Good day, ladies and gentlemen, and welcome to the "Data Thefts and Protecting Client Tax Information" webinar. At this time, it is my pleasure to turn the floor over to your host Gerry Kelly-Brenner. Ma'am, the floor is yours.

Thank you. And hello. My name is Gerry Kelly Brenner and I am with the Internal Revenue Service. I would like to welcome you to today's webinar titled "Data Thefts and Protecting Client Tax Information." Before I introduce the participants in today's webinar, I would like to introduce a special guest. John Koskinen was appointed commissioner of the IRS in December 2013. Given the importance of this topic, Commissioner Koskinen wanted to spend just a few minutes with you today. Commissioner.

Thank you and welcome to all of you tax professionals. I wanted to speak to you personally today to remind you and to acknowledge how critical and important you are to ensuring the security of taxpayer information. You and your clients are on the frontlines in defending against identity thieves. You will hear more about our security summit in a minute, but I want you to know we are committed to working in partnership with you and the tax professional's organizations to protect the integrity of the tax system. We, the tax industry, states, and the IRS, all have a role to play in this effort. We all share a common enemy, those who are stealing your clients' personal information and committing refund fraud. And we all share a common goal, protecting taxpayers.

It is clear that criminals have been able to gather significant amounts of personal information as the result of data breaches at sources outside the IRS, which makes protecting taxpayers increasingly challenging and difficult. That's why we had the security summit that Ken will talk about today, and why we joined with the states and the tax industry to make substantive changes for 2016. No one of us can fight this enemy alone, but together we have a chance to achieve our goal of protecting taxpayers.

The purpose of this webinar is to talk about your role. We want to make sure you are aware of the dangers out there, that you know the best practices for protecting taxpayer data, and if you suffer a data loss you know what to do about it. I'm also here to ask for your help. We are making a major outreach effort to individual taxpayers, raising awareness about their need to protect their own data. I would ask you to help us spread the word. As you work with your clients, please talk to them about identity security. Encourage them to treat their personal data like they do their cash, don't leave it lying around. They should be using security software, avoid oversharing on social media, and refrain from opening suspicious emails.

We're updating publication 4524, that's 4-5-2-4, Security Awareness and Identity Theft. This publication is aimed at taxpayers. You can easily print it and include it in the completed tax package you give your clients. There will also be updated information on IRS.gov this filing season. Finally, I want to thank you for all the work you do day-in and day-out. You are critical to maintaining the integrity of the tax system. And thank you for your interest in this webinar. I think you will find it very helpful.

Thank you for that message Commissioner Koskinen. We appreciate you taking the time to join us today. Our webinar today, we'll discuss one of the most challenging issues, protecting taxpayer information in the data theft era. The objective is to increase your awareness about data loss threats, provide you with information about best practices, and ensure that if you do suffer a loss you know the next steps to take.

Before we begin, let me review a few items. If you are with the media, please send us an email message at sbse.webinars@irs.gov with your contact information. Our media relations staff can assist or answer questions you may have. All forms, instructions, publications, and webpages mentioned today are available on www.irs.gov. For your convenience, we have provided you with a PDF file of this presentation to download, print, and take notes on. It includes a list of the majority of the resources we'll mention today. If you did not notice it previously, you will see a button labeled "Materials" or a link to download the file on this webinar page.

You can ask questions during the webinar by clicking the "Ask Question" button under the photo window and selecting the "Submit" button. At the end of this presentation our subject matter experts will respond to your questions. We will answer as many questions as time allows. Please limit your questions to the

webinar topic. Also, please do not ask any questions about specific case-related situations, and please avoid inappropriately disclosing any sensitive or identifying information about you, your business, your clients, or anyone else when you submit a question. And, finally, I would like to remind our audience that the information discussed today is current as of the presentation date, and it should not be considered official guidance. The program will be archived on our website at www.irsvideos.gov for later viewing.

Now, let's get started with the presentation. Joining us today are the key players at the IRS in combatting identity theft and one of your colleagues who has experienced a data theft. Ken Corbin is the director of IRS Return Integrity and Compliance Services. Ken is responsible for pre-refund revenue protection and the oversight of refundable credits. This includes screening returns for potential fraud and identity theft. Shawn Tiller is the executive director of Refund Crimes in the IRS Criminal Investigation. He is responsible for guiding the activities of Refund Crimes Headquarters staff and employees in eight scheme development centers located across the United States. Mark Kahler is currently the National ID Theft Coordinator for IRS Criminal Investigation in the Office of Refund Crimes. In that position, he coordinates criminal investigation efforts to combat tax-related ID theft refund fraud. And David P. Lyons III, CPA, CFP, is from Connecticut, and he has experienced ID theft firsthand. He is the president of Lyons & Lyons, PC. Lyons & Lyons, PC has offices in Richfield and Fairfield, Connecticut, and has been in existence since 1980. Ken, will you please start us off?

Thank you, Gerry. And thanks to all of you tax professionals who are taking time today for this webinar. I also want to thank Shawn, Mark, and David for joining us as well. The IRS has made significant inroads in combatting tax-related identity theft, but the depth and breadth of the problem continues to present a challenge, not only to the IRS but I would argue to every business and organization in the country. This includes the tax-preparer industry. Personal data, whether it's credit card numbers or names, bank accounts, addresses, and social security numbers, are commodities, products that can be stolen and then bought and sold on a global black market, and used for fraudulent purposes. The thieves can be international cybercriminals beyond our reach, or they can be that disgruntled employee you just fired.

The Bureau of Justice Statistics reports identity theft now costs U.S. victims more than all other property crimes combined. The Federal Trade Commission reports identity theft is the number one compliant by citizens. A March 2015 study by a California research company found criminals stole $16 billion from 12.7 million American consumers in 2014. That's a new fraud victim every two seconds, and two-thirds of those victims were data breach victims.

Also this spring, IBM issued a study that found more than one billion personal records, many with personally identifiable information, were stolen in 2014. Many of these data breaches most often in the news involve credit cards. But, more important, especially for the tax industry, are the data thefts involving personally identifiable information, or PII. This often involves an individual's name, social security number, address, and maybe even a list of their dependents and their SSNs. Criminals can do far greater damage to victims with stolen PII.

Generally, you're not liable for elicit charges to your credit card, but if a thief opens a financial account in your name or, even worse, hijacks your bank account, you can suffer horrible financial, emotional, and personal losses. The Department of Health and Human Services keeps a record of data thefts involving health care-related entities involving more than 500 people. So far, for 2015, data thefts involving health care-related entities results in more than 150 thefts of PII and/or health care information for more than 100 million Americans.

