Report

June 2016

2016 Security Summit

Protecting Taxpayers from Identity Theft Tax Refund Fraud

IRS

2016 Security Summit

Protecting Taxpayers from Identity Theft Tax Refund Fraud

Contents

2016 Security Summit

Protecting Taxpayers from Identity Theft Tax Refund Fraud

Overview

Tax refund fraud caused by identity theft is a serious and complicated threat. Criminals – many of them sophisticated, organized syndicates - are redoubling their efforts to gather personal data to file fraudulent federal and state income tax returns that can bypass our fraud filters and allow them to claim refunds.

No one entity can fight this crime alone. It takes all of us, working together, to contain this global epidemic. That is why the Security Summit - the unprecedented partnership between the IRS, state tax agencies, and the private-sector tax industry - came together in 2015 to form a united and coordinated front against this common enemy.

This ground-breaking partnership, marking its first year, made great progress in 2016 implementing scores of new safeguards, agreeing on a cybersecurity framework and taking the initial steps to create a new "early warning" system that will help quickly identify and share identity theft schemes.

Because of the Security Summit initiative and our cooperative efforts, we protected more taxpayers from tax-related identity theft, stopped more suspicious tax returns, and prevented more fraudulent refunds from getting into criminals' hands. Because of the safeguards enacted by this partnership, fewer people became victims of tax-related identity theft this year.

A few 2016 Security Summit highlights:

- The Security Summit group members identified and agreed to share more than 20 data components from federal and state tax returns to improve fraud detection and prevention this filing season. For example, group members are sharing computer device identification data tied to the return's origin, as well as the improper or repetitive use of the numbers that identify the internet "address" from where the return originates.

- Tax software providers agreed to enhance identity requirements and strengthen validation procedures for new and returning customers to protect their accounts from being taken over by criminals. This change was one of the most visible to taxpayers during the 2016 Filing Season, because it included new verification procedures they needed to follow to log in to their accounts. These actions will serve as the baseline for ongoing discussions and additional enhancements for the 2017 Filing Season.

- The Security Summit group gathered more endorsements for its Memorandum of Understanding (MOU) regarding roles, responsibilities, and information sharing pathways among IRS, states and industry. So far, 40 state departments of revenue and 21 tax industry members have signed the MOU, along with the IRS and seven endorsing organizations.

- The Security Summit partners also realized that the public had a role to play. The Security Summit launched a “Taxes. Security. Together” campaign to increase public awareness about the need for computer security and provide people with tips on how to protect their personal information. The easiest way a criminal steals personal data is simply to ask for it by posing as a bank, credit card company, or even the IRS.

These accomplishments had real and substantial impact on curbing stolen identity refund fraud:

- From January through April 2016, the IRS stopped $1.1 billion in fraudulent refunds claimed by identity thieves on 171,000 tax returns; compared to $754 million in fraudulent refunds claimed on 141,000 returns for the same period in 2015. Better data from returns and information about schemes meant better filters to identify identity theft tax returns.
- Thanks to leads reported from industry partners, the IRS suspended 36,000 suspicious returns for further review from January through May 8, 2016, and $148 million in claimed refunds; twice the amount of the same period in 2015 of 15,000 returns claiming $98 million. Industry’s proactive efforts helped protect taxpayers and revenue.
- Because of the Security Summit efforts, the number of anticipated taxpayer victims fell between/during 2015 to 2016. Since January, the IRS Identity Theft Victim Assistance function experienced a marked drop of 48 percent in receipts, which includes Identity Theft Affidavits (Form 14039) filed by victims and other identity theft related correspondence.
- The number of refunds that banks and financial institutions return to the IRS because they appear suspicious dropped by 66 percent. This is another indication that improved data led to better filters which reduced the number of bad refunds being issued.
- The Security Summit Rapid Response Team tackled emerging issues. This team, working together with Summit partners, was able to shut down one scheme in which a criminal stole client data from a tax preparer. The Rapid Response Team also was critical to protecting taxpayers when criminals, using data stolen elsewhere, were able to impersonate taxpayers and access IRS.gov self-help tools.
- Working together, the Security Summit partners were able to warn the public, especially payroll industry, human resources, and tax preparers, of emerging scams in which criminals either posed as company executives to steal employee Form W-2 information or criminals using technology to gain remote control of preparers’ office computers.

