Our presenters are Kelly Moening and Dale Forrester. Please, take it away, Dale.

Dale Forrester: Hey. Good morning. My name's Dale Forrester. I'm the –

Special Agent in Charge in the TIGTA Cyber Crime division looking at abuses of the IRS external portals mostly, and I'm excited to talk to you today. Kelly?

Kelly Moening: Hello. My name is Kelly Moening. I am the Special Agent in Charge of the Great Lakes Field Division here at TIGTA. Prior to joining TIGTA, I worked as a special agent with IRS Criminal Investigations for 12 years where I investigated and prosecuted individuals including tax preparers and attorneys for tax violations, including tax evasion, and money laundering and bank fraud. Next slide, please.

Today, our webinar will define TIGTA's role in protecting the integrity of tax administration, clarify TIGTA's main components, discuss preparer ethics and misconduct issues, and discuss scams and cyber fraud activity targeting tax professionals. Next slide.

What is TIGTA? TIGTA is an acronym for the Treasure Inspector General for Tax Administration. We provide independent oversight of the IRS, protect the integrity of federal tax administration, detects, and prevents waste, fraud, and abuse at the IRS. We have three primary operating divisions the Office of Audit, the Office of Inspection and Evaluations, and the Office of Investigations. Next slide.

The Office of Audit promotes the economy efficiency and effectiveness of tax administration. It provides recommendations to improve IRS systems and operations and to ensure the fair and equitable treatment of taxpayers. And audit recommendations result in cost savings, increased revenue protection, protection of taxpayers' rights and entitlements, and more efficient use of resources. Next slide.

Here are some examples of TIGTA audits. The IRS processing of Economic Impact Payments. They alerted the IRS of EIPs that had been issued to potentially ineligible individuals.

In response to our alert, the IRS added instructions to IRS.gov to inform these types of individuals of their ineligibility and the need to return these payments, including the process to be followed. As of October 1, 2020, individuals voluntarily returned 65,477 payments totaling more than $80 million. IRS compliance efforts regarding high income taxpayers recommended that the IRS emphasize the use of income information to identify high income taxpayers who have the ability to pay their delinquent taxes, establish high-income balance-due cases as a higher collection priority, and develop a strategy for working high-income balance due cases. Also, that the IRS implement controls that will assist to identify and prioritize high-income non-filers who are repeat offenders.

IRS strategy for gig economy workers determine that almost $481 million in self-employment taxes could have potentially been assessed if the IRS had a strategic plan to address gig economy taxpayer noncompliance. Next slide, please.

This is our first poll question. "Which of the following is not an auditable area for TIGTA Office of Audit? A Effectiveness of IRS strategy for gig economy workers; B – Efficiency in processing Economic Impact Payments; C – Efficiency in processing small business administration loans; or D – Effectiveness of tax exempt and government entities operations?"

And it looks like we're pretty evenly split between options C and D. Back to the presenter.

Kelly Moening: The answer to poll question number one is C – Efficiency and processing small business administration loans. Next slide.

Our Inspections and Evaluations Division provide factual and analytical information, assess the effectiveness and efficiency of programs and operations, and inquire into allegations of fraud, waste, abuse, and mismanagement.

These reviews often result in recommendations to streamline operations, enhance data quality, and minimize inefficient and ineffective procedures. Next slide.

Here are some recent inspections and evaluations. The *Oversight of Reported Sexual Harassment Allegations Needs Improvement* from March of 2021. The objective of this evaluation was to review the IRS's tracking of reported sexual harassment allegation, the investigation or inquiry into the alleged harassment, and the discipline of IRS employees in substantiated allegations.

TIGTA found that sexual harassment allegations were not reported to the IRS's Anti-Harassment Program in accordance with guidance issued by the Equal Employment Opportunity Commission that there was no consistency or standardized approach to document management investigations, or the investigations overall findings conclusion, and recommendation.

We made a recommendation to the IRS that it revise its policy to ensure that all sexual harassment allegations are reported to the Anti-Harassment Program and develop a system that centrally tracks all allegations of sexual harassment. Another inspection and evaluation was *The IRS Leveraged Its Telework Program to Continue Operations During the Covid-19 Pandemic,* March 2021.