There is a glut of PII on the black market. A good illustration of this is our own "Get Transcript" application. In this sophisticated effort, third parties succeeded in clearing a multi-step authentication process that required prior personal knowledge about the taxpayer, including social security number, date of birth, tax filing status, and street address before accessing IRS systems.

By the way, we recognize the severity of the situation for these taxpayers and we are doing everything we can to help them. But this incident underscores the vast amount of personal data already in the hands of criminals and the impact it can have on tax administration. And our goal today is to urge you to learn the

lessons of the past year. That each one of you will walk away from this call and immediately start a review of data security, upgrade when necessary, and create a plan of action for both protecting data and for reacting in the case of data theft.

Let me turn to tax-related identity theft specifically. Not all breaches result in identity theft, and not all identity theft results in tax-related identity theft. From 2011 through October 2014, the IRS stopped 19 million suspicious returns and protected more than 63 billion in fraudulent refunds. In calendar year 2015 through September, the IRS rejected or suspended the processing of 4.5 million suspicious returns. So far, we've stopped 1.2 million confirmed identity theft returns, totaling $7.2 billion.

Additionally, year-to-date, we've stopped $2.3 billion worth of refunds and other types of fraud totaling $9.5 billion in confirmed fraudulent refunds protected. It is important to point out that preventing refund fraud and identity theft involves a delicate balance. This is because the IRS has a dual mission when it comes to issuing refunds. We must balance the need to issue refunds in a timely manner, with the need to ensure that claims are proper and taxpayer rights are protected. Years ago, taxpayers could expect to wait several weeks for a refund. Now more than 85% of taxpayers file their tax returns electronically, and when coupled with direct deposit they can get their refunds in 21 days or less.

Typically, we receive third-party information, such as forms W-2, that verifies information on the return after the tax return is filed. We address this lag time by using data modeling and filters and compliance checks to identify potentially identity theft and fraud. This pre-refund compliance work is performed by my organization, RICS. The IRS has stepped up efforts against refund fraud in many ways in recent years. We have implemented new identity theft screening filters to improve our ability to spot false returns before we process them and issue refunds.

In 2012, tax returns passed through 11 filters. Today, returns must pass through nearly 200 filters. We also have accelerated, to the extent we can under present law, the use of information returns in order to identify mismatches earlier. We are also limiting the number of refunds that can be electronically deposited into a single financial account or prepaid debit card. We have implemented a variety of mechanisms to stop the growing use by criminals of decreased individuals' identity information to perpetuate tax fraud. We routinely lock accounts of deceased taxpayers, and have locked nearly 29 million accounts to-date. Also, the Bipartisan Budget Act of 2013 included the administration's proposal to limit public access to the Death Master File, which should further help to reduce identity theft related to tax fraud.

We have developed better procedures to use information about identity theft victims received from law enforcement officials. We are working to eliminate or reduce the use of SSNs with our systems or employ masking techniques. We have developed procedures to better stop the processing of fraudulent returns from prisoners and we've established the External Leads Program for receiving leads from financial institutions that have agreed to participate in the program. In 2014, 286 institutions participated in the program and helped return nearly 198,000 erroneous tax refunds, totaling $545.6 million. In the past three years, we have recovered over $3 billion, with over 200,000 leads per year.

For those of you who have EFINs, Electronic Filing Identification Numbers, you should know we are doing a comprehensive review of this program to determine what we can do to improve safeguards. We already have stepped up efforts to expel those who are abusing EFINs for fraudulent purposes. We are working hard to prevent them from using stolen identities to obtain your EIN or using your EIN to e-file identity theft returns. Also, we have increased our number of on-site visits as a part of our monitoring program to ensure EFINs are being used properly.

That is a much abbreviated rundown of our recent actions. And I want to say here that thanks to all of those actions we are able to stop the vast majority of fraudulent returns. In the 2015 filing season it became clear these efforts, while important, weren't enough. Our criminal investigation division found increase in identity theft crime being perpetrated by organized crime syndicates. To improve our efforts against this complex and evolving threat, Commissioner Koskinen convened a security summit this

spring. We joined with state departments of revenue, tax software providers, financial institutions, including the debit card industry, to come up with some immediate actions for 2016.

Our focus was on new steps to validate taxpayer and tax return information at the time of filing. We have centered our efforts initially on the do-it-yourself products. This is an area where we could make that immediate impact and where the immediate risk was. Industry will be sharing more than 20 new data elements with the IRS that will help us verify individuals. We're not disclosing all of those elements, but the information shared will assist us in identifying those returns that may be mass generated or reveal certain patterns related to identity theft or fraud schemes.

We've agreed on a new password standards for do-it-yourself software and other verification methods for new or returning customers. The idea is to help prevent criminals from taking over taxpayers' accounts. We also agreed to share fraud leads. For the first time, the entire tax industry and other parts of tax industry will share aggregated analytical information about their filings with the IRS to help identify fraud. If we have information on emerging schemes, we can adjust our filters to identify them. Providers who transmit 2,000 or more returns will share any schemes they identify on a weekly basis.

We also agreed that more can and should be done to raise taxpayer awareness about the protection of sensitive, personal, tax, and financial data to help prevent refund fraud and identity theft, and this also applies to tax preparers, which is why we are here today. We also have moved to create additional workgroups, including one for tax preparers like yourselves, because we all recognize the critical role you play in protecting the integrity of the tax system. That workgroup is just now getting underway.

The tax preparers have just the type of personal data that are so valuable to thieves, and you often have it for hundreds of people. If that data is stolen, it makes it difficult for us to identify fraudulent returns and determine the identity of legitimate taxpayers. With this type of PII and personal data, thieves can cause all kinds of headaches and heartaches for your clients. We can sit here and tell you how important data security is, but we think David Lyons' story will really hit home for you. David is a certified public accountant from Connecticut who has, unfortunately, experienced this issue firsthand. David?

Hello everyone. I want to share some information with you to help you possibly avoid what happened to me. My firm was the victim of a data breach. Fortunately, $100,000 of my expenses were covered by insurance, however, I needed $250,000 of coverage. Prior to February 2013 I had limited exposure with identity theft. Annually, we would have approximately three clients per year who were victims of identity theft. Most of these clients were residents of the State of Florida. I never thought what I'm going to describe to you would have ever happened to my firm.