From the beginning, the Security Summit focused on identifying and enacting safeguards that would help ensure the legitimacy of the tax return filed and the authentication of the taxpayer filing it. Equally important is improving the information sharing among the partners so that identity theft schemes are quickly identified and shared among partners so they may take protective actions.

For 2017, the emphasis remains on authentication, information sharing and cybersecurity. A few new or expanded efforts include:

- The IRS and its partners in the payroll industry will expand a pilot program to add a W-2 Verification Code to approximately 50 million forms in 2017. Adding this 16-digit code helps validate not only the taxpayer's identity but also the accuracy of the information on the form.
- The States and the IRS will receive additional data elements from returns that will help improve authentication of the taxpayer and identify possible identity theft scams. Partners also will receive data elements from corporate tax returns and enhance authentication efforts of tax professionals filing returns.
- The new Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (IDTTRF-ISAC) will launch in 2017. A tax ecosystem ISAC will allow for significant gains in detecting and preventing identity theft tax refund fraud and will enhance real-time information sharing platform.
- The Security Summit's "Taxes. Security. Together." campaign will focus its efforts on education and outreach aimed at tax return preparers and making sure they have the information they need to protect themselves from cyberattacks and to safeguard taxpayer data.
- Twenty-three states will work with participating financial industry partners on a program to help identify those state tax refunds that appear fraudulent and return them to the states for validation rather than depositing them.

Seven work groups perform the hard work of the Security Summit, identifying and implementing the initiatives. Each work group has a co-lead from the IRS, the states, and the industry.

Their accomplishments for 2016 and their plans for 2017 make up the 2016 Security Summit Report.

Security Summit Work Group Initiative Updates

Authentication Work Group

Authentication was the fundamental starting point for the Security Summit, as participants agreed to do more to verify the authenticity of the taxpayer and the tax return at the time of filing.

For 2016, the Authentication Work Group identified and successfully tested the inclusion of new data elements from tax return submissions shared with the IRS and the states that assisted in detecting and preventing identity theft returns.

The Authentication Work Group reached an agreement for software providers to enhance identity requirements and strengthen validation procedures for new and returning customers to protect against account takeover by criminals. These provisions were some of the most visible to taxpayers in 2016 because they included new password standards to access tax software and the use of security questions.

These 2016 Filing Season actions serve as the baseline for on-going discussions and additional enhancements for the 2017 Filing Season. These actions led to stronger protections for filing tax returns this filing season and into the future.

For 2017 and beyond, the Authentication Work Group is carving out short-term and long-term objectives to improve authentication. These objectives address recommendations from the Security Summit to assist in preventing account takeovers and assist in identifying and potentially preventing incidents where fraudsters already have and are using stolen personally identifiable information data.

The Authentication Work Group identified additional data elements from the electronic tax return that will strengthen the authentication of the individual. This will be in addition to the more than 20 data elements shared during the 2016 Filing Season.

Additionally, the Authentication Work Group will share data elements from business tax returns to expand the authentication efforts to include corporate filings.

The Security Summit partners also will step up authentication efforts of tax return preparers, including enhanced trusted customer requirements for tax professional software and better validation for the Electronic Filing Identification Number (EFIN) used by tax professionals and e-file return originators.

A pilot program for the W-2 Verification Code will greatly expand for 2017 to 50 million Forms W-2 issued by payroll service providers. In 2016, a partnership between the IRS, four payroll service providers, and tax software providers showed great promise in verifying taxpayer identities and other information. Taxpayers and tax preparers who were part of the pilot enter a 16-digit code, unique to each form, when prompted by software. The verification code also is a way to help protect business’s Employer Identification Numbers sometimes used by criminals to create fake Forms W-2.

Communication and Taxpayer Awareness Work Group

The Communication and Taxpayer Awareness Work Group aims to increase awareness among individuals, businesses, and tax professionals on the need to protect sensitive tax and financial information.

In 2016, the Communication and Taxpayer Awareness Work Group helped increase public awareness and encourage better protection of personal data by publicizing key messages, resulting in broad and continued coverage in traditional and social media. The Communication and Taxpayer Awareness Work Group developed and implemented an integrated communications strategy based on government and industry best practices that consisted of the following:

- Repetitive and persistent use of common key messages developed as a team
- High volume of products publicized in various formats for the general public and tax professionals

The Communication and Taxpayer Awareness Work Group developed and released Fact Sheets, Tax Tips, videos, and updated Publication 4524, *Security Awareness For Taxpayers*. The Communication and Taxpayer Awareness Work Group posted these items on IRS.gov and used these resources in the coordinated media campaign called “Taxes. Security. Together.”

