Identity Theft Information for Tax Professionals

August 2017
2017 Filing Season

• Processed 135.6 million tax returns
• Issued 97 million refunds
• Dispersed $270 billion in refunds
  — Average refund: $2,700
• 69 percent of IRS collections from payroll managers
Voluntary Accelerated Information Return Processing Program
- 22 million private sector W2s last year
- 6 million government agencies
Objective: Speed verification of taxpayer income/combat fraud
Analysing benefits of program in light of PATH ACT acceleration requirements
Tax-Related Identity Theft Actions

- Improved IDT filters
- Limited direct deposits
- Locked deceased taxpayers accounts
- Partnered with banks to ID suspicious refunds
- Created Identity Protection PINs
- Convicted more than 2,000 identity thieves
Security Summit Initiatives - 2016

- Shared data elements from return
- Required stronger password protocols
- Agreed on ISAC (Information Sharing & Assessment Center)
- Agreed on stronger cybersecurity framework
- Two-factor authentication protections for certain IRS.gov tools
Initiative Results for 2016

- More returns stopped before entering processing pipeline
- Confirmed identity theft returns dropped 30 percent
- Fraudulent refunds identified by banks fell 50 percent
- People identifying themselves as IDT victims fell 46 percent
Security Summit Initiatives - 2017

- Shared data from business tax returns
- W-2 Verification Code test expanded
- Additional data elements identified
- States partnering with banks
- Summit partners working to identify “ultimate bank accounts”
- New Payroll Professional Work Group
Form W-2 Verification Code Initiative

Verification Code:

• 16 alphanumeric characters
• A unique code on each W-2, calculated using data on that form
• In a separate box, labeled “Verification Code,” on copies
  — B ("To be filed with employee's federal tax return")
  — C ("For employee's records")

W-2 Instructions: Verification Code:

• If this field is populated, enter this code when it is requested by your tax return preparation software. It is possible your software or preparer will not request the code. The code is not entered on paper-filed returns.
• Focus on authentication
• Expand ISAC (Information Sharing Assessment Center) capabilities
• W-2 Verification Code test will continue into next year
• “Verification Code” box will appear on 2017 Form W-2
IRS Identity Theft Victim Assistance
The Process and the Improvements
Tax-Related Identity Theft

Three Warning Signs

• Taxpayer learns of a duplicate SSN either from an IRS notice or e-file return rejects

• IRS notice about additional tax owed, refund offset or collection action when no return filed

• Taxpayer receives information from an employer unknown to them
Tax-Related Identity Theft

- Taxpayer Protection Program generates:
  - Letter 4883C for prior-year suspicious returns
  - Letter 5071C for current-year suspicious returns
    - Most common correspondence
    - Taxpayer self-verifies at Idverify.IRS.gov
  - Letter 5447C for suspicious returns with foreign addresses
Steps for Victims of Tax-Related Identity Theft

- Complete and file IRS Form 14039
- Respond to any IRS letters or notices
- Continue to pay taxes, even if by paper
- Place a “fraud alert” on credit accounts by contacting one of the three main credit bureaus
- Close any accounts opened by criminals
- File a complaint with the FTC
Form 14039
Identity Theft Affidavit

Section A - Check the following boxes in this section that apply to the specific situation you are reporting (required for all)

1. I am submitting this Form 14039 for myself (required)
2. This Form 14039 is submitted in response to a Notice or Letter received from the IRS (required)
   - Please check box 1 in Section B and see special mailing and handling instructions on reverse side of this form.
   - Please provide Notice or Letter numbers, on the line to the right.
3. I am submitting this Form 14039 on behalf of my dependent child or dependent relative
   - Please complete Section E on reverse side of this form.
   - Caution: If filing this on behalf of your dependent child or dependent relative, filing this form will protect his or her tax account but it will not prevent the victim in Section B below from being claimed as a dependent by another person.
4. I am submitting this Form 14039 on behalf of another person (other than my dependent child or dependent relative)
   - Please complete Section E on reverse side of this form.

Section B - Reason for Filing this Form (required)

Check only one of the following boxes that apply to the person listed in Section B below:

☐ 1. Someone used my information to file taxes
☐ 2. I don’t know if someone used my information to file taxes, but I’m a victim of identity theft

Please provide an explanation of the identity theft issue, how you became aware of it, and provide relevant dates.
If needed, please attach additional information and/or pages to this form.