In late February 2013 a number of our clients contacted us saying they had received letters from the Internal Revenue Service advising them that their 2012 returns were being reviewed. Our firm had not filed the returns nor had the client submitted the return. I informed our clients that they should contact the IRS immediately to notify the service that the returns in question were fraudulent. I then reached out to several other CPA firms in the local area to see if their clients were receiving a similar letter. No other firm had been contacted by their clients regarding this particular IRS notification. At this point in time I believed that a breach may have occurred. My firm did not have any data breach plan, but at this time I did contact my insurance carrier to make them aware that a cyber breach may have occurred.

I attempted to notify the Internal Revenue Service of a possible firm breach, but was unable to get specific guidance on my next course of action. The guidance I received related to an individual having identity theft, not a firm having a cyber breach. After being on the telephone for four hours with the Internal Revenue Service I decided to contact the executive director of the Connecticut State Society of CPAs for guidance. He provided me with a specific contact person in the Internal Revenue Service. Based on my discussions with this IRS contact person, it was clear to me that a significant number of my clients had had fraudulent returns filed. A number of these clients had not even received notification from the IRS that their returns were being reviewed.

We spent a weekend looking through the tax program and noticed all clients in the 2011 tax program had been backed up to an unknown source in the early hours of a morning in October of 2012. No such download had been authorized by me, and the actual download files were no longer on the system, which indicated that whoever downloaded the files took steps to cover their tracks. Now that we were confident that a cyber breach had taken place, I, again, contacted my insurance carrier and engaged a legal firm.

Our attorney contacted the IRS Criminal Investigation Unit and they advised our attorney that the Homeland Security Division of the Secret Service was aware that fraudulent tax returns were being filed on behalf of our clients. They were in the process of planning a surprise visit to our office. But since we had notified the IRS of the cyber breach, rather than confiscating our computers, they requested permission to allow them to image our computers in an effort to find out how hackers accessed our clients' information.

During this time, the Secret Service would not allow us to notify our clients that their information was compromised. It took more than a week for the Homeland Security officers to come to the office. During this time, more clients were getting letters stating that the IRS was reviewing their 2012 tax returns. Two Homeland Security officers, two IRS Criminal Investigators, arrived at our office, as well as our attorneys and IT people. Homeland Security imaged all of our computers to try to find out how the hackers got in. It was at this time that the Homeland Security advised us that they knew who was responsible and that they had used a remote access program to gain access to our server. They then used a program known as Brute Force to crack the password protection.

Homeland Security was in the process of extraditing an individual from Bulgaria who was responsible for our hack, and we're hoping to find the person who developed the malware used in our breach and various other breaches. They were also hoping that he would implicate people in the United States who were assisting in collecting the fraudulent refunds. This individual is currently in prison in New Jersey. Once the imaging was completed, we were then allowed to notify our clients. Working with our attorneys, we engaged ID experts to provide identity theft protection and restoration services to our clients.

It took days compiling the names and addresses of all of our clients affected by the breach. An individual letter was required to be sent to every taxpayer, spouse, and dependent. Each person had to receive a letter individually. Letters also needed to be sent to all partners, shareholders, in all corporations, as corporations, and 1065s that we prepared. Some of our partnerships had 40 to 70 partners who never heard of Lyons & Lyons, PC. It was necessary for each individual who received this letter to call into a call center or sign up online to obtain the service using the personal identification number provided in the notification letter. This was extremely difficult for many of our elderly clients.

Our attorneys notified the appropriate attorney generals and other government agencies of the data theft, as required under individual state law. Not all stats have the same individual state laws. The attorney general for each state in which a client or potential client resided was required to be notified of the breach. We probably notified between 35 to 40 attorney generals in the various states.

Once our clients received the letter, the number of telephone calls was overwhelming. We literally did not have enough lines to handle all the calls. We had to rehire an employee who had recently retired, and also hire additional administrative help. Every client wanted to speak with me. Even though the staff was given speaking points by our public relations firm, I still felt it my responsibility to speak to my clients individually.

For those clients who had a fraudulent return filed, the IRS required that taxpayers send in a form 14039 with picture ID to certain IRS centers. This required paper filing and mailing by our staff. Victims were advised to go to their local police department and file a report. This sent a red flag to the local newspaper when they saw a large number of ID thefts being reported. Victims needed to call the IRS directly. This resulted in our clients spending a great deal of time on hold with the IRS. Depending on which IRS agent they spoke to, they received different advice instructions, making it very confusing in certain situations. Tax returns needed to be paper filed with form 14039, and picture identification attached. This created additional time with copying and mailing and walking clients through the new process.

We advised clients to contact the Federal Trade Commission and the Social Security Administration. We advised our clients to register with the Social Security Administration; in case there was any activity or claims to their social security account, they would be notified if they had properly registered. Except for one unique case, none of my clients met current Taxpayer Advocate Case criteria, so the Taxpayers Advocate Office could not help me or my clients. The IRS, at this point in time, had no specific liaison for me to work with. Fortunately, there were several IRS personnel that were invaluable in our firm's survival.

What steps have we taken? Computer passwords were increased to at least 12 alphanumeric symbol characters. If a password is typed in incorrectly more than three times, our computers shut down. All taxpayers have individual passwords in the tax program. Our computer passwords are changed every three months. Firewall, antivirus, malware programs are updated by our IT firm regularly. We even installed motion detectors in our offices, and new locks at our office. All information sent to clients over the Internet that contains any type of personal information is encrypted. Our office computers completely shut down with no access available during certain hours of the day. In our particular case the systems are shut down between 11:30 PM and 5:30 AM. We do not have Wi-Fi in our office.

Besides fraudulent returns being filed, there was also what I refer to as collateral damage. The first related to mortgage applications. In some instances, when the financial institution requested tax information from the IRS, they were provided with the fraudulent return. It would then be necessary for us to write to the financial institutions and provide a copy of the correct return. There were damages that related to FAFSA applications. In some instances, when the college requested tax information from the IRS they were provided with the fraudulent return. It would then be necessary for us to write to the college and provide a copy of the correct return.

In many cases, client's overpayments that were to be applied for the following year were either refunded or improperly applied. Medicare premiums were affected due to the fact that social security was using information provided on fraudulent returns. A number of our clients received notices from state agencies. The notices were based on the fact that the fraudulent federal returns had been filed and that information had been forwarded on to the state. And in many cases, erroneous estimated tax payments -- tax penalties were assessed.