The objective of this review was to determine whether the IRS effectively used its telework program to reduce the impact of the Covid-19 pandemic on IRS operations. We found that the Covid-19 pandemic began to have a significant impact on IRS operations in mid-March 2020. Between March 14th and March 28, 2020, the number of employees who worked any amount of time at IRS facilities declined from about 70,000 to 19,000 and the number of employees who teleworked any amount of time increased from about 27,000 to 41,000.

By March 28, 2020, the IRS placed nearly 35 employees on paid weather and safety leave because they could not work in IRS facilities or telework during some of the portion of the 2-week period. Between April 2020 and the end of September 2020, the IRS steadily increased telework participation and reopened facilities to some employees. By September 26th of 2020, almost 60,000 employees teleworked a portion of the week while approximately 25,000 employees worked from an IRS facility for a portion of the week.

For this same week, approximately 6,700 employees reported to time and weather safety _____. TIGTA made no additional recommendations on this report. The final report was *Controls Over the Pseudonym Program Need Improvements,* from June of

2020. A pseudonym is a fictitious name that IRS employees can use to interact with taxpayers. The object of this evaluation was to determine whether the IRS has established policies and procedures to manage its pseudonym program effectively. We found that the IRS could not provide adequate documentation to support the justification for issuing pseudonyms to 51 percent of the employees included in our statistical sample. The IRS could not provide documentation to support that a manager approved the use of a pseudonym for 43 percent of the employees included in our statistical sample. Next slide, please.

Now, we are to poll question number two. "The Office of Inspections and Evaluations identifies potential reviews based on A – Emerging issues likely to affect tax administration; B – Congressional inquiries; C – Discussions with IRS executives –

members of Congress and their staff, and Department of Treasury staff, or D – all of the above?"

And it looks like just about 95 percent said D. Back to the presenter.

Kelly Moening: The correct answer to poll question number two was D – all of the above. Next slide, please.

The last office of TIGTA is the Office of Investigations, which is where I'm employed. We identify and investigate IRS employee misconduct.

We protect the IRS from external threats and corruption. We protect the integrity of IRS programs, operations, critical infrastructure, and detect and prevent waste, fraud, and abuse. Next slide.

Disclosure restrictions. As a component of the Treasury Department with tax administration duties, TIGTA is bound by Title 26, United States Code Section 6103 -the Tax Information Confidentiality Law. Section 6103 prohibits the disclosure of tax returns or tax return information, except as authorized by an exception contained in the statute or as made public record in a tax administration proceeding. Next slide.

Ethics and integrity. Ethics defined a set of moral principles, a theory or system of moral values. Integrity firm adherence to a

code of moral or artistic values. Incorruptibility meaning always doing the right thing, even when no one is watching. Next slide.

Circular 230 also known as Subtitle A, Part 10 of Title 31 of the Code of Federal Regulations sets forth rules under which tax preparers can represent clients before the IRS. And the IRS's Office of Professional Responsibility otherwise known as OPR oversees most preparer conduct. Next slide.

Preparer Misconduct Examples. False statements on an IRS Form 2848 – or the *Power of Attorney and Declaration of Representative failure* to disclose that preparer is a disbarred or otherwise unauthorized to appear before the IRS. Next slide.

Sending e-mails or fabricating documents purporting to be from the IRS. Improper disclosure of a client's tax information. Fraudulent levy releases and/or unauthorized disclosure of protected tax information. Next slide.

So, here's an example of one of the cases that was prosecuted by TIGTA. On December 14, 2020, a tax preparer was sentenced to two years imprisonment for conspiracy to defraud the United States. He was initially charged with aiding the filing of a false tax return, and conspiracy to defraud the United States. The tax preparer added false income information such as wages, fictitious businesses and erroneous tax credits to his client's tax returns without their knowledge or consent. The tax preparer kept a portion of the fraudulent tax refunds for himself. Upon learning the IRS froze several of the client's tax returns, he furthered the conspiracy by filing a complaint with TIGTA. The tax preparer was sentenced to 24 months imprisonment, 3 years of supervised release, and ordered to pay over $110,000.00 in restitution. Next slide.

The Volunteer Income Tax Assistance Return Preparers Indicted for Defrauding the IRS this is another example. On December 9, 2020, 2 tax preparers were indicted for jointly conspiring to commit wire fraud and wire fraud in connection with the submission of a false application to the IRS for the Volunteer Income Tax Assistance VITA Grant.