Section C - Name and Contact Information of Identity Theft Victim (required)

Victim's last name
Current mailing address (apartment or suite)
Current city
Tax years you experienced identity theft (if not known, enter “unknown” in one box below)
What is the last year you filed a return
Address used on last filed tax return (if different than current)
City on last tax return filed
State ZIP code
Telephone number with area code (optional, if deceased, please indicate deceased)
Language (if you would like to be contacted)

Section D - Penalty for Perjury Statement and Signature (required)

Under penalty of perjury, I declare that, to the best of my knowledge and belief, the information entered on this Form 14039 is true, correct, complete, and made in good faith.
Signature of taxpayer, or representative, conservator, parent or guardian
Centralizing Victim Assistance

- Most victim assistance work centralized under one director
- New Identity Theft Victim Assistance organization created
- Policy and operations under one leadership team
- More consistent treatment for taxpayers
- Reviewing IDTVA process for improvements
About the Identity Protection PIN (IP PIN)

- Six-digit number that adds an additional layer of protection along with the SSN or ITIN
- Victims notified once tax-related IDT case resolved
- Taxpayer will receive a CP01A notice containing a new IP PIN each year
- Some taxpayers have the option of getting an IP PIN from IRS.gov
- Enter numbers for all IP PIN holders
Recap Victim Assistance Changes

- We’ve centralized most of identity theft victim assistance work
- We’re reviewing victim assistance procedures
- We’re continuing to test the IP PIN in three locations, and
- We’re strengthening verification procedures for Get Transcript and IP PIN
IRS Impersonation Scams

- IRS doesn’t make threats of lawsuits or jail
- IRS does not use email, texts or social media to ask for personal or financial data
- Impersonation scams netted $29 million from more than 5,500 victims
Six Steps to Protect Your Clients and Protect Yourself from Identity Theft
It CAN happen to you!

- Cybercriminals targeting tax professionals
  - January-May 2017 – 177 tax professionals reported data breaches
  - IRS receiving reports from 3 to 5 tax pros each week
- Simple steps can help protect your clients and your business
1. Review Pub 4557

- Publication 4557, Safeguarding Taxpayer Data
  - Checklist to review current security practices
  - Identify your risks
  - Create a security plan
  - Review your plan annually
### Checklist 1

#### Administrative Activities

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Complete a Risk Assessment. Identify the risks and potential impacts of unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems that can be used to access taxpayer data. How vulnerable is your customer’s data to theft, disclosure, unauthorized alterations or unrecoverable loss? What can you do to reduce the impact to your customers and your business in such an event? What can you do to reduce vulnerability?</td>
</tr>
<tr>
<td>2.</td>
<td>Write and follow an Information Security Plan that:</td>
</tr>
<tr>
<td></td>
<td>- Addresses every item identified in the risk assessment.</td>
</tr>
<tr>
<td></td>
<td>- Defines safeguards you want affiliates and service providers to follow.</td>
</tr>
<tr>
<td>3.</td>
<td>Requires a responsible person to review and approve the Information Security Plan.</td>
</tr>
<tr>
<td>4.</td>
<td>Requires a responsible person to monitor, revise, and test the Information Security Plan on a periodic (recommended annually) basis to address any system or business changes or problems identified.</td>
</tr>
<tr>
<td>5.</td>
<td>Periodically (recommended annually) perform a Self-Assessment to:</td>
</tr>
<tr>
<td></td>
<td>- Evaluate and test the security plan and other safeguards you have in place.</td>
</tr>
<tr>
<td></td>
<td>- Document information safeguards deficiencies, create and execute a plan to address them.</td>
</tr>
<tr>
<td>6.</td>
<td>Retain a copy of the Self-Assessment and ensure it is available for any potential reviews.</td>
</tr>
<tr>
<td>7.</td>
<td>If required by the FTC Privacy Rule, provide privacy notices and procedures to your customers.</td>
</tr>
<tr>
<td>8.</td>
<td>Specify in contracts with service providers the safeguards they must follow and monitor how they handle taxpayer information.</td>
</tr>
<tr>
<td>9.</td>
<td>Ask service providers to give you a copy of their written security policy on safeguarding information.</td>
</tr>
</tbody>
</table>
### Checklist 2

#### Facilities Security

<table>
<thead>
<tr>
<th>Item</th>
<th>Complete</th>
<th>Done</th>
<th>NA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Item 1**: Protect from unauthorized access and potential danger (e.g., theft, floods and tornadoes) all places where taxpayer information is located.
- **Item 2**: Write procedures that prevent unauthorized access and unauthorized processes.
- **Item 3**: Ensure that taxpayer information, including data on hardware and media, is not left un-secured on desks or copiers, in mailboxes, vaxxies, trash cans or rooms in the office or at home where unauthorized access can occur.
- **Item 4**: Authorize and control delivery and removal of all taxpayer information, including data on hardware and media.
- **Item 5**: Lock doors to file rooms and/or computer rooms.
- **Item 6**: Provide secure disposal of taxpayer information, such as shredders, burn boxes or temporary file areas until it can be securely disposed.