The 2016 Filing Season efforts provided nationwide media coverage in a variety of news outlets, as well as state level coverage. The IRS engaged taxpayers directly using social media outlets such as Twitter, YouTube and Tumblr, to distribute information on the topic of protection of personal data.

The Communication and Taxpayer Awareness Work Group created common messages for industry, states, and the IRS around its “Taxes. Security. Together.” campaign to reinforce the fact that everyone has a roll to play in protecting taxpayer data including the public.

The Communication and Taxpayer Awareness Work Group also shared alerts as scams emerged. One scheme targeted company payroll personnel. Criminals posing as the company executive would send emails to payroll personnel requesting the Forms W-2 for all employees. Another scheme saw return preparers fall victim to cybercriminals who gained remote control of their computers, completed client tax returns and diverted refunds to their own accounts.

During 2017, the Communication and Taxpayer Awareness Work Group, working with the Tax Professionals Work Group, will launch a national campaign aimed at the nation’s 700,000 tax return preparers. Tax professionals increasingly are the targets of identity thieves and cybercriminals who seek to steal the tax and financial data that preparers maintain on clients. The objective of this new national campaign will be to educate tax return preparers about the various tactics of the identity thieves and the steps necessary to protect data. Safeguarding taxpayer information is everyone’s responsibility, and all tax return preparers must take active steps to remain secure.

Financial Services Work Group

The Security Summit established the Financial Services Work Group to examine and explore additional ways to prevent and deter criminals from potentially accessing tax-time financial products, deposit accounts, and pre-paid debit cards.

By identifying best practices, this could assist government and industry in preventing identity theft and combatting stolen identity refund fraud.

In January 2013, NACHA – The Electronic Payment Association, worked with IRS and the Department of Treasury on a protocol that allowed financial institutions that received direct deposit refunds to opt into a new External Leads Program. Financial institutions that noticed mismatched account name information or suspected fraudcould return those refunds to the IRS.

The Financial Services Work Group worked in 2016 to achieve an agreement on a naming convention that will help participating financial institutions identify state tax refunds. Without the naming convention, financial institutions are unaware when a product for deposit is a state tax refund. The Financial Services Work Group developed a definition of Ultimate Bank Account (UBA) that will help identify the final destination of refunds.

For 2017, the Financial Services Work Group expects 23 states will be working with participating financial institutions that can help identify suspicious state tax returns and return them to the states for enhanced scrutiny.

For 2017, the definition of the UBA will include all refund transfer products, including gift and pre-paid cards, paper checks, and direct deposits. The objective is to determine the final destination of refunds.

For 2017, the Financial Services Work Group also will conduct several "test and learn" pilot programs that will enhance ways of identifying and stopping fraudulent or questionable refunds. The States and the financial industry will share data and information in an effort to improve their ability to identify possibly fraudulent state tax refunds.

The Financial Services Work Group also will work with financial institutions to identify best practices for identifying identity theft or fraud. These best practices will be shared with other financial institutions.

Information Sharing Work Group

Information Sharing Work Group is working on identifying opportunities for sharing information that would improve our collective capabilities for detecting and preventing identity theft refund fraud.

During 2016, this Information Sharing Work Group agreed on the need to create an Information Sharing and Analysis Center (ISAC). The ISAC sub group is developing requirements to design and create the ISAC. The following pages provide details on the ISAC activities.

For 2016, the Information Sharing Work Group facilitated a Memorandum of Understanding (MOU) that set out information sharing procedures and governance. To date, the MOU has been signed by 40 state departments of revenue, 21 industry partners and seven endorsing organizations.

The Information Sharing Work Group collaborated to establish a requirement for industry e-file providers who file 2,000 or more returns to perform research and analysis and provide any identity theft data to the IRS. The Information Sharing Work Group published this requirement in IRS Publication1345, *Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns,* and Publication 3112, *IRS E-File Application and Participation*, for 2016 Filing Season.

For 2016, the state operating agreements have like-kind requirements for data sharing and lead reporting to the IRS. At the request of industry and states, the IRS acted as a conduit and facilitated industry data sharing with states via a Secure Data Transfer “flow through” process.

The Information Sharing Work Group helped establish a Rapid Response Team (RRT) with membership from IRS, states, and industry, with the intent to share details around the security awareness incidents. The Information Sharing Work Group worked quickly to share information about emerging issues that helped protect taxpayers.