My final thoughts. In 2012 tax year, we had approximately 400 to 425 fraudulent returns filed. This represented over 50% of our individual tax clients. The 2013 tax year we had approximately 80 to 85 fraudulent returns filed. These were primarily single individuals and elderly people. In the 2014 tax year, which just ended, we've had between five to ten fraudulent returns filed. We are still working with the IRS regarding some clients who have not received refunds mainly due to estimated tax payments being either returned to taxpayers or improperly manually inputted by IRS personnel. We also have some ongoing problems with Medicare premiums.

The hackers were able to get into our computer through firewalls and passwords, and back up all of the data on our tax program without us knowing until it was too late. Make sure you have ID theft protection insurance. This money will be used for IT help, legal fees, ID theft protection, public relations, and additional staffing necessary. Unfortunately, if a hacker wants to get in, they will get in. They're always developing new forms of malware. We need to make it very difficult so they move on to someone else. That's my story and my advice to all of you. I'll turn it over to Shawn Tiller now.

Hello, this is Shawn Tiller. I just want to say thank you to David for coming forward with his story. Sadly, this is a story we in Criminal Investigation see more than you think. You should know that fighting tax-related identity theft at CI is top priority. In the past two fiscal years, CI initiated over 1,800 identify theft-related investigations. During that time, our enforcements efforts resulted in more than 1,500 perpetrators being sentences to prison. The courts continue to impose significant jail time, with the average jail sentence exceeding three years in 2015. One individual was sentenced to over 27-and-a-half years in connection with a tax-related identity theft scheme.

The nationwide Law Enforcement Assistance Program provides for the disclosure of federal tax return information associated with the accounts of known and suspected victims of identity theft with the express written consent of these victims. To-date, over 1,100 state and local law enforcement agencies from 48 states have participated in this program. In FY15 over 6,700 requests were received from state and local law enforcement agencies, representing over 119% increase over FY14. The Identity Theft Clearinghouse continues to develop and refer identity theft refund fraud schemes to criminal investigation field offices for investigation. Since its inception in FY12 it has received over 7,600 individual identity theft leads. These leads involved approximately 1.68 million returns, with over $11.4 billion in refunds claimed.

CI continues to be the lead agency or actively involved in more than 70 multiregional taskforces or working groups, including state, local, and federal law enforcement agencies focusing on identity theft. I'm going to turn this over to Mark to discuss what Criminal Investigation is seeing. I want to thank all of you for the efforts to secure your files and assist us in protecting the tax system.

This is Mark. And I want to highlight some of the tactics being used by data thieves. Let me start by noting that data thieves constantly evolve and you really must be on guard at all times. The easiest way for criminals to obtain PII is to ask for it, and they do this by phishing, and that's "phishing" with a "ph" instead of an "f." There are phishing emails, phishing phone calls, phishing popups, all designed to steal your bank account number, credit card number, social security number, and/or your user name and passwords to financial accounts.

Thieves may send an email posing as your bank, Twitter, PayPal, your best friend, your tax software provider, and even the IRS, or they may send you an email announcing you just won a grand prize. Some emails may target a mass audience. Some hone in on specific groups, such as tax preparers. That's called "spearphishing." The phishing email may contain a link or an attachment and may tell you your bank account needs updating or your password has been compromised and you must create a new one, and it may redirect you to a webpage that appears like it's your bank or even the IRS. It may at some point ask for your social security number or credit card number, or that link or attachment you open may silently be tracking your keyboard strokes, waiting for your username and password on key accounts. Oftentimes, the unsolicited emails contain a malware virus designed to install concealed software, which is used to take control of your computer and/or gain access to sensitive data.

Phishing emails, texts, websites, and phone calls seemingly come in an endless variety. Earlier this year, thieves sent emails impersonating IRS e-Services, specifically targeting tax preparers and asking you to update your accounts. Many of you gave them your user names and passwords. A phishing phone scan making the rounds now leaves an automated message saying the IRS is suing you and gives you a number to call where they will ask for your sensitive personal information or demand immediate payment.

Phishing schemes, especially phishing emails, are a way hackers can gain entry into your systems and scrape away all the PII data you have on all your clients. I cannot stress this enough, never click on a link or open an attachment in an email from someone you don't know or if you think it's your bank or the IRS. No legitimate business will ask for sensitive information in this manner. If you have employees, you must educate them about phishing attacks. The hazards of opening an email from an unknown or suspicious source and the dangers from opening an email from what seems to be a known source with links or an attachment.

The IRS generally does not send unsolicited emails and it will never ask for sensitive information such as a password or SSN. If the IRS Return Preparer Office does send you an email it will contain no links, either just the message or directions for you to go to your PTIN account for a message. It will also have an irs.gov address. If an IRS special agent were to email you, the return address will always include their first name, last name, followed by "@ci.irs.gov." When you hear about a data compromise, one way these occur is because an employee opened an email they shouldn't have and gave the criminals access either through malware or by giving up a password.

I can assure you we are dealing with a different type of criminal than we were just a few years ago. Cybercriminal gangs are real and they are active. They are sophisticated hackers based overseas and

here in the U.S. Maybe you've heard about the Dark Web, that's the part of the Internet that you don't see from Google or Yahoo or Bing searches. It's a place where cybercriminals gather to trade SSNs, credit card numbers, and other sensitive data. They also have their own chat groups where they trade information about how to reengineer IRS processing systems to maximize their thefts. We in CI recently observed two criminals discussing upcoming tactics for filing fraudulent tax returns in 2016. Or the criminals can be even less sophisticated and still have a dramatic impact.

In August, eight people from Georgia and Alabama were sentenced for a wide-ranging scheme that included, among others, stealing the identity of the Fort Benning soldiers who were overseas defending our nation. That's how low these thieves are. They ended up with jail terms of 31 years collectively. Key to their scheme's initial successes was recruiting a postal carrier who ensured the refunds were directed to them, and a Walmart employee who cashed the refund checks.

But as noted in the outset -- excuse me -- but as noted at the outset, the tax preparer and taxpayer are the first line of defense, and the data you hold can be vulnerable in so many ways. The thief may break into your office and steal your computers. Your data can be just as vulnerable to an inside attack, such as from a disgruntled employee, or from a compromised computer, or it can be accidental, such as improperly disposing of an old computer, fax, copier, or paper files.