In 2015, the IRS called for a Security Summit to increase cooperation in place to fight identity thieves. Tax preparers are critical players in this effort, because of the taxpayer information they store, increasingly a target for identity thieves.
## Checklist 3

### Personnel Security

<table>
<thead>
<tr>
<th>Item</th>
<th>Checklist</th>
<th>Date</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Create and distribute Rules of Behavior that describe responsibilities and expected behavior regarding computer information systems as well as paper records and usage of taxpayer data. Have all information system users complete, sign, and submit an acknowledgement that they have read, understood, and agree to comply with the rules of behavior. An example of rules of behavior can be found in Appendix A of NIST SP 800-19 Guide for Developing Security Plans for Federal Information Systems.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>2. Ensure personnel from third-party providers such as service bureaus, contractors, and other businesses providing Information Technology services meet the same security requirements as those applied to your personnel.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>3. Address Rules of Behavior for computer system management.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>4. When interviewing prospective personnel, explain the expected Rules of Behavior.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>5. When possible, perform a background and/or reference check on new employees who will have contact with taxpayer information. Conduct background screenings that are appropriate to the sensitivity of an assigned position.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>6. Screen personnel prior to granting access to any paper or electronic data. This will help ensure their suitability for a position requiring confidentiality and trust.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>7. Hire personnel who will have access to taxpayer information sign nondisclosure agreements on the use of confidential taxpayer information.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>8. Develop and enforce formal compliance policies and processes, including possible disciplinary action, for all personnel who do not comply with the business’ established information security policies and procedures.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>9. Terminate access to taxpayer information (e.g., login IDs and passwords) for those employees who are terminated or who no longer need access.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>10. For each employee who is terminated, conduct an exit interview and ensure the employee returns property that allows access to taxpayer information (e.g., laptops, media, keys, identification cards and building passes).</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>11. Train staff on Rules of Behavior for access, non-disclosure and safeguards of taxpayer information. Provide refresher training periodically.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
2. Use Best Security Practices

- Learn to recognize and avoid phishing emails and phishing scams
- Use strong security software to protect against malware and viruses
- Use security functions on your tax prep software
- Encrypt taxpayer data
- Use strong, unique passwords
3. Lose data? Call IRS immediately

- Contact your local Stakeholder Liaison
  - www.irs.gov keyword search “stakeholder liaison” to find contact for your state
  - IRS may be able to help protect your clients if notified quickly

- Review “Data Loss Information for Tax Professionals” at IRS.gov/identitytheft for additional steps
4. Maintain, monitor & protect EFIN

- Keep e-File Application up-to-date with names, addresses and phone numbers
- Monitor use of your EFIN weekly via your e-File application
  - Monitor PTIN filings as well from PTIN account
- Protect EFIN from theft; avoid e-Services scams
- NOTE: IRS only official source for EFINs
5. Educate Clients and Staff

- Share Publication 4524, Security Awareness for Taxpayers, with clients
- Ensure all staff are aware of and maintain security protocols
6. Spread the Word on W2 Scam

- Poses as company executive, asks payroll employee for list of all employees W2s
  - 50 victims last year; 200 this year
  - Hundreds of thousands of new IDT victims
- Targets: businesses, public schools, universities, tribes
- Employer/victims should email dataloss@irs.gov and provide POC
Recap

1. Review Pub 4557 to create a security plan
2. Use best security practices at all times
3. Contact IRS immediately of data loss
4. Maintain, monitor and protect EFIN
5. Educate clients and staff
6. Warn employers about W2 scam

Bonus – stay in contact with IRS, via e-News for Tax Professionals, Quick Alerts and Social Media
QUESTIONS?
Protección de Identidad: Prevención, Detección y Asistencia a Víctimas

El robo de identidad es una carga para sus víctimas y representa un desafío a los negocios, organizaciones y agencias gubernamentales, incluyendo al IRS. El IRS combate el robo de identidad relacionado a los impuestos por medio de una estrategia agresiva de prevención, detección y asistencia a las víctimas. Estamos progresando en rímas. Pero aún así sigue siendo una de nuestras prioridades mayores.

El robo de identidad relacionado a los impuestos sucede cuando alguien utiliza su número de Seguro Social robado y presenta una declaración de impuestos reclamando un reembolso fraudulento. Si usted llega a ser una víctima de este crimen, estamos comprometidos a ayudarlo a resolver su caso lo más pronto posible.