The tax preparers applied for and was awarded a grant for $50,000.00 from the IRS's VITA program. Upon review, it was discovered that taxpayers provided false information in their VITA

grant applications, failed to disclose a relevant, personal relationship, and submitted fabricated receipts and volunteer logs to the IRS. If convicted, both tax preparers could individually receive a statutory maximum penalty of 30 years imprisonment and/or a fine of up to $1 million. Next slide.

Here's an example of a tax preparer sentenced for wire fraud and theft Economic Impact Payments. On February 24th of this year, a tax preparer was sentenced for wire fraud related to a scheme to defraud the IRS and obtain money by filing fraudulent tax returns. The tax preparer had previously been indicted on June 18, 2020, for wire fraud, theft of government money, and aggravated identity theft. The tax preparer allegedly unlawfully obtained personal identifying information PII of individuals which included their names, birth dates, and social security numbers from his employer and other sources. The tax preparer also unlawfully obtained IRS electronic filing numbers assigned to tax preparation firms which they were not affiliated to electronically file the returns and claim false tax refunds totally $7,814.00. The filing of the false tax returns also triggered the issuance of Economic Impact Payments totaling $3,400.00. The tax preparer received 6 months imprisonment, 3 years of supervised release, and was ordered to pay $5,800.00 in restitution, and a $100.00 assessment fee. Next slide.

[Break in audio] to poll question number three. "Section 6103 permits the disclosure of tax returns or return information A – Only when TIGTA discloses the information; B – When made public record in a tax administration proceeding; C – only when the IRS gives permission to disclose the information; D: Never; or E –

None of these."

And it looks like just about 45 percent of us said

B. Back to the presenter.

Kelly Moening: The correct answer to poll question number three is B – when made public record in a tax administration proceeding. Next slide.

The IRS Impersonation Scam. It is one of the largest telephone scams. Calls have been received by taxpayers in every state.

The callers claim that the taxpayers owe taxes and must pay immediately, and in many cases, the callers are aggressive and threatening. Next slide.

TIGTA's approach. TIGTA is dedicated to educating the public to prevent fraud against the IRS and to protect taxpayers. PSAs are available on YouTube in English and Spanish and advise and disrupt strategy created to help combat the impersonation scam. Next slide.

The Traits of Scam Callers. They may know information about the intended victim – such as digits of a social security number, address, banking information. They may spoof caller identification information to appear on Caller ID as if they're calling from the IRS. They may demand payment via wire transferred or a pre-paid money card such as Green Dot, iTunes, MoneyGram, or Western Union. They may send bogus IRS e-mails to legitimize the scam, and they may follow-up with subsequent calls claiming to be the police, the Department of Motor Vehicles, or the IRS to verify initial debt claims and confirm threatened legal action. Next slide.

This slide presents a map where you can see the losses by state. The states that are highlighted in red are all states that have reported losses over $2 million. Next slide.

Here are some examples of IRS impersonation scam investigations. On November 30, 2020, telemarketing call center owner and director plead guilty in Eastern District of New York to conspiracy to commit wire fraud in connection with a fraudulent scheme directed at thousands of individuals in the United States. October 24, 2020, man and Voice Over Internet protocol provider were indicted in the Northern district of Georgia in connection with facilitating the passage of tens of millions of scam calls to American taxpayers on behalf of phone scammers. July 9, 2020, a man plead guilty in the Northern District of Georgia for his role in a wire fraud conspiracy to defraud US citizens. He uses approximately 15 false identities to pick up wire transfers in multiple states from victims of the scams. May 28, 2020, a woman was indicted in the District of Oregon with bank fraud while on pre-trial release for other federal offenses. She created a fictitious IRS identity to conceal her role in a scheme to defraud a former employer by stealing more than $1 million over several years. July 2, 2020, a woman plead guilty in the District of Nevada to

conspiracy to commit wire fraud and aggravated identity theft for her role in a scheme. She admitted to being a leader in the conspiracy, recruited at least 10 additional runners and directed others to recruit more. Next slide.

Other Impersonation Scams. The "Lottery" scam. On March 11, 2020, in the District of Connecticut, 5 individuals were charged in an 11-count indictment for their roles in defrauding elderly victims of more than $4 million. Some victims were told that they had won the lottery but that they must send payment for taxes and other fees before receiving their winnings. The defendants could each face 10 years or more for imprisonment for each count. Next slide.

