

IRS Fact Sheet

Media Relations Office

Washington, D.C.

Media Contact: 202.317.4000

www.IRS.gov/newsroom

Public Contact: 800.829.1040

IRS, States and Tax Industry Combat Identity Theft and Refund Fraud on Many Fronts

FS-2016-01, January 2016

Combating identity theft is a top priority, and across the IRS many important steps are being taken to fight it. A key part of this involves the [Security Summit Initiative](#), a unique partnership between the IRS, state revenue departments and the private-sector tax industry leaders.

This unprecedented Security Summit Initiative is the first public-private partnership of its kind. Our objective was putting new and innovative safeguards in place to protect taxpayers in time for the 2016 filing season.

By working together, the IRS, state tax administrators and private-sector tax industry leaders will help protect taxpayers' information and the integrity of the federal and state tax systems.

In addition, through the "[Taxes. Security. Together.](#)" campaign, the Security Summit Initiative is reaching out to taxpayers to enlist their help in the battle against identity theft and refund fraud. The campaign urges everyone to take an active role in protecting their personal and financial information both online and at home. With the public's help, the Security Summit Initiative participants hope to amplify the new security protections it's putting in place.

Refund Fraud Detection and Prevention

For several years, the IRS has fought aggressively against refund fraud, which includes identity theft. In calendar year 2015, through November, the IRS rejected or suspended the processing of 4.8 million suspicious returns. So far, we stopped 1.4 million confirmed identity theft returns, totaling \$8 billion. Additionally, through November we stopped \$2.9 billion worth of refunds in other types of fraud. That's a total of \$10.9 billion in confirmed fraudulent refunds protected.

Many new safeguards in place will be invisible to taxpayers but invaluable in helping fight against the stolen identity refund fraud. Many changes are designed to better authenticate the taxpayer's identity and the validity of the tax return at the time of filing.

The most visible change will be new password protections for private-sector tax software accounts. New standards require a minimum 8-digit password using a combination of letters, numbers and special characters. There also will be new security questions, new lock-out features and new ways to verify emails.

The password standards are intended to help protect taxpayers from identity thieves who take over their software accounts and file fraudulent tax returns using their names and Social Security numbers.

Many states also have enacted their own new safeguards. In an effort to protect you, some states may request driver's license numbers and release refunds only after verifying data or issue paper refunds. Visit your [state's tax agency web site](#) to see if there are changes for 2016. (Although you may e-file your federal and state tax returns together, they are processed separately by the IRS and your state tax agency.) Please note taxpayers will not need a driver's license to file their federal return.

The tax software industry also will be sharing many new data elements with the IRS and the states which will help determine if the return is valid. The IRS continues to increase both the number and efficiency of the identity theft data models and filters that are used to identify potentially fraudulent returns. These pre-refund filters stop the vast majority of fraudulent returns. Additionally, the IRS continues to expand its partnerships with financial institutions to identify and stop fraudulent refunds.

The IRS, states and tax industry also will routinely share information about identity theft trends or new schemes so that all parties can react quickly and appropriately.

Increasing Efforts to Help Victims

The IRS understands that identity theft is a frustrating, complex process for victims. While identity thieves steal information from sources outside the tax system, the IRS is often the first to inform a victim that identity theft has occurred. The IRS is working hard to resolve identity theft cases as quickly as possible.

While the IRS has made considerable progress in this area, more work remains. Fighting identity theft is an ongoing battle as identity thieves continue to create new ways of stealing personal information and using it for their gain. Identity theft cases are among the most complex handled by the IRS. The IRS is continually reviewing processes and policies to minimize incidents of identity theft and to help those who find themselves victimized. Among the steps underway to help victims:

Centralizing victim assistance work: During 2015, the IRS centralized most of its victim assistance work within one function and created an Identity Theft Victim Assistance organization. The agency also is reviewing its process and procedures to better serve taxpayers and to help reduce the time it takes to resolve cases. A typical case can take 120 days to resolve, but complex cases can take longer.

IP PIN: The IRS Identity Protection PIN (IP PIN) is a unique six-digit number that is assigned annually to victims of identity theft. It helps show a particular taxpayer is the rightful filer of the return. For 2016, everyone with an IP PIN must have it entered on the return. This includes primary and secondary taxpayers as well as dependents. Please be aware: some states also may have new security PINs this year. If the IRS issued you an IP PIN you must use it to file your federal tax return.

IP PIN Pilot: The IRS will continue its IP PIN pilot program that allows taxpayers who filed tax returns last year from Florida, Georgia or the District of Columbia to opt into the IP PIN program.

IRS Criminal Investigation

In the most recent three fiscal years, [Criminal Investigation](#) (CI) has helped convict approximately 2,000 identity thieves.

In fiscal year 2015, the IRS initiated 776 identity theft related investigations, which resulted in 774 sentencing through CI enforcement efforts. The courts continue to impose significant jail time with the average months to serve in fiscal year 2015 at 38 months— the longest sentencing being over 27 years.

The nationwide [Law Enforcement Assistance Program](#) (LEAP) provides for the disclosure of federal tax return information associated with the accounts of known and suspected victims of identity theft with the express written consent of those victims. There are now more than 1,100 state/local law enforcement agencies from 48 states participating. For FY2015, more than 6,700 requests were received from state and local law enforcement agencies.

The Identity Theft Clearinghouse (ITC) continues to develop and refer identity theft refund fraud schemes to Criminal Investigation Field Offices for investigation. Since its inception in FY2012, ITC has received over 10,750 individual identity theft leads. These leads involved approximately 1.72 million returns with over \$11.4 billion in refunds claimed.

CI continues to be the lead agency or actively involved in more than 70 multi-regional task forces or working groups including state/local and federal law enforcement agencies solely focusing on identity theft.

More information is available at IRS.gov/identitytheft, including the [Taxpayer Guide to Identity Theft](#).