For 2017, the Information Sharing Work Group is collaborating with the Authentication Work Group to evaluate proposed additional data elements from electronic returns and collaborating with industry and state partners for testing the proposed data elements.

The Information Sharing Work Group will improve existing documents, reports and processes, including enhancing analysis of leads to provide more meaningful communication to state and industry partners. The improved communication may provide alerts on filing patterns and other actionable information on questionable filing activity that will boost efforts to reduce identity theft refund fraud across all platforms.

Confirmed identity theft account information will be provided to industry and states at the start of the filing season to provide the Security Summit partners with the opportunity to analyze the information and update their filters. The Information Sharing Work Group also will address and analyze industry lead reporting compliance with Publication 1345 and the requirement upon industry to provide identity theft data.

Information Sharing and Analysis Center Work Group (ISAC)

Since its formation in 2015, the Security Summit focal point targeted three major challenges: improving authentication, detecting fraudulent returns, and enhancing information sharing.

The Security Summit partners studied information sharing possibilities and reviewed the practices followed at the Department of Health and Human Services (HHS), which works with its industry partners to curtail health care fraud, and the Federal Aviation Administration (FAA), which works with its industry partners on aviation issues. Both HHS and FAA use an Information Sharing and Analysis Center Work Group to exchange ideas, schemes and trends.

In 2016, the Security Summit agreed to create an Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (IDTTRF-ISAC), which is a highly secure web-based way for states, industry, and the IRS to share and exchange information. This IDTTRF-ISAC subgroup was created so partners could work together and with external third parties to create an ISAC devoted to tax refund fraud.

Like a radar array, the IDTTRF-ISAC serves as an early warning alarm for states, industry, and the IRS for refund fraud, identity theft schemes, and cybersecurity issues.

The IDTTRF-ISAC will build upon the leads program within IRS by creating a Public-Private Partnership to collect and analyze stolen identity refund fraud information and threats against the IRS or its IDTTRF-ISAC partners (states and industry).

The IDTTRF-ISAC information and analysis will assist stakeholders in defense of critical mission functions and increase the security of the tax ecosystem. The IDTTRF-ISAC will eventually centralize, standardize, and enhance data compilation and analysis to facilitate sharing actionable data and information. The Security Summit target date to deploy a pilot of the IDTTRF-ISAC for certain operations is 2017 Filing Season.

The Security Summit tasked a contractor, MITRE, with assessing the entire Lead Reporting and Information Sharing process and developing the pilot of the IDTTRF-ISAC that consists of two components, cybersecurity and identity theft refund fraud. Potential capabilities of the IDTTRF-ISAC include, providing a centralized location for sharing alerts, leads, best practices, analytical practices and documents.

Strategic Threat Assessment and Response (STAR) Work Group

In 2016, the tax industry participants agreed to align with the IRS and the states under the National Institute of Standards and Technology (NIST) Cybersecurity Framework to promote the protection of Information Technology (IT) infrastructure.

The IRS and the states currently operate under the tenants of this framework, as do many in the tax industry. During the first half of 2016, the STAR Work Group developed a strategy for how participating organizations will implement the NIST Cybersecurity Framework.

For the remainder of 2016, tax industry participants will begin implementation of the NIST Cybersecurity Framework. STAR Work Group plans include determining future assessment criteria, compliance options, and sharing best cybersecurity practices through continued education and outreach.

For 2017, the STAR Work Group plans to develop a cyber-threat assessment of the tax ecosystem, incorporate any changes in the NIST guidance and continue implementation of the Cybersecurity Framework. In addition, there will be continued support for the Authentication and Information Sharing Work Groups as well as a focus on continued outreach and education for the participants.

Tax Professionals Work Group

The nation’s tax professionals play a critical role within the tax industry, in both the federal and state arenas. The initial work of the Security Summit focused on self-preparers, the do-it-yourself taxpayers, because of the urgency at the time. The Tax Professional Work Group was created in recognition that tax preparers are often the first line of defense against identity theft.

The Tax Professionals Work Group is charged with determining how the tax professional community can contribute in the prevention of identity theft and refund fraud and how the overall data capture and reporting requirements affect tax preparers.