Some of the other impersonation scams false IRS websites on the internet, a hyperlink on a spam e-mail, and also, phishing. Next slide.

Dale, I'm gonna turn it over to you now.

Dale Forrester: Thanks, Kelly. Morning, again. Dale Forrester of Cyber Crimes. This is a common theme here, as Kelly was mentioning, just before every – everybody's probably been impacted by the calls and the impersonations and that has taken on in electronic format. This example in this slide is a violation, essentially of 31 USC333, which is a misuse of the Treasury names and symbols. It is unlawful to use even the words "Department of Treasury" or any of their bureau or offices or title of an officer, such as the Secretary of Treasury, or to impersonate any employee of the treasury in part of any type of scheme like this. So, it's so very important because of the easily proliferation of e-mail that you pay careful attention to who is sending you e-mails and what the actual "Reply to" address is on the e-mail, I believe. In this example, as you can see, it looks like it comes from the IRS. It uses a Treasury symbol, but you are replying to someone else. So, it's critically important to pay attention to that sort of thing as you will probably be inundated, as tax professionals, with this type of phishing exercise.
Next slide, please.

Steps for handling suspicious IRS e-mails are firstly, to not respond and then, on this slide, forward that e-mail or e-mails to phishing@irs.gov. My division works closely with that department and the IRS, and we have access to all of your reports, and we will frequently reach out, following up with you about such reports on phishing – different websites that you report or e-mails. If you have questions about whether or not the call you're receiving from

us is legitimate, that's perfectly acceptable, and we encourage you to question us and to follow-up by hanging up with us, calling us back, or requesting someone in person to contact you.

Step two is to delete the e-mail then from your computer and do not reply, open any of the attachments that could be malicious, or click on any of the links inside that e-mail. Next slide, please.

We're on to our fourth poll question. "Which of the following are traits of a scam caller? A – May have information about the intended victim such as digits of a social security number, address, banking information, *et cetera*; B – They may spoof caller identification information to appear they're calling from the IRS; C – They may follow up with subsequent calls claiming to be the police, the Department of Motor Vehicles, or the IRS to verify initial debt claims and confirm threatened legal action; D – They may demand payment via wire transfers or pre-paid money cards such as Green Dot, iTunes, MoneyGram, or Western Union –

or E – All of the above." And it looks like –

99 percent of us said, "E". Back to the presenter.

Dale Forrester: Thank you. Yes, 99 percent of you are correct. E – All of the above – is the correct answer. Next slide, please.

As you may well be aware, there's no shortage of scams, the newest of which surrounds the many programs put out by the government to support victims of the coronavirus and those who have been impacted economically due to the coronavirus. So, our next slides will be talking about kind of, you know, touch on those. There's a wide breadth of those covering many programs or many government agencies so, it's important to be aware and at least be cognoscente that they're out there. Next slide, please.

The IRS's Role in the Coronavirus Aid.

The CARES Act – or Coronavirus Aid, Relief, and Economic Security Act – was signed into law March 27, 2020, and that provided some relief to American taxpayers through different programs, one of which was through the small business administration, in which case, the businesses that were impacted had to be in existence before February 15, 2020. And so, one of the

biggest things we saw with this scam is an influx in requests for these SBA loans, but then, they're saying that they establish a business by getting an EIN with the IRS. They said that they did that before February 15th, but, in fact, the IRS records will show that many of these were obtained after February 15, 2020, making the entire loan package a fraud. The other more recent coronavirus aid package the American Rescue Plan Act ARPA signed into the law March 11, 2021. That deals with the from our perspective, primarily, the Child Tax Credits, the Advanced Child Tax Credits, and then, the IRS has also implemented a plan to deliver Economic Impact Payments, annual recovery rebates, to eligible taxpayers and individuals receiving social security benefits. Next slide, please.

IRS-Related Coronavirus Scams Need to Knows. The Treasury Department and the IRS will not call, text, e-mail, or mail individuals claiming to offer coronavirus-related grants or economic impact payments in exchange for personal financial information. And the IRS will not request a fee or the prepayment of your taxes to receive a qualifying EIP Economic Impact Payment including the purchase of gift cards. So, if you're contacted with a type of quid pro quo like where someone says, "I'm the IRS. Please, give us something and we'll give you the grant" that's not going to happen. Report it. You can report it to phishing@Irs.gov, or you can just hang up. Next slide, please.

