

IRS News Release

Media Relations Office

Washington, D.C.

Media Contact: 202.317.4000

www.irs.gov/newsroom

Public Contact: 800.829.1040

IRS, Security Summit Partners Expand Identity Theft Safeguards for 2017 Filing Season, Build on 2016 Successes

IR-2016-144, Nov. 3, 2016

WASHINGTON – The Internal Revenue Service, state tax agencies and industry partners today finalized plans for 2017 to improve identity theft protections for individual and business taxpayers after making significant inroads this year against fraudulent returns.

Public and private sector leaders announced today that their collective efforts through the Security Summit initiative have led to a marked improvement in the battle against identity theft during 2016. This is highlighted by the number of new people reporting stolen identities on federal tax returns falling by more than 50 percent, with nearly 275,000 fewer victims compared to a year ago.

At a Washington press conference, Summit leaders also detailed new and expanded safeguards for taxpayers in the upcoming 2017 tax season. The 2017 focus revolves around “trusted customer” features that will help ensure the authenticity of the taxpayer and the tax return - before, during and after a tax return is filed. The additional protections will build on the 2016 successes that prevented fraudulent returns and protected tax refunds.

“We’ve made remarkable progress this year in our efforts to protect taxpayers following the unprecedented coordination with the states, the tax industry and the financial sector,” said IRS Commissioner John Koskinen. “Working together, this coalition has expanded its activities in many different areas, and we are focused on strengthening our systems and processes even more for the upcoming tax season.”

“It is gratifying to see how many different ways we have already identified and begun to implement changes,” said Dawn Cash, Commissioner, Oklahoma Tax Commission and President, Board of Trustees of the Federation of Tax Administrators. “Taxpayers in states across the country are benefiting from this important work.”

Summit Helps Produce Successes in 2016 Against Identity Theft; Victims Down by Half

Security Summit initiatives put in place in 2016 had a dramatic impact on the collective ability to identify and stop fraudulent returns. Key IRS statistics show decreases because Summit efforts were successful at preventing fraudulent returns from entering tax processing systems. This meant fewer bad returns, fewer bad refunds and fewer taxpayers becoming victims.

Among the examples seen by the IRS:

- **Identity theft affidavits fell sharply.** The number of people who filed affidavits with the IRS saying they were victims of identity theft dropped 50 percent during the first nine months of this year compared to 2015. The number of new affidavits filed fell to 237,750 compared to 512,278 for the first nine months of 2015.

- **More fraudulent returns stopped before processing.** IRS statistics show a nearly 50 percent drop in the number of fraudulent returns that made it into the IRS tax processing systems— another sign the Summit efforts are working up front in the tax process. Through September of this year, the IRS stopped 787,000 confirmed identity theft returns, totaling more than \$4 billion. For the same nine-month period in 2015, the IRS stopped 1.2 million confirmed identity theft returns, totaling about \$7.2 billion.
- **Fraudulent refunds fell.** The number of bank partners grew to 620 institutions from 514 institutions in 2015, enabling internal processes to continue improving. The number of suspect refunds stopped by banks and returned to the IRS dropped by more than 50 percent, to 108,539 in 2016 compared to 243,361 in 2015, demonstrating our improved ability to stop fraudulent returns before refunds are paid. The dollar amount of suspect refunds dropped to \$239 million from \$829 million in 2015.
- **Shared information stopped more bad returns.** Industry and state partners provided information that helped improve IRS fraud filters and stop additional bad tax returns, including 57,000 that would have bypassed IRS processing filters without Summit assistance.
- **Shared data elements helped identify new areas.** Several new data elements shared on tax returns from Summit partners helped the IRS stop over 74,000 suspicious returns, representing over \$372 million in refunds that were prevented from being paid.

“We’ve come a long way in a short time following the creation of the Security Summit,” Koskinen said. “But much more work remains to be done, and the partnership has agreed to take even more steps to protect taxpayers in 2017.”

More Steps Planned for 2017 Tax Season

For the 2017 filing season, the IRS and Summit partners will take additional actions. As with 2016, many of the new features will not be visible to taxpayers but will provide the IRS and states with the information they need to identify and stop fraudulent identity theft returns.

Among the new or expanded features for 2017 that will protect taxpayers and the tax system:

- New data elements transmitted by the tax industry with every tax return have been updated and expanded. In all, 37 new data elements will be added for 2017, providing additional information to strengthen the authentication that a tax return is being filed by the real taxpayer.
- The tax industry will share with the IRS and states 32 data elements from business tax returns – extending more identity theft protections to business filers as well as individuals.
- More than 20 states are working with the financial services industry to create their own version of a program that allows the industry to flag suspicious refunds before they are deposited into taxpayer accounts. Also, private sector partners are enhancing efforts to identify the “ultimate bank account” to ensure that the refunds go into the true taxpayers’ accounts – not fraudsters.
- The Form W-2 Verification Code initiative started by the IRS last year will expand to 50 million forms in 2017 from 2 million in 2016. When completing a tax return, the 16-digit verification code should be entered when prompted by tax software used by both individuals and tax professionals to validate the information on the Form W-2. The IRS anticipates the verification code will be expanded in future years for all Forms W-2.
- The software industry will continue to enhance software password requirements for individuals and tax professional users – providing additional safety prior to filing.

Taken together, these “trusted customer” features will help the IRS and states do an even better job of detecting fraudulent returns and protecting taxpayers.

As part of that effort, the Summit partners will launch a new Identity Theft Tax Refund Fraud Information Sharing and Analysis Center, or ISAC. This project, in its initial stages for 2017, will serve as an improved early warning system – identifying emerging identity theft schemes and quickly sharing that information among Summit partners so that all of the participants can enact safeguards.

Summit partners believe an ISAC ultimately promises significant gains in detecting and preventing identity theft refund fraud and will provide better data to law enforcement to investigate and prosecute identity thieves. This effort will provide all Summit partners with a threat assessment capability, early warnings about problems and insights about identity theft fraud schemes through nimble and agile information sharing.

Education Campaign Continues for Taxpayers, Tax Professionals

The Security Summit will continue its campaigns to increase awareness about data security to both taxpayers and tax preparers. Last year, the Summit partners launched the “[Taxes.Security.Together](#).” campaign to encourage taxpayers to take greater data security precautions and to learn how to recognize and avoid phishing emails that seek to trick people into providing sensitive data such as Social Security or credit card numbers.

This year, the Summit partners expanded the campaign to include tax professionals, who increasingly are being targeted by criminal syndicates. Summit partners initiated a new campaign called “[Protect Your Clients; Protect Yourself](#)” and urge tax professionals to use the best security practices available. Tax professionals should review Publication 4557, Safeguarding Taxpayer Data, to see an action check-list for ensuring data security.

As tax season approaches, the IRS and Summit partners will share more tips for tax professionals in upcoming weeks. And for taxpayers, the “Taxes.Security.Together” campaign will resume for a second year in the weeks leading up to the opening of the 2017 filing season in January with important information that taxpayers can use to protect their sensitive taxpayer and financial data.