A survey of the tax professional community netted more than 9,100 responses, with most reporting that they have clients who had experienced tax-related identity theft. Most preparers also reported they had never suffered a data breach nor had they ever had their Preparer Tax Identification Number (PTIN) or Electronic Filing Identification Number (EFIN) compromised. Most also reported they had a process in place to protect client data.

The survey results also made clear that there is a need for additional awareness and education in the preparer community surrounding the importance of data and system security. Given that tax return preparers are increasingly becoming targets for cyberattacks and other types of system intrusion, heightening awareness and education is essential.

The Tax Professionals Work Group is leveraging the 2016 Nationwide Tax Forums to spread this outreach and education message to thousands of tax professionals and outlining the steps they may take to protect their systems and taxpayer data.

In 2016, Tax Professionals Work Group also designed and put into service a secure data transfer protocol for the submission of complaints involving individual preparers or preparer offices. The Tax Professionals Work Group collaborated with the Authentication Work Group to help identify business data elements from corporate returns and EFIN issues.

In 2017, the Tax Professional Work Group and the Communication and Taxpayer Awareness Work Group will collaborate on an outreach and education campaign on more specific security areas throughout the summer and fall.

This outreach will also include a filing season focus on locating available information regarding returns filed with a preparer EFIN or PTIN and the importance of using the capability regularly to detect potential id theft.

Related Activities

Electronic Tax Administration Advisory Committee (ETAAC)

ETAAC will begin its new role with the Security Summit Group with the establishment of a new ETAAC charter and supporting documents. The ETAAC solicited for new members in late March with an announcement in the Federal Register and IRS news release. The new member process continues in May and June. The first meeting of the ETAAC with new members will convene in July 2016.

Secure Access

In June 2016, the IRS introduced a new taxpayer authentication platform called Secure Access. That process relies on two-factor authentication for returning users. The two factors are the username credentials and security code texts to mobile phones. Secure Access meets federal guidelines and matches financial industry best practices. With Secure Access, the application Get Transcript Online returned to IRS.gov. Other IRS.gov applications will be updated with Secure Access as warranted throughout 2016 and 2017.

State Driver’s License Numbers

Several states made use of their own databases to help authenticate taxpayers during the 2016 Filing Season. Several states asked taxpayers or tax preparers to provide the driver’s license number of the taxpayer filing the state tax return. The additional verification step was just one more way to help protect taxpayers from identity thieves.

Congressional Authority (Pending Legislative Proposals)

Congress provided significant help in the fight against identity theft refund fraud by passing several important legislative proposals in the President’s FY 2016 Budget proposal, including the following:

- Acceleration of information return (Forms W-2, 1099, etc.) filing due dates
- Extending IRS authority to require truncated SSNs on Form W-2
- Expansion of the due diligence requirements to AOTC and CTC/ACTC

Pending legislative proposals in the President’s FY17 Budget:

- Streamlined critical pay authority: This would allow the IRS, with approval from Treasury, to hire well-qualified individuals to fill positions deemed critical to the agency’s success in areas such as international tax, IT, cybersecurity, online services, and analytics support. This authority expired at the end of FY 2013.
- Correction procedures for specific errors: This would allow the IRS to fix errors where the IRS has reliable information that a taxpayer has an error on his/her return.
- Authority to require minimum qualifications for return preparers: The proposal would provide the agency with explicit authority to require all paid preparers to have a minimum knowledge of the tax code. It would thereby help the IRS to focus resources on the truly fraudulent returns.

Summary - Filing Season 2016 Accomplishments

- The Security Summit group members identified and agreed to share 20 data components from federal and state tax returns to improve fraud detection and prevention this filing season. For example, group members are sharing computer device identification data tied to the return's origin, as well as the improper or repetitive use of the numbers that identify the internet "address" from where the return originates.
- Tax software providers agreed to enhance identity requirements and strengthen validation procedures for new and returning customers to protect their accounts from being taken over by criminals. This change is one of the most visible to taxpayers during the 2016 Filing Season, because it includes new verification procedures they need to follow to log in to their accounts.
- The Security Summit group gathered additional endorsements for the Memorandum of Understanding (MOU) regarding roles, responsibilities, and information sharing pathways among the IRS, states and industry. So far, 40 state departments of revenue and 21 tax industry members have signed the MOU, along with the IRS and seven endorsing organizations.
- Tax industry participants have aligned with the IRS and the states under the National Institute of Standards and Technology (NIST) Cybersecurity Framework to promote the protection of information technology infrastructure. The IRS and the states currently operate consistently with this framework, as do many in the tax industry. The STAR Work Group has started implementing the NIST Cybersecurity Framework.
- The Security Summit group members agreed on the need to create an Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC) to centralize, standardize, and enhance data compilation and analysis to facilitate sharing actionable data and information.
- Recognizing the critical role that the nation's tax professionals play within the tax industry in both the federal and state arenas, the Security Summit group created a team that will examine issues related to return preparers, such as how the preparer community can help prevent identity theft and refund fraud.
- Summit partners also realized that the public had a role to play. The Security Summit launched a "Taxes. Security. Together" campaign to increase public awareness about the need for computer security and provide people with tips on how to protect their personal information. The easiest way a criminal steals personal data is simply to ask, posing as a bank, credit card companies or even the IRS.
- The states and financial institutions worked together on a new naming convention for state tax refunds and a process for financial institutions to return to the states suspicious state tax refunds. Currently, financial institutions may not know when they are receiving a state tax refund. Financial institutions have worked with the IRS on a federal external leads program since 2013.