A continuation of some need to knows for IRS-related coronavirus scams are anyone who receives an e-mail or text message or phone call claiming to help get them benefits, you should not respond to those people. Anyone eligible to receive an EIP will have it deposited into their account that is already annotated on their last filed tax return from 2018 or 2019, and anyone whose last filed tax return did not list a bank account, will have a check mailed to their last address of record. Next slide, please.

As you may have anticipated, we've run several coronavirus scam investigations, some of which are the following – one is on May 19, 2020. A man was charged in the Eastern District of Texas with wire fraud, bank fraud, false statements to a financial institution, and false statements to the Small Business Administration in connection with the Coronavirus Aid Relief and Economic Security – the CARES Act. He had allegedly obtained an EIN from the IRS in March of 2020 in order to document a business to use in fraudulent CARES Act-related loan applications, and I believe, in

this case, he actually modified the form after the fact and submitted it to the bank and the SBA saying that the business was, in fact, in business prior to February 15th. Another one is on May 22, 2020. A man is charged in the Western district of Washington with wire fraud and bank fraud in connection with the CARES Act. He obtained EINs from the IRS in April of 2020, so, he obtained the EIN after the statutory cutoff date to document two fictitious entities. He then submitted fraudulent CARES Act related loan applications in the names of these entities. And April 29, 2020, a man was charged in the Eastern District of New York with theft of mail, including multiple EIP payments from the United States Treasury Department, otherwise known as stimulus payments. Next slide, please.

What should you report related to the IRS-related coronavirus scams? You should report any individuals or businesses that purport to be from or working with the Treasury Department or the IRS and ask you for personal information to receive qualifying Economic Impact Payments. Report individuals who offer early check delivery in return for personal information and report those who say that pre-payment of taxes or fees are required in order to receive the qualifying Economic Impact Payment. Next slide, please.

Reporting IRS-related coronavirus scams – the Treasury Inspector General for Tax Administration has set up a tips portal – tips.tigta.gov which will take you to a multi-page forum depending on the type of scam, and you can report any scams related to – any IRS scam or coronavirus-related scam here. And we've tried to make the website so that it categorizes it by the type of scam. It could be impersonation, but if it's coronavirus, we just ask that you try to use that. That helps us kind of work the case a little faster and get the data to the right places. But if you do receive any kind of information you know, maybe it's a phone call so, you don't really have anything to forward to phishing@irs.gov you can certainly go to this web page and type in any information that you have and that's useful in aggregate. Once we get a bunch of these complaints, we kind of – helps us build a picture of a bigger case that's going on across the country. Next slide, please.

Cyber-fraud targeting tax preparers. Just some quotes from different press releases are in here you know, generic warnings. I mean, tax preparers have always been warned about this. The IRS is a trove of personal information, which helps malicious actors get access to all types of financial benefit mortgages, loans, small –

you know, payday anything other government programs and things of that nature. So, while the IRS receives a great deal of funding to help bolster and build out security around their applications and we are charged with investigating abuses of those, that leaves you all at a target for the same activity. So, you know, you just have to be vigilant about people trying to social engineer you, pretend to be someone they're not, through e-mail, phone, *et cetera*. And if you get malware on one of your information systems, you have taxpayer data on your systems and that's compromised. You need to report that. They are coming to you, and they will continue to come to you in an effort to get as much data as they possibly can, and it is imperative that you, you know be vigilant and also, report the information so that we can take swift action against those who seek to undermine our tax system. Next slide, please.

Some cyber-fraud statistics. 2020 reports to the FBI Internet Crime Complaint Center IC3. If you're not familiar with IC3, IC3.gov is a place a generic place where anybody can kind of go and put in any information about any type of internet crime, whether it's the Nigerian prince type scheme where they have money for you or somewhere or someone's just trying to phish you, and we have access, through the FBI's portal, to those reports as well. And so, we can aggregate information. For example, if 100,000 people file a complaint in IC3 and say, "This phone number called me", "I received an e-mail from this e-mail requesting this thing", then we can say, "Okay. This e-mail is really hitting hard, and they are trying to phish a lot of people" and we'll pivot from that, and we can use that investigatively. IC3.gov is a good resource to give to your clients who may you know, being phished, or have something particular that they wish to report.

