your clients and protect your business. In fact, we've created an awareness campaign aimed at tax professionals called Protect Your Clients, Protect Yourself. It can be found at IRS.gov/ProtectYourClients. One, please review publication 4557, Safeguarding Taxpayer Data, because you have a legal obligation to protect your taxpayer data. Use it as a guide for conducting a review of your current security measures and outlining how to create and update your security plan. It is critical you assess your current security –

precautions and address any weaknesses. If there is a way, they will find a way in. Again, the pub can help you complete a risk assessment, create a security plan to better protect your data. It will show you how to create a security plan that addresses those risks, and it advises at least once a year, if not more often, to perform an internal assessment. You should evaluate and test your existing security plan and safeguards for deficiencies and weaknesses and create a plan to address them.

Number two, use best security practices at all times. So, the most common way for cyber criminals to steal identities, passwords, and other sensitive data is to simply ask you for it.

So, you know where I'm going. They send phishing emails to bait you into opening a link or an attachment that contains malware, viruses, et cetera. Of course, IRS, we currently have a campaign underway called Don't Take the Bait, which is aimed at increasing awareness amongst tax professionals about phishing emails. So, simple steps go far. Use unique passwords, use good security or great security software, and encrypt sensitive data. There's a governmental agency called the National Institute of Standards and Technology, NIST, and they set out a cyber security framework that all –

governmental agencies must use. Recently, they published a guide for small business which we also recommend that you review. It is "Small Business Information Security; the Fundamentals". You can find that at NIST.gov.

So, we also ask that you please maintain direct contact with the IRS. You can sign up for e-news for quick – for tax professionals on IRS.gov, sign up for quick alerts. You can follow us on social media, Facebook.com/IRSTaxPros or Twitter.com/IRSTaxPros and we'll try to keep you abreast of any emerging scams and schemes.

Number three; contact the IRS immediately –

in case of data loss. So, our stakeholder liaisons are your designated point of contact. You can find a number and contact information for each state on IRS.gov. Keyword search is "Stakeholder Liaison." We have a page on IRS.gov called "Data Loss Information for Tax Professionals" that can offer guidance to those who have theft. Excuse me. Again, check out IRS.gov/identitytheft. Just know, once you contact the state liaison, they will contact others within the IRS including the Criminal Investigation Division. So, if notified quickly enough, we can take steps –

to help prevent your clients from being victims of tax related identity theft.

Number four; maintain, monitor, and protect your e-FIN and e-services accounts. We urge you to maintain, monitor these accounts. They are a target, a routine target for phishing scams. So, it's critical that you maintain your e-file application. We ask that you keep them up to date, current list of all personnel, addresses phone numbers. Remember, your e-FIN is not transferrable. Therefore, if you sell the business, the new principles must apply for their own e-FIN. Also, if you are –

seeking an e-FIN for the very first time, you can only get an e-FIN from the IRS. Do not fall for applying for an e-FIN through third party providers. You can only get that from the IRS. You should also monitor the number of returns filed with both your e-FIN or your PTIN. So, for the e-FIN, you access your e-services account, your e-file application. If the numbers are too high, please, call the e-help desk immediately. It's very important that you monitor that account. If you are an enrolled agent, a CPA, attorney, or participate in the annual filing season program, from your PTIN account, select "Returns Filed per PTIN."

If a minimum of 50 returns has been processed with your PTIN in the current calendar year, a chart will display with your numbers. It's updated weekly and includes only Form

1040 return data. If you suspect misuse of your PTIN, complete the Form 14157, the Return Preparer Complaint. Please, monitor your accounts.

You must protect your e-services – excuse me – e-FIN information. As I mentioned, criminals routinely try to steal – excuse me – e-service passwords and e-FINS so they can file fraudulent tax returns. That's why we're moving toward a stronger identity verification process for e-services accounts. Last year, -

I'm told that they discussed a secure access process. So, this is a two-step process so that criminals need more than just your user name and password. For example, they may need a security code sent via a text. So, we recognize the need to strengthen the authentication process and we hope you do as well.

Also, number five, share security tips with your clients. During our earliest meetings at the Security Summit, we recognized that we were missing an important partner in this effort, the public. So, most safeguards similar to those for you are easy. Use strong and unique passwords, use security software to protect against malware and viruses, encrypt sensitive data, learn to recognize and avoid –

phishing scams. We absolutely need your help to get this information out to taxpayers and to your colleagues. So, here's what you can do. Routinely share the publication 4524, "Security Awareness for Taxpayers" with your clients to help improve their online security awareness.