So how do you make sure you are safeguarding your clients? Where do you even start? Our advice is to make two plans. The first is a security plan. Identify those steps that you are taking and that you need to take to safeguard data. The second is a data compromise plan. If tomorrow thieves steal your client data, what would you do? Ken has more information about how to get it started.

Thanks, Mark, for that overview. The first thing we would urge you to do is to review publication 4557, 4-5-5-7, "Safeguarding Taxpayer Data." That pub is on irs.gov as both an online and as a PDF that you can print and save. This has a checklist that you can and should use to help you build your own security plan. Here are a few things you should consider. You should have a top notch security software that includes a firewall, antimalware, and antivirus programs. Make sure the software is set to automatically update to stay current against the latest threats. And consider having firewalls for both hardware and software.

Here's another important one, educate all of your employees to ensure they understand the dangers of phishing emails and other threats to taxpayer data. Pub 4557 also has several items related to employees such as halting their access to your computer systems when they leave your employment. Create strong passwords that are changed periodically. Consider having different levels of password protection. For example, have one password to access your computer system and have a separate password to access your tax software program or client files. That way, if your computer system is breached, perhaps not all of the information on your system will be exposed.

Secure your wireless connection. If you use Wi-Fi in your office, make sure it is password-protected. This will protect thieves and others from accessing your Wi-Fi, which allows them to see taxpayer data. Encrypted email programs to exchange PII information with taxpayers. Be sure to back up taxpayer data frequently, perhaps on an external hard drive, and ensure that that hard drive is kept in a secure location, with limited access by others. If you keep paper files, make sure they are stored in a secure location. Access IRS e-Services weekly during the filing season and periodically throughout the year to see the number of returns filed using your EFIN. If the number is excessive, contact us immediately at the e-Help Desk.

There are scores of other steps, some easy, some that may require some expenditures, that you can take to better secure taxpayer data. And I want to pause right here to remind you that securing taxpayer data is a federal statutory requirement. You all may be familiar with IRS regulations that require the protection of data from disclosure, but additional federal laws also apply to tax professionals. In the Gramm-Leach-Bliley Act, the safeguards rule requires return preparers to ensure the security and confidentiality of customer records and information. The Act's financial privacy rule requires return preparers to give their customers privacy notices that explain the financial institution's information collection and sharing practices. In turn, customers have the right to limit some sharing of their information.

The Internal Revenue Code IRC 7216.1 imposes criminal penalties on any person engaged in the business of preparing or providing services in the connection with the preparation of tax returns who knowingly or recklessly make unauthorized disclosures, or use information furnished to them in connection with the preparation of an income tax return. Internal code section 6713 imposes monetary penalties on the unauthorized disclosures or use of taxpayer information by any person engaged in the business of preparing or providing services in connection with a preparation of tax returns.

Let's now turn to developing a data theft plan. Developing a security plan should be your first priority, but right behind it is having a plan should you experience a data theft. It's critical that you know what to do so you don't waste any time. There are a number of best practice recommendations on the Federal Trade Commission website, and I'll touch on a few in a moment. But first, we have a new procedure for preparers who experience data loss. Mark, can you explain this new procedure?

Of course. If you experience a data theft or accident, please contact your local stakeholder liaison. These are IRS employees who work on outreach to the taxpayer preparation and business communities. You can obtain your stakeholder liaison contact either from your state association, if you belong to one, or go to irs.gov, search using keywords "stakeholder liaison," and the first item on the search results should be local contacts. The stakeholder liaisons will notify CI, who will review the matter for any potential impact on tax-related identity theft. If there is, the IRS can take steps to protect the individual taxpayers who may be impacted. Of course, you should also always contact your local law enforcement in cases of data theft.

Thanks, Mark. When you craft a data theft plan, be sure to include the stakeholder liaison contact as one of the items. I would urge you to check out the Business Center on the Federal Trade Commission website. Again, FTC is the lead federal agency in dealing with identity theft. Its website has a lot of good information on what businesses, in general, should do. I would especially directly you to "Information Compromise and the Risk of Identity Theft: Guidance for Your Business." There is the link to that page in the IRS factsheet being issued today with this webinar.

Here are a few other steps your data theft plan, based on the FTC advice. You should notify law enforcement. If your local police are not familiar with investigating information compromises, contact the local office of the FBI or the U.S. Secret Service. Again, contact your stakeholder liaison so he or she can contact IRS CI. You should notify affected businesses. For example, you may want to notify the major credit bureaus that a data theft involving SSNs has occurred, and you will be recommending your clients place fraud alerts on their accounts.

And you should notify the individuals. This is the hard part, but the earlier you notify clients about the data theft, the faster they can take action to mitigate any damage. You should also consider these actions. Discuss the notification timing with law enforcement to avoid impeding the investigation. Designate a person within your firm responsible for releasing information. Communication is critical. The FTC has a model letter that you can use as a template to notify clients about the data theft. In your notice to clients, describe what you know about the compromise, including how it happened, what information was taken, and what actions you have taken to remedy this situation. There are additional steps you can take, such as offering free credit monitoring for clients. Again, IRS publication 4557 is a great resource and it has the web addresses to the key FTC pages I've mentioned here.

We need to start wrapping up here. I want to briefly go back to something Commissioner Koskinen mentioned, you and your clients are on the frontlines of defending PII. You will see the IRS being more aggressive in educating taxpayers about the need for the latest computer security technology to protect all their online activities. We would urge you to help us in this campaign. Starting in November, we will begin an awareness campaign. We will be sharing numerous tips, articles, and security ideas with taxpayers. We hope that you will think about online security before they start the holiday shopping season. This will be an ongoing awareness campaign up to and during the 2016 filing season. We would urge you to share the security information with your clients as well. Again, publication 4524 is a good source for your clients. Mark, any final thoughts from you?

Thanks, Ken. I just want to reiterate, I can't stress enough the importance of having a security plan. And you must regularly review and regularly update that plan. You must keep on top of the latest security technology to be safe. Also, this must be a priority for everyone in your firms, not just you. If you have employees, please educate them on ways thieves can use phishing techniques and spam emails to trick them into turning over sensitive information. Again, if you do have a data theft, contact your IRS stakeholder liaison. Contact information found on irs.gov by using keyword search "Stakeholder liaison." Dave, let me bring you back into the conversation. Do you have any final words of advice for our listeners?

