

**Identity Theft
Don't Be a Victim**

How IRS and Tax Professionals Can
Prevent Identity Theft and Assist
Taxpayers Who Are Victims



Narina Bchtkian
Stephen Connor
Senior Stakeholder Liaison
IRS Small Business/Self-Employed Division
December 2012
Federal and State Tax Institute

IRS and Privacy

- Maintaining close security of IRS systems and proper protection of taxpayer information is a top priority for the IRS
- Protecting privacy and preventing identity theft helps to instill confidence and public trust in tax administration



**Laws for Tax-Related Identity
Protection**

- IRC § 7216
- USC § 6713
- Privacy Act (5 USC 552a)
- Freedom of Information Act (5 USC 552)



ID Theft Continued Major Problem

- Number one consumer complaint reported to FTC for past 12 years
- An average victim now spends 12 hours and \$354 out of pocket to resolve crime
- Incidents related to government benefits
 - most common
 - more complex
 - more time and money to detect and resolve



3

Recognizing ID Theft

- Taxpayers may have awareness that they are
- victims of ID theft in several ways:
 - E-file return rejects because SSN used on another return
 - IRS contacts taxpayer about reported income taxpayer did not earn
 - Taxpayer begins receiving bills or notices for unauthorized purchases or actions



4

ID Theft Affect on Clients' Taxes

- Scenario 1: Refund-related crime, Identity thief uses stolen SSN to file forged tax return and obtain refund early in the filing season
- Scenario 2: Employment-related crime, Identity thief uses stolen SSN to obtain employment



5

Combating Tax-Related ID Theft

- Goal: IRS strives to prevent identity theft and detect refund fraud *before* it occurs and assist taxpayers who are victims.
- IRS has developed a comprehensive identity protection program that uses a three-pronged approach
 - Prevention and detection
 - Protection
 - Victim assistance



IRS Prevention and Detection Efforts

- Using business filters and rules to analyze returns filed on ID theft victim accounts to ensure legitimate returns are accepted and false returns rejected
- Placing identity theft indicators on taxpayer accounts to track and manage identity theft incidents
- Identifying and investigating refund fraud



Business Filters

- *Identify* possible identity theft
- *Ensure* only legitimate returns are processed
- *Flag* questionable returns for manual review to validate legitimacy
- *Reject* fraudulent returns



ID Theft Indicators

- *Prevent* victims from facing the same problems every year
- *Distinguish* legitimate tax returns from fraudulent returns
- *Identify and track* tax-related identity theft problems
- *Measure* the problem, *monitor* victims' accounts, and *develop* processes to resolve



ID Theft Indicators

- They reflect different types and risks of identity theft
 - Refund-related identity theft
 - Employment-related identity theft
 - Accounts with no filing requirement
 - Increased risk due to a lost item such as a wallet



New Business Rules to Deter False Returns

- Suspension of fraudulent return detection, ID verification letter sent to filer
 - If unable to establish identity, return archived without processing
 - If able (and no compliance issues found), refund released



IRS Victim Protection Efforts

- Notifying taxpayers when identity theft has affected their tax accounts
- Sending a notification letter to a victim when an identity theft indicator is placed on the victim's account
- Issuing victims Identity Protection PINs



ID Protection PIN

- IP PIN is a six-digit number assigned to taxpayers who:
 - Were identified as identity theft victims
 - Submitted required documentation
 - Had their account issues resolved



Key IP PIN Information

- The IP PIN is specific to the tax year
- A new IP PIN is issued every year
- The IP PIN should not be confused with the electronic signature 'self-select' PIN
- Allows legitimate return to bypass identity theft filters
- Prevents processing of fraudulent returns
- Allows taxpayers to avoid delays in their federal tax return processing



IRS Victim Assistance Efforts

- Develop specialized units quickly and efficiently resolve identity theft cases
- Provide more training for employees who assist ID theft victims
- Step up outreach and education so taxpayers can prevent and resolve tax-related ID theft issues quickly



11

Identity Protection Specialized Unit

- Central point of contact for taxpayers who are reporting their identities as stolen
- Toll-free: 800-908-4490
- Monday - Friday, 7 a.m. - 7 p.m. local time
- Taxpayers may self-report they are victims before tax accounts are affected



12

IRS Specialized Groups

- Functions within the Service are developing 'specialized groups' of employees dedicated to ID theft
- Taxpayer benefits:
 - More streamlined processing of ID theft cases
 - Single point of contact upon case commencement
 - Prioritization of all ID theft cases
 - Enhanced communication with the taxpayer



13

Employee Training

- Updated training for telephone representatives to ensure proper level of sensitivity when dealing with ID theft victims
- Developed training for employees who are not telephone assistants but interact with taxpayers or otherwise work ID theft cases



Outreach

- Launched new section on IRS.gov dedicated to ID theft matters
- Heightened awareness of ID protection through filing season messages
- Conducted outreach to educate preparers about IP PIN and ID theft
- Worked closely with software developers on inclusion of IP PIN



Tax Pro Responsibilities

- Educate clients to safeguard personal information
- Advise to regularly check credit reports and other financial records
- Remind them the IRS does not initiate contact with taxpayers by email to request personal or financial information
 - Any type of electronic communication
 - text messages
 - social media channels



Actions for ID Theft Victims

- Contact the IPSU
- Contact financial institutions
- Contact credit bureaus to place a fraud alert and obtain free copies of credit reports
- File police report with local law enforcement
- Contact Federal Trade Commission, visit www.consumer.gov/idtheft/index.html



Online ID Theft

- Phishing via the phishing Web form
- Malware by downloading malicious executable code
- Email via email (or money order)
- Vishing via the faxback form
- Stock via email (or wire transfer)



Online Fraud Mitigation by IRS

- De-register malicious domains
- Remove malicious/fraudulent content
- Suspend email accounts
- Disable FAX numbers
- Report unregistered securities entities



Receipt of Suspicious IRS-Related Communications

- Report all unsolicited email claiming to be from the IRS to phishing@irs.gov
- Go to IRS.gov, click on 'Report Phishing' on the bottom of web page



Preventing Online ID Theft

- Avoid phishing scams
- Secure computers
- Use strong passwords
- Limit accessibility of personal information
- Never answer 'yes' to pop-up screens



IRS's Continued Fight Against ID Theft

- ID theft is an ongoing battle for IRS
- ID theft landscape is constantly changing, as identity thieves continue to create new ways of stealing personal information
- IRS is committed to continuing to improve our identity theft protection programs



Contact Information

Name: Narina Bchtikian
Phone Number: 215-861-1061
E-Mail Address: Narina.Bchtikian@irs.gov



Contact Information

Name: Stephen Connor
Phone Number: 215-861-1405
E-Mail Address: Stephen.Connor@irs.gov