Number six; warn your employer clients about the W2 scam. We ask your help to warn your business clients or employers of the most dangerous scams we've seen. This scheme involves identity thieves posing as a company's chief executive or a supervisor and sending a legitimate-looking email to the payroll department. They will simply –

ask for the information. They will ask for a list of all company employees and their W2s. This is the second year we've seen this. These emails are being seen nationwide. It's been in the media. Major companies are seeing this email. Hospitals are seeing these emails. These types of scams are called Business Email Compromise, BEC – because IRS has an acronym for everything – or Business Email Spoofing, BES. When the IRS is aware of data losses such as this, there are steps you can take to help protect employees, but time if critical here. We've created a new information page for employers and payroll professionals about this W2 scam. You can find it at IRS.gov/identity theft in the business section. So, if employers receive a W2 scam –

email or is a victim of a W2 crime involving data loss, on the slide there are email addresses that are critical for you. Employers should also make their states aware of the W2 theft as well. That email is listed on the slide. It's the last bullet for the states. So,

scams in general have been extremely prolific in recent years. We must do more to educate everyone; the tax professional, payroll professionals, and the public about these phishing emails in general.

What's new for 2018 filing season? I can tell you –

that we will be working very hard in this upcoming filing season to reduce false positives. False positives are those legitimate – I'm sorry – are those suspicious returns that we put through the Taxpayer Protection Program that are filed by legitimate taxpayers. This is a priority for us for 2018. Trust us. We know false positives are a burden for your taxpayers, your clients, for you, and, absolutely, for us. We will also continue with the W2 verification code initiative. So, we are creating a specific box, a specific number box on the W2 for the verification code. However, not every W2 will have a unique code. We have –

50,000 – I'm sorry – 50 million W2s in this year. Going forward for 2018, we don't have the number yet, so we'll make that announcement later how many W2s we'll issue with a unique code.

There is one area of concern that is the business-related identity theft. So, we've seen an increase in the number of fraudulent Form 1120s, 1120 Ss, 1041s and Schedule K1s. Do not underestimate the tax code savviness of these national and international criminal syndicates. As we've made great progress on individual returns, we've seen a jump in business return fraud to 10,000 –

fraudulent returns this year which is up from 4,000 last year. Although that number may seem small compared to individual returns, but the dollar figures, you can imagine, are significant. Here's an issue that we're seeing. So, if a criminal breaches a tax preparer system to steal client data, they will steal business data as well. Not only that, they are savvy enough to know if there is K1 information available, they can file fraudulent K1 returns that goes for trusts in the states. So, for 2018, we will be asking tax practitioners to provide additional information about business returns as part of the tax preparation software requirements. We need you to provide this information so we can better determine the legitimacy of the return. This will help your client.

New 1120 verification data points are we will be looking, verifying the name and Social Security Number of the executive authorized to sign the tax return – is the person authorized to do so – payment history or their estimated tax payments, parent company information – is there a parent company – additional information based on deductions claimed. We'll be looking at filing history. Has the business filed Forms 940, 941, or

other business-related tax reforms? Also, be aware of any potential business clients that say they do not currently have an employer identification number.

The bottom line is we need your help.

So, this last slide highlights just a few of the resources that we do have available. Again, we do currently have underway a campaign, Don't Take the Bait. So, of course, I mentioned the focus here is on security protections for tax professionals, especially against phishing emails and all the risks that they bring. We would ask for your help in urging tax payers to protect themselves. You can share publication 4524, "Security Awareness for Taxpayers". We need your help to warn your employer clients about the threat posed by W2 scams. Most of all, we need your help to protect client data by using all the security tools at your disposal. The IRS cannot fight –

identity theft on its own. This is a critical problem and we all must address it. So, we all have a role to play. So, let me just – I just want to thank the tax professional community, the national associations for their work on this outreach effort as well as taking a very active role in our security summit initiatives over the past year. Clearly, there's still much more for all of us to do, but thanks to the security group, we've come a long way in a short time. Thank you for attending.

Glossary

EFIN - An Electronic Filing Identification Number is needed by providers electronically file tax returns. The IRS assigns an EFIN to identify firms that have completed the IRS *e-file* Application to become an Authorized IRS *e-file* Provider.

IP PIN - An Identity Protection Pin is a six-digit number issued to a taxpayer who has previously been the victim of identity theft. The IP PIN is used to protect the taxpayer by preventing their tax account from being used by anybody else. Once a taxpayer receives an IP PIN, it is required to file a return to authenticate the taxpayer's identity.

ISAC - The IRS created the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC) to help states, the software industry, and tax processors spot and stop fraud.

NATP – National Association of Tax Professionals is the largest nonprofit organization, with members in all 50 states, focusing specifically on federal tax preparation.

PII - Personally Identifiable Information is any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

TDS – The Transcript Delivery System provides self-service for return and account information requests by external customers through the e-services portal. TDS automates the validation, processing and delivery of taxpayer information to the authorized Third Party user.

PTIN - Preparer tax identification numbers are used by individuals who prepare or assist in preparing federal tax returns for compensation. All enrolled agents must also have a valid PTIN.

Index