I know some of you may think that this will never happen to you, and that is exactly what I thought, but it did. And it was devastating both personally and professionally. I would just like to remind everyone of what I said earlier, discuss cyber breach insurance and identity theft protection with your insurance carrier. Have a data theft plan in place. Make it as difficult for hackers as possible by adding security to your business. Modify computer passwords and the number of times someone can try to access your computers. Give all your clients individual passwords in your tax program. Change your passwords every three months. Consider having passwords as long as 12 alphanumeric symbol characters. Update your security software and hardware regularly. Encrypt all your information sent to clients. Look into changing the hours your computers are available during the day. It's better to be safe than be sorry, take my word for it. Now I think Shawn has some final words.

David, thank you again for sharing your story and for those tips. This is Shawn again, and I just want to summarize what we've all said here today. First and foremost, the threat is real. Make a security plan, that's number two. And number three, create an action plan in case of data compromise. And number four, contact your local stakeholder liaisons if you have a data compromise. Again, fighting tax-related identity theft is CI's top priority, and we want to keep the tax practitioner community aware of what everyone in IRS is doing to prevent it before it starts, and assist you when it happens.

Thanks to all of you for sharing those important points. For those of you who are joining us, there are resources available to help you if you have a data security breach, as mentioned throughout the presentation and on this slide. Publications 4557, which is "Safeguarding Taxpayer Data," and 4524, "The Security Awareness for Taxpayers," they contain information for you and your clients. And irs.gov also has information by using search words "Identity theft."

This concludes the broadcast portion of the webinar and we thank you for watching. Ken, Shawn, Mark, and David are standing by and ready to answer your questions. If you would like to submit a question, select the "Ask Question" button under the photo window and click the "Submit" button. And, again, I am Gerry Kelly-Brenner, one of the stakeholder liaisons that Mark mentioned in reference to the new procedure for contacting the IRS if you experience a data theft. I will be moderating for the Q&A portion of the broadcast, and so far we hope you have found today's webinar helpful and informative. Thanks so much to all of you, Ken, Shawn, Mark, and David, for staying on to answer the important questions that we've received.

Ken, the first question has to do with paper versus e-filing. Would it be safer to file paper returns versus e-file returns in this data theft era?

No. Thank you for that. Absolutely not. E-file is safe and secure. The IRS has processed more than one billion tax returns over the past couple of decades safely and securely. E-file is still the best way to file your return.

Wow, one billion. Oh, my goodness, I guess we have a record going there, huh, Ken?

Absolutely.

Ken, there seems to be some confusion as far as IP pins are concerned the identity protection pins. First of all, a taxpayer is a victim of identity theft and a person files a return that year, and then the next year

the person gets an ID pin, or excuse me, in this particular case is an IP pin I think is what the person means.

Yeah.

And is able to e-file. Then how many more years will this be required? Will the person need a new IP pin each year?

Yes. If your client has an IP pin or identity protection pin, a new number will be issued each year prior to the start of the filing season. We mail those IP pins to taxpayers as a part of the CP01A notice process.

CP01A, is that what you said?

Yes, that's correct.

Okay. And they'll be getting it by mail; is that correct, Ken? They're not going to get an e-mail.

That's correct. It will not be in e-mail, it will be in the mail.

Okay, perfect. So they should be looking out for the mail then and not for an e-mail.

Shawn and Mark, there are a lot of questions. Apparently a lot of people are concerned now about what to do about encrypting their hard drives with passwords. Can you give them any specific guidance as far as should they be swapping our their hard drives for encrypted hard drives? Would that be a good recommendation to stop any hacking?

Well this is Mark, and first and foremost the only thing we can do is recommend to you to have a good security plan with IT security. There are a number of firms out their publicly. The Federal Trade Commission website has some options. There's other alternatives with your trade groups, but we in IRS don't specifically identify a particular product or item to use but would only recommend that you seek the advice of a professional IT security specialist.

Okay. And in doing so, that person is an expert. We have a lot of experts on our session today. They're so good at what they do. But, really, what I'm hearing you say is to recommend that they seek out a security specialist, someone who really knows what they're doing to assist them in protecting them and their clients.

That's correct.

Okay, thank you so very, very much. Ken, there are a few questions here about clients not receiving refunds after a year or two of being worked in the IDT victim assistance. Can you comment about that?

Yes, I can. You know, generally most cases filed this year have been resolved within 120 days. You should also know that this year we have realigned and centralized our identity theft victim assistance work under one leadership team. We believe this will make us more efficient. You should know that at this time we are taking a soup-to-nuts look at our victim assistance process and hope to make changes to reduce the timeframe.

You know, I would say if you've got clients who still have not received their return to be processed or their refund issued, and it's been beyond that timeframe, you know, I would say reach out to IRS and talk with someone here so we could work on those individual cases.

When you say "beyond that timeframe," are you talking about the 120-day timeframe, or is there another timeframe, Ken, that you would recommend?

No, generally if it's been more than 120 days, I would say reach out to the IRS.

Okay. Is there anyone in particular that they should reach out to, or any particular team?

You know, I'd have to get back with you on that. I mean I believe you can either do toll three or the 1 (800) 829-1040 number and they'll be able to direct you to the right person in the IRS.

Okay. Thank you so very, very much. David, there are lots of questions here for you. First of all, they're wondering if you had an IT person, do you think that the IT person would have discovered what you found before the four months?

Well we had an outside IT firm. What Homeland Security indicated to us was that when the breach took place, that when our tax program was downloaded, he went back, he then deleted it and made it extremely difficult to determine that anyone had actually even been in the system.

Wow. So they were really experts at what you were doing is what you're saying. The IT person could not have necessarily have protected you at that point.

Not at that point.

Or had figured it out before you discovered it.

That is correct.

Okay. We have practitioners who are wondering if there are any measures that you're still regretting that you didn't put in place, or anything that you're still working on to put in place even now?

There are some steps that we're considering. For example, we had a meeting with our IT people last week, and they suggested that any Internet search-type questions that I or my staff may have, i.e., going to Google or something of that nature, that we have standalone computers that we use those computers just strictly for that, nothing that could tie back into our server or any other programs, any of our individual computers. So it's a work in process. We're constantly meeting with our IT people, and they are giving us additional suggestions.

You say it's a "work in process," because unfortunately just as soon as you think that you get ahead of the game, unfortunately there are those who are just that much one or two steps ahead.

That is correct.

And, Ken, how do I check EFIN status, weekly during the filing season? Where is that?

Sure. Your EFIN numbers are updated weekly in your E-services account. If you notice an excessive number then you should contact the E-help desk. You can search irs.gov using keyword "E-helpdesk" for the toll free number.