Maybe it's something. Maybe it's not something. It doesn't hurt if they are just suspicious to put it in here. It does no harm. And so, they can kind of report it there.

If it has to do with TIGTA, we can still act with it. If it doesn't have to deal with TIGTA or the IRS, it's made available to the FBI and the other federal law enforcement agencies. Some of the statistics from the 2020 report out of IC3 collected data are that business e-mail compromises have 19,382 victims which represent $4.9 billion in losses. Technical support fraud thinking it be Microsoft Help Desk 15,780 victims, for example. $412 million in losses. Corporate data breaches 2,796 reported victims with $2.2 billion in losses. Those data breaches a lot of corporations don't

like to necessarily report because of it may impact their corporation negatively and so they might not be in IC3. Phishing or Vishing scams are 241,347 victims $1.2 billion in reported losses. Government impersonators 12,841 victims have reported inside of IC3 in 2020. $8.1 billion in reported losses, and then, malware – 1,429 victims affected with malware reported in IC3 $14 million in losses.

Next slide, please.

Primary Cyber-Fraud Targets. You know, they're really looking for financial and personal information so that's going to be, like I said before, it's going to be on your the tax preparer local computer network, in your software if you use online software, you know, whatever you know, there's a handful of companies out there that you probably leverage and, you know, if someone if you use a common password, for example, you know, SuperSecretPassword1 for your e-mail and for your login to your company's e-mail and then, you use the same password for, you know, your online tax preparation software and someone compromises one, then they will try it everywhere else. So, you know, it's important to make sure that you keep those passwords safe and then, also try to separate those out depending on what the access is to. So, if you're using your for your personal bank, you know, you might want to have a different password than for your professional tax preparation firm's log-on, even though it's convenient. That way, it just helps if one gets compromised, you don't have to go and now, worry about every log-on you have needing to be reset. And then, in your preparer's IRS e-services account. Please, always ensure the numbers in the IRS e-services account match what you're filing. This is kind of a big thing. We'll frequently see, you know, a large number of tax returns come through related to some portal activity. They steal an identity you know, a bunch of identities – and they come back, and they file tax returns with a stolen PTIN, and the tax preparer's none the wiser, 'cause they're not really paying attention to the e-services account, and they don't notice that they didn't file 100,000 tax returns in the last week. So, that's something that you might want to pay attention to. Next slide, please.

Common cyber scams – phishing e-mail scams to harvest user account information or to unlock your tax software accounts, posing as tax accounting or professional associations just trying to get you to execute malicious software or malware designed to steal your financial network account passwords. So, if you get pop-ups

asking you to in your browser asking you to escalate permissions or allow some type of java to be installed to do something, I would just say it's safer to click "No". Advanced cyber-attacks against poorly secured networks and ransomware becoming more popular, designed to encrypt your network devices and then, offering to un-encrypt those for a fee. So, it's important to reach out, try to get some professional help for ransomware, which typically involves backups. Next slide, please.

Cyber warning indicators suspicious activity indicating compromise of your local network. If there's files missing or moved, or additional programs installed you do not recognize there's a particular log-in history or unusual numbers of filings in your e-services account, unusual CAF history or activity – Centralized Authorization File activity. Take note of unauthorized IRS Form 8821s, which are the *Tax Information Authorizations* or the 2848, *Power of Attorney and Declaration of Representative* that are filed in your name.

You know, just periodically go look and just make sure everything looks like it's still in order and, if you didn't do something, it doesn't hurt you even if you forgot or it got busy and maybe it's fine it doesn't hurt to call in and just make sure, 'cause then, they can re-issue a PTIN and shut the old one down and just prevent fraud and a lot of headache for you and for your customers. Next slide, please.

The Electronic Filer Identification Numbers of Preparer Tax Identification Number PTIN activity higher than the number of returns you submitted which I said before; your customers receiving mailed, unsolicited tax transcripts from previous years; customers receiving notification for the establishment of an e-authentication account, which they did not create because once, when your customers go online to the IRS portal and create an account, it will generate a mailing to the last address of record. They'll get something in the mail saying that they – "You created an account. If you did not create an account, call the IRS." When they get those notices, they should make sure that the number that they're calling is actually the IRS and not just take it for granted that the letter they got in the mail has the IRS's phone number on it.