Summary - Filing Season 2016 Accomplishments – Continued

- Partners worked to expand the definition of Ultimate Bank Account that will help determine the final destination of refunds.
- Partners collaborated with industry on new requirements for large industry e-file providers to perform research and analysis and provide any identity theft data to the IRS and the states.
- The new Tax Professional Work Group conducted a survey of the tax professional community to learn more about their understanding of tax-related identity theft. Eighty-three percent of 9,100 responding preparers reported they had at least one client who was a victim of tax-related identity theft.
- From January through April 2016, the IRS stopped $1.1 billion in fraudulent refunds claimed by identity thieves on 171,000 tax returns; compared to $754 million in fraudulent refunds claimed on 141,000 returns for the same period in 2015. Better data from returns and information about schemes meant better filters to identify identity theft returns.
- Thanks to leads reported from industry partners, the IRS suspended 36,000 suspicious returns for further review from January through May 8, 2016, and $148 million in claimed refunds; twice the amount of the same period in 2015 of 15,000 returns claiming $98 million. Had industry not flagged these returns, they would have passed through filters.
- Because of the Security Summit efforts, the number of anticipated taxpayer victims fell between/during 2015 to 2016. Since January, the IRS Identity Theft Victim Assistance function experienced a marked drop of 48 percent in receipts, which includes Identity Theft Affidavits (Form 14039) filed by victims and other identity theft related correspondence.
- The number of refunds that banks and financial institutions return to the IRS because they appear suspicious dropped by 66 percent. This is another indication that improved data led to better filters which reduced the number of bad refunds being issued.
- Our Rapid Response Team tackled emerging issues. This team, working together, was able to shut down one scheme in which a criminal stole client data from a tax preparer. The Rapid Response Team also was critical to protecting taxpayers when criminals, using data stolen elsewhere, were able to impersonate taxpayers and access IRS.gov self-help tools.
- Working together, the Security Summit partners were able to warn the public – especially payroll industry, human resources, and tax preparers of emerging scams in which criminals either posed as company executives to steal employee Form W-2 information or criminals using technology to gain remote control of preparers' office computers.

Summary - Filing Season 2017 Initiatives

- The IRS and its partners in the payroll industry will greatly expand a pilot program to add a W-2 Verification Code to approximately 50 million forms in 2017. A smaller test in 2016 was extremely successful in validating information at the time of filing. Adding this 16-digit code helps validate not only the taxpayer's identity, but also the accuracy of information on the form. This will be among the most visible safeguards for taxpayers in 2017.
- The states and the IRS will receive additional data elements from returns that will help improve authentication of the taxpayer and identify possible identity theft scams. Partners also will expand enhanced authentication efforts to business taxpayers as well as tax preparers.
- The new Identity Theft Tax Refund Fraud Information Sharing & Analysis Center (IDTTRF-ISAC) will launch in 2017. A tax ecosystem ISAC will allow for significant gains in detecting and preventing identity theft refund fraud and will provide better data to law enforcement to investigate and prosecute identity thieves. The idea is it would provide all Security Summit partners with a threat assessment capability, early warning and insights about identity theft fraud schemes through nimble and agile information sharing.
- The Security Summit's "Protect Your Clients; Protect Yourself" campaign will focus its efforts on education and outreach aimed at tax return preparers and making sure they have the information they need to protect themselves from cyberattacks and to safeguard taxpayer data.
- Twenty-three states worked with the financial industry on an external leads program, similar to the IRS External Leads Program. The program, starting in 2017, allows the financial industry to help identify those state tax refunds that appear fraudulent and return them to states for validation rather than depositing them.
- In an effort to determine the final destination of refunds, the Security Summit partners expanded the definition of Ultimate Bank Account to include all refund transfer products, including gift and pre-paid cards, paper checks and direct deposit. The states and the IRS also will expand real-time communications with the pre-paid card industry to block accounts associated with fraud.
- The STAR Work Group plans to develop a cyber-threat assessment of the tax ecosystem, incorporate any changes in NIST guidance and continue implementation of the Cybersecurity Framework.
- Starting this summer, the Security Summit's efforts will be institutionalized through the auspices of the Electronic Tax Administration Advisory Committee (ETAAC.) An amendment to ETAAC's charter expanded its scope to include identity theft.