Okay. So then, again, that's on irs.gov, and they put in E-helpdesk; is that correct?

That's correct, E-help and then desk, E-helpdesk.

Oh, okay. Okay, perfect. Thank you so very, very much. Here's another one for you, Ken. I called a practitioner's hotline a few days before October 15th because we had not received several E- file rejection notices due to the fact that the taxpayer SSNs were apparently on a return that had already been filed by the IRS. I know that we need to file paper file, but can you clarify if form 1403 is required to be filed in these cases versus whether it is strongly recommended to be filed?

So the form 14039 is the identity theft affidavit. And, you know, we strongly encourage that if you have a client whose return is rejected and you are filing a paper return because another return has already been

filed under that client's social security number, that you do attach the 14039. You know, it lets us know to take certain steps to protect your client's account, and it also allows us to work with you and work with that taxpayer so that we can get the right taxpayer, your client, the refund or that's do.

You can file the 14039 with the paper return and just follow the directions on the 14039 exactly, and that will get our attention and put it in the right treatment stream here at the IRS.

So it really sounds like it's quite beneficial to them, that it really puts the person on record.

Absolutely. Absolutely.

Perfect. Thank you. Shawn and Mark, is having passwords on Wi-Fi, is that sufficient?

This is Mark, and I wouldn't say a password on a Wi-Fi is your only sole security technique. I might push that over to Dave. But certainly having a password on your Wi-Fi is critical, because I can't tell you how many data thieves would take your information if you don't have a password-protected Wi-Fi system. That's like basic data theft that even an elementary data thief could do, so I would highly recommend having a password on your Wi-Fi.

But I would also suggest, much like David talked about dealing with his IT folks, different things and techniques to use to protect the data. I don't think just a password on your Wi-Fi is going to protect you from all these problems that we've discussed today. Dave, anything to comment on that?

Our firm has elected not to utilize Wi-Fi, and when you talk about e-mail addresses, in my meeting in the last couple weeks with my IT people, they actually suggested that we not include on our website the e-mail addresses of our employees because the hackers utilize that information to send bogus e-mails to you under the pretense of a question that they have, and obviously they attach viruses to those e-mails.

Wow, I had not heard that before. Thank you so much for sharing that. I'm sure that that will be best practice many will put in place. On the one hand, you want so much to be able to have the connection and the communication. On the other hand, you have to protect yourself as well. Thank you.

Ken -- excuse me, no, Mark and Shawn, we have some questions here about wondering if you just shut down your computer every night will that stop access?

This is Shawn. They wouldn't really -- this is Shawn, they wouldn't really have access. The big issue that we continuously see is when they -- through fishing, where they send you an e-mail and someone hits upon a URL that gives them access, like a Trojan horse concept. But that's the most common that we see.

So it's really not so much shutting it down at night or whenever during the day, but it's also what happens when the computer is actually on.

True. So the encryption thieves that both David and Ken discussed is a very smart idea, and also sending e-mails out to your clients, and then just minimizing the personal use that you have on your work computer to not open opportunities for the fishing, if you will.

Well thank you for sharing that. Ken, it sounds as though there is some question about IP pins and whether they're getting the same IP pin or keeping the same IP pin forever and that the letter that's being sent out is just reminding them to use the same one year after year after year, or if it's really that they're getting a new IP pin each year.

They are getting a new IP pin each year, so the IP pin is changing each year.

Okay, thank you for clarifying that, because we had several questions about that. All right.

Yeah.

David, was any of this attributable -- of course, Ken said that on our side, meaning the IRS's side, that E-filing is safe and secure. Do you feel that -- were you mainly E-filing your returns? Do you feel that in any way, shape, or form, because you were E-filing your returns that this had happened to you, if it had been paper, that you would have been any safer?

Our breach was not attributable to E-filing our returns, and we probably filed 99% E-file, 99% of all of our returns prior to the breach. But I would not say that it was attributable to E-filing by our firm.

Okay, thank you for clarifying that. You mentioned though, David, that your files are now encrypted as a result of your data breach. Can you explain specifically what you mean by that? How exactly are you encrypting your files without giving out too much information that might be --

Well our files, when I'm using the term "encrypted," our files were encrypted prior to the breach. They were password protected when a lot of our clients will ask us to send them data or information over the Internet via e-mail, they request that we use a password, in many cases, the last four digits of their social security number, and we will not do that anymore. So we establish a password and we encrypt what we're sending with that password, and we ask the client to call us on the phone and request what that password is. And that's how we transmit all our data now.

Thank you so much. That's great information. Many others have probably put something similar in place, but it's good to hear it from you. Ken, going back, again, to the IP pins, there are practitioners are wondering that if a person has an IP pin, can they opt out once they've used it for a few years?

So this is Ken again, and at this time clients cannot opt out of the IP-pin process. We are looking at it. But as of now, and for the near future, once you're in the IP-pin program, it is not optional for years after that. But we are looking into it.

So it's not until the IRS actually tells you that you're no longer needing to use the IP pin?

That's correct, yes.

Okay, perfect. Thank you so much. Ken, another one. Why does the IRS use the full social security numbers and not the last four of the social security numbers?

So the IRS has historically used the full social security numbers as a part of how our systems were originally established. We are now in the process of working on masking social security numbers on our notices and in our system. We've made tremendous strides in changing a lot of our collection and balance due notices that have been sent out that now have masked or partial SSNs on them, but we are working on updating our system so that the full social security will not be required.

So when you use the term "masking," what exactly does that mean? What would someone see on their notice?

So masking on your notice would potentially be the last four digits of your SSN or maybe the two middle digits and then the last two digits. Masking means that we don't use the full SSN but maybe one or two or three characters of your SSN on the notice so that we can validate it.

So, again, we're going additional steps to try to protect the taxpayers as well.

Absolutely, yes. Thank you. Shawn and Mark, is faxing information more secure than e-mailing?

Assuming that people still have fax machines.

Okay.

I honestly don't have that deep knowledge on fax machines. Do you have anything to add with that, Mark?

I believe it's secure, but you also have to remember that once you get an incoming fax, if it prints you've got to somehow do something with those documents, because as we spoke earlier, you know, just some offices that I've seen, you know, they'll, once a year, clean out all their old files, throw them in the dumpsters. If somebody were to get those, a lot of times there's fairly sensitive financial data on those documents. So I would just caution anybody to make sure that they burn or shred or have document disposal services that would secure that type of information from being getting into the wrong hands.