I would not be surprised if, you know, the scammers figured this out and started mailing fake mail-outs so, it's good to double check. Go on IRS.gov. Check the numbers. Make sure they line up

before you place that call. Tax software vendors may advise that fraudulent IRS document or EFIN has been submitted to a secure software purchase so, just pay attention to that. A lot of times, they reach out to us and say you know, "We think that there's suspicious activity involving these PTINs or EFINs. They've applied for software, and you know, we think it's unusual." Next slide, please.

We went over this slide's also what to report to TIGTA. You can report to TIGTA or to the IRS stakeholder liaison the suspicious log-ons or activity on your e-service account that were not done by you. Submissions of fraudulent IRS forms, fraudulent IRS EFIN memos or software vendors if someone asks you, you know, calls you up to verify that you're legitimate, "Did you submit this but you're not using them" you should report that to us. Customers who receive unsolicited transcripts or these notices for their e-auth account access or now, ID.me as well. If they created an account with the IRS, they get a letter in the mail, they don't recognize it – they can report that at tips.tigta.gov. Next slide, please.

Some helpful IRS publications that you may wish to read. Publication 4557 – *Safeguarding Taxpayer Data,* 5293 – *Data Security Resource Guide for Tax Professionals,* Publication 3112 – the *e-File Application and Participation,* and Publication 1345 – *Handbook for Authorized e-File Providers for Individual Tax Returns.* Next slide, please.

What else can you do to help protect federal tax administration? You can report instances of tax preparer or IRS employee misconduct.

We do investigate IRS employees and are interested in any of your interactions with them that you believe to be misconduct. Report potential threats to IRS employees and facilities so, if you are made aware of any type of threat to an IRS employee, staff, contractor, or one of the IRS facilities, please, report that immediately and you can report that directly to us or to your local police.

It will get to us. You can warn your other colleague and clients about these scams and make sure that you update client addresses of record on the Form 8822. Next slide, please.

How to contact TIGTA. We accept e-mail at complaints@tigta.treas.gov. So, if you know, you don't feel like whatever your complaint is fits into the tips.tigta.gov and you want

to forward some type of suspicious thing to us, you can use complaints@tigta.treas.gov. You can call us at our 800 number here – 1-800-366-4484 – or you can visit us on the internet and just make sure if it's United States government, it's .gov at the end so, just you know, pay attention, and make sure you're not being phished and put into a fake site. That's www.tigta – T-I-G-T-A – .gov, and one final thing before I get off here, the new advanced Child Tax Credit application that allows your clients – or you if you're eligible to receive that credit to look at the portal and manage their payments. The identity verification process is now being handled through ID.me. Something to be aware of is that because ID.me is not a .gov domain, some of that authentication and identity assurance that happens on the front end does not happen on a .gov, and so, it's very important to pay attention to the URL and make sure it's not, you know, something else besides just the ID.me.

And already, we're seeing evidence of websites being stood up that, you know, say something else -ID.me and then, the website is built to look just like the identity authorization site. So, you know, make sure that you go to the IRS.gov website first and that should pivot you to the correct ID.me identity assurance platform. If you're getting e-mail or something that says, "Click this. This is from ID.me" unsolicited, I would warn you against clicking those and please, report those to phishing at IRS.gov. We already have a pretty good case because someone reported something like that to us at phishing@irs.gov so, it's very useful to us and we hope we can stamp out some of this fraud by your assistance. We really can't do it without you reporting things to us.

And that is all I have. I'll turn it back –

to you, the moderator. That's, Alec.

Alec Johnston: It looks like we have time to answer some of the questions that have been submitted. We remind everybody that in order to earn CE credit, you must be present for the entire presentation, which includes this Q&A and the survey at the end. Let's move on to our first question. Question one – "What should I do if my computer system has been compromised?"

Dale Forrester: Hey, this is Dale. I'll take that. You know, I guess it sort of depends what the system's used for. So, if it's your professional system, you use it and all your taxpayers' documents are on that, I would you know it's compromised, I would suggest taking it off the internet right away and then, I would suggest, you know, calling you know, filing a local police report obviously does help. Report any details that you might have as a result of an incident response. Some companies – you know, I'm sure all of you are not giant companies Some companies have incident response where someone a third-party company comes out, performs some type of triage and report. Those reports are useful to law enforcement.