About the Participants

Security Summit partners range from a cross-section of the public and private sectors, including the IRS, state tax agencies, and through their associations, tax software developers, preparers, transmitters, financial institutions, refund product providers, payroll service providers among others.

American Coalition for Taxpayer Rights (ACTR)
ACTR advocates for policies to protect taxpayers and the voluntary income tax compliance system. ACTR members include the following companies: CCH Small Firm Services, H&R Block, Intuit, Jackson Hewitt, Liberty Tax Service, Refund Advantage, Republic Bank & Trust Co., Tax Products Group, TaxSlayer and TaxAct.

American Payroll Association (APA)
Established in 1982, the American Payroll Association is the nation's leader in payroll education, publications, and training. Representing more than 20,000 members, APA is the industry's highly respected and collective voice in Washington, D.C.

Council for Electronic Revenue Communication Advancement (CERCA)
CERCA, launched in 1994, was founded at the direct request of the IRS in order to provide a forum and a liaison point between the IRS and industry as well as other key stakeholders. CERCA’s board members include the following companies: Drake Software, Tax Products Group, Intuit, H&R Block, ADP, FileYourTaxes.com, Jackson Hewitt, Liberty Tax Service, Petz Enterprises, River City Bank, TaxSlayer, Thomson Reuters, and Wolters Kluwer.

The Electronic Tax Administration Advisory Committee (ETAAC)
ETAAC provides an organized public forum under the Federal Advisory Committee Act for discussion of electronic tax administration issues in support of the overriding goal that paperless filing should be the preferred and most convenient method of filing tax and information returns. ETAAC members convey the public’s perception of the IRS electronic tax administration activities, offer constructive observations about current or proposed policies, programs, and procedures, and suggest improvements.

Federation of Tax Administrators (FTA)
FTA was organized in 1937 to improve the quality of state tax administration by providing services to state tax authorities and administrators. These services include research and information exchange, training, and intergovernmental and interstate coordination. The federation also represents the interests of state tax administrators before federal policymakers where appropriate.

Network Branded Prepaid Card Association (NBPCA)

NBPCA is a tradeassociation open to all companies involved in providing prepaid cards that carry a brand network logo to consumers, businesses and government, which can be used at numerous retailers nationwide.

Background – About the Security Summit

In recognition of escalating challenges related to identity theft, IRS Commissioner John Koskinen convened an unprecedented Security Summit meeting in Washington, D.C. on March 19, 2015. IRS Officials, the chief executive officers of the leading tax preparation firms, software developers, payroll and tax financial product processors and state tax administrators came together to discuss common challenges and ways to leverage our collective resources and efforts. This meeting established the following three work groups to address specific challenges. The groups were:

- Authentication Work Group
- Information Sharing Work Group
- Strategic Threat Assessment and Response Work Group

In June of 2015, IRS issued the 2015 Security Summit Report that detailed the recommendations of the three specialized work groups established during the Security Summit meeting. Participants recognized the need for creating additional teams to enhance and expand collaborative efforts. Since June 2015, participants created four new work groups:

- Tax Professionals Work Group
- Communication and Taxpayer Awareness Work Group
- Financial Services Work Group
- Information Sharing and Analysis Center Work Group

The recognition was that no silver bullets exist in the fight against this crime and that adopting a multi-layered and coordinated approach is critical to protecting taxpayers and creating barriers for thieves across the entire tax ecosystem, on both the federal and the state levels. The work groups' unprecedented and rigorous collaboration is critical to the success of this partnership and the ongoing and proven success of the Security Summit initiatives.