Or even checking the fax machine to see if a fax has come in, something even as simple as that. Ken, if a refund was given by fraud to whoever, will the taxpayer still receive their refund?

So the answer to that is, yes. Once we've got through the victim assistance process and we work to reconcile the account, I mean it is our due diligence to make sure that we get the right amount of money to the right taxpayer. So we'll work with them to do that.

Okay. So it will take longer but at least, ultimately, the correct taxpayer will receive the refund then.

Yeah.

Okay. Thank you so much. David, this person says, "I may have missed it. Did you give the root cause for what eventually led to the breach? Maybe it's good to repeat that one more time. They were able to log into our systems through a remote access program.

That sounds so simple, and yet it made so much damage.

That is correct.

Wow, I'm so sorry about that. Shawn and Mark, is there any outreach to police departments to get them on board with what's taking these ID theft -- about taking the ID theft reports. It says, "My local police department has told two of my clients that they can't do anything about it." Is there any kind of outreach with the police?

Yes, this is Shawn. So we have worked with many organizations with the National Association of Attorney Generals is one, the International Associations of Chief of Police, and others to essentially share our LEAP program, our Law Enforcement Assistance Program that I mentioned earlier in our broadcast, to really educate them about the issue and also give them tools to help them.

Many -- probably most states have laws in place ensuring that local law enforcement agencies take a police report, because many times dealing with identity theft, as a victim, you have to have a police report. So, although the venue of where that occurred, the victims might be spread across the United States, and many situations the suspect is overseas perhaps. So, again, most state haves that law. I would argue whatever state the folks are in, you might look up the law "reporting identity theft." Do a Google search and find that, because there more than likely is a law that requires them.

And understand that local police departments are held to a standard of police statistics and they don't like numbers to go up, even though the crime probably did not occur in their local area.

That sounds like there's more and more outreach and more and more partnering, really, to battle against this.

True. The identity theft boom essentially started in the mid '90s, and IRS is seeing it now. So most police departments are knowledgeable about different kind of schemes, but, again, taking that report takes time,

and they don't like to impact their criminal statistics in their local area. But, again, check the local law. I would argue that most states, if not all, have that law in place.

Thank you. One more for you, Ken. Question here about why not just delay refunds until fully matched returns and not issue any refunds at all until everything's been matched?

So there are a lot of challenges with that question. The first one being that in legislation, if we at the IRS delay refunds over 45 days, we are required to pay interest on those refunds that take longer than the 45-day due date of the refund or when the return is filed. We are working with congress and our legislators to get the information sooner, and working with changes that we could do to our current tax code that would help in that effort. And, you know, some states may be able to apply that at a state level to their return process, but unfortunately for us right now, we are not in a position to be able to do that.

David, one more for you, having to do with your client's reaction. What was your client's reaction to the data breach? Were you able to retain most of your clients going forward? I think many practitioners heard what you went through and are suddenly realizing, "Oh, my gosh, if I went through that what would happen to me? Would I end up having to shut my doors?"

Well it's two-and-a-half years later, and we're still in business. But certainly it was a tremendous struggle. Of our roughly 800 individual tax returns that we would have done in 2011 year, and that's the year's program that was backed up, I would say that we probably lost probably less than 20 of those clients in the two-a-half years since then.

20 out of how many?

Over 800. A little over 800. Wow. So you had built up faith and trust long before.

It was 30 -- yes, we had a very personal relationship, but I will say this. These are conversations that you are gut wrenching to have with family, friends and clients that you've had for 30 years or more.

Oh, I can't even imagine. We have so many amazing questions, and this is such an important topic. But unfortunately that's all the time we have for questions today. Before we close today's broadcast, are there any final remarks that any of you want to make; Ken, Shawn, Mark, David, anything else that you want to add?

This is Ken. I would just say, you know, listen the experiences you heard here on this call. You know, take our advice about coming up with the plan and being an active participant in educating the taxpayer about identity theft.

And as you said, Shawn, those four points, that threat is real and make a security plan, number two, and number three, create an action plan in case your data is compromised, and, of course, contact your local stakeholder liaison if you have a data compromise, which, of course, stakeholder liaison. Your local stakeholder liaisons can be found by keyword search on irs.gov at stake holder liaison. Anyone else want to comment, have any final words?

This is Mark. Just one thing to one of the questions Ken answered briefly about waiting for all the matching data and holding off for a refund to go out. One caution I would advise everyone on the audience is, one of the reasons we're targeting the return preparation community to be on the alert and be safeguarded is if somebody has your client's last year's return and that return is somewhat consistent and they have all that data, they are going to be able to generate a return that is going to mirror their actual return, which makes it that much nor difficult for IRS to filter that out and identify it. So we appreciate your due diligence, and hopefully we walk away from this with you folks having a plan to have a security plan and we're happy to work with you and continue this battle, and that's all I have. Thanks.

Thank you, Mark. David, any points you want to make? No additional points at this point in time.

Okay. I know when we were talking earlier, you had mentioned that working with the IRS was very, very beneficial to get you through all of this.

If it had not been the help of several individuals inside the service, I'm not sure that our firm would still be here today. I say that sincerely. Sincere thanks to all those individuals.

Thank you so much for sharing that. Wow, and thank you so much, for all of you watching our webinar today. We hope you learned a few best practices to assist in better protecting taxpayer data and if you experience a data theft loss or refund fraud, what you can do to overcome it and how the IRS can help.

If you have any question that is were not answered today, please visit the IRS website at www.irs.gov, using key words "identity theft" to access the identity protection, prevention, detection, and victim assistance site containing numerous resources. And if you're participating to earn credit, no further action is required. Certificates of completion will be issued to those who qualify, and they will be e-mailed in approximately two weeks from the date of this broadcast. And in case you would like to review this information again or refer someone who was not available to view the webinar today, it will be posted in approximately three weeks in the IRS video portal at www.irsvideos.gov.

As you exit today's webinar, you should get a pop-up box with a survey regarding this presentation. Please take a few minutes to complete the webinar survey. While participation in the survey is optional, your feedback will help us in developing future webinars. And in case you do not receive the survey, you may need to disable your pop-up blocker.

Thanks again for your time and attendance. And as Commissioner Koskinen said, together we have a chance to achieve our goal of protecting taxpayers. Have a great day.

Thank you. This does conclude today's webinar. We thank you for your participation. You may disconnect your lines at this time, and have a great day.