So, if you would like to make those reports available to us, you can certainly forward those to us at the complaints@tigta.treas.gov e-mail or the phishing@IRS.gov. Although, it's typically just phishing, they do kind of handle other incidents of that nature. And you know, and then, just you'll probably have to start with a clean slate again, but that's basically my recommendation. If you find out what the source of the compromise was if it was just passwords were compromised versus malware, you certainly are gonna want to go on a clean system and reset all of your credentials.

Thank you for your participation.

Glossary

Advanced Child Tax Credit – allows qualifying families to receive early payments of the tax credit many people may claim on their 2021 tax return during the 2022 tax filing season.

ARPA – acronym for American Rescue Plan Act; a $1.9 trillion economic stimulus bill signed into law on March 11, 2021, to speed up the United States' recovery from the economic and health effects of the COVID-19 pandemic and the ongoing recession.

CAF – acronym for Centralized Authorization File; allows the input of codified additional acts authorized on a Form 2848, Line 5a.

CARES Act – acronym for Coronavirus Aid, Relief, and Economic Security Act. Signed on March 27, 2020, this stimulus bill was aimed to blunt the impact of an economic downturn due to the global coronavirus pandemic.

Economic Impact Payments – funds to help people during the coronavirus pandemic.

EFIN – acronym for electronic filing identification number; number issued by the IRS to individuals or firms that have been approved as authorized IRS e-file providers**.**

EIN – acronym for Employer Identification Number; a unique nine-digit number assigned by the IRS to business entities operating in the United States for the purposes of identification.

Equal Employment Opportunity Commission – a federal agency that was established via the Civil Rights Act of 1964 to administer and enforce civil rights laws against workplace discrimination.

Gig economy – commonly referred to as the sharing economy or access economy; a labor market based on flexible, temporary, or freelance jobs where individuals earn income by providing on-demand work, services, or by selling goods.

IC3 – acronym for the Internet Crime Complaint Center; IC3 provides the public with a reliable and convenient reporting mechanism to submit information to the FBI about suspected Internet-facilitated criminal activity and to develop alliances with law enforcement and industry partners.

ID.me – an American online identity network that allows people to prove their legal identity online.

IRS's Anti-Harassment Program – program to provide an IRS work environment free from all forms of discrimination, including harassment, regardless of the motive of the harasser.

IRS Pseudonym Program – provides the necessary framework and process to ensure an IRS pseudonym is assigned to IRS employees requesting one for their personal safety and the prevention of harm or danger to themselves and their families.

Levy release – the release of property or assets that were legally seized due to unpaid tax debt.

malware – any software intentionally designed to cause damage to a computer, server, client, or computer network.

Office of Professional Responsibility – IRS office that support effective tax administration by ensuring all tax practitioners, tax preparers, and other third parties in the tax system adhere to professional standards and follow the law.

Phish, Phishing - a type of social engineering where an attacker sends a fraudulent message designed to trick individuals into revealing sensitive information or to deploy malicious software on the victim's network.

PII – acronym for personally identifiable information. PII is any information about an individual that can be used directly, or in connection with other data, to identify, contact or locate that person.

PSA – acronym for public service announcement. A PSA is a message in the public interest disseminated by the media without charge to raise public awareness and change behavior.

PTIN – acronym for preparer tax identification number; an identification number that all paid tax return preparers must use on U.S. federal tax returns or claims for refund submitted to the IRS.

Ransomware – a type of malicious software designed to block access to a computer system until a sum of money is paid.

SBA – acronym for Small Business Administration. A United States government agency that provides support to entrepreneurs and small businesses.

TIGTA – acronym for the Treasury Inspector General for Tax Administration. TIGTA provides independent oversight of the IRS, protect the integrity of federal tax administration, detects, and prevents waste, fraud, and abuse at the IRS.

Unauthorized disclosure – an incident where an IRS employee discloses a return or return information to someone who is not authorized to receive the information.

Vishing – the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies to trick individuals to reveal personal information.

VITA – an acronym for Volunteer Income Tax Assistance. This IRS initiative is designed to support free tax preparation service for the underserved through various partner organizations.

Index