Información y orientación

<table>
<thead>
<tr>
<th>Individuos</th>
<th>Profesionales de impuestos (en inglés)</th>
<th>Negocios</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guía para el contribuyente sobre el robo de identidad</td>
<td>Información acerca del robo de identidad para profesionales de impuestos</td>
<td>Robo de Identidad del SSN/Formulario W-2: Información para proveedores de servicios de nómina y negocios (en inglés)</td>
</tr>
<tr>
<td>Información de robo de identidad para los contribuyentes (PDF)</td>
<td>Información acerca del robo de identidad para preparadores de impuestos</td>
<td>Información para negocios sobre el robo de identidad y filtración de información.</td>
</tr>
<tr>
<td>Información sobre el robo de identidad relacionado al empleo</td>
<td>Publicación 6199 Guía para el preparador de impuestos sobre el Robo de Identidad (PDF)</td>
<td>Los socios de la cumbre de seguridad actualizan para el 2017 las iniciativas sobre el robo de identidad (en inglés)</td>
</tr>
<tr>
<td>Filtración de información: la información relacionada con los impuestos</td>
<td>Guía para el preparador de impuestos sobre el Robo de Identidad de Negocios</td>
<td></td>
</tr>
</tbody>
</table>
What is tax-related identity theft?
Tax-related identity theft occurs when someone uses a stolen Social Security number to file a tax return claiming a fraudulent refund. Thieves also may use stolen Employer Identification Numbers to create false Forms W-2 to support refund fraud schemes.

Warning signs for individual clients
Your client’s SSN has been compromised, putting them at risk when:
• A return is rejected; IRS reject codes indicate the taxpayer’s SSN already has been used.
• Your client notices activity on or receives IRS notices regarding a tax return after all tax issues have been resolved, refund paid or account balances have been paid.
• An IRS notice indicates your client received wages from an employer unknown to them.

Remember: You must have a power of attorney on file and authenticate your identity before an IRS customer service representative can provide you with any taxpayer information.

Warning signs for business clients
• Your client’s return is accepted as an amended return, but the taxpayer has not filed a return for that year.
• Your client receives IRS notices about fictitious employees.
• Your client notices activity related to or receives IRS notices regarding a defunct, closed or dormant business after all account balances have been paid.

Tax preparers also can become targets of criminals. Remember to follow the security guidelines outlined in Publication 1345. Online providers who experience a data breach must contact the IRS within one business day.

Assisting victims of identity theft
The Federal Trade Commission, the lead federal agency for identity theft, recommends these steps:
2. Contact one of the major credit bureaus to place a fraud alert on your records:
   • www.Equifax.com 1-888-766-0008
   • www.Experian.com 1-888-397-3742
   • www.TransUnion.com 1-800-680-7289
3. Close any financial or credit accounts opened fraudulently.

IRS victim assistance
In addition to the FTC recommendations, you should take these steps if clients’ SSNs are compromised and they suspect or know they are victims of tax-related identity theft:
• Respond promptly to IRS notices; your client may be directed to IDVerify.IRS.gov to validate their identity
• Complete Form 14039, Identity Theft Affidavit, if your client’s e-file return rejects because of a duplicate SSN or you are instructed to do so. This form allows us to put an indicator on the client’s tax records for questionable activity.
• Clients should continue to file returns and pay taxes, even if it must be done by paper, while the case is being researched.
• If you previously contacted the IRS and did not have a resolution, call us for specialized assistance at 1-800-908-4490.
• Be aware that the nature of these cases is complex.

Resources for tax preparers
• www.identitytheft.gov (FTC web site)
• www.IRS.gov/identitytheft
• Pub 1345, Handbook for Authorized IRS e-file Providers (Security)
• Pub 4557, Safeguarding Taxpayer Data
• Pub 4600, Safeguarding Taxpayer Information
• Pub 4535 (EN-SP), Identity Theft Prevention and Victim Assistance
• Search IRS.gov, Keywords: Identity Theft
What is tax-related identity theft?
Tax-related identity theft occurs when someone uses your stolen Social Security number (SSN) to file a tax return claiming a fraudulent refund. If you become a victim, we are committed to resolving your case as quickly as possible.

You may be unaware that this has happened until you e-file your return and discover that a return already has been filed using your SSN. Or, the IRS may send you a letter saying it has identified a suspicious return using your SSN.

Know the warning signs
Be alert to possible tax-related identity theft if you are contacted by the IRS about:

• More than one tax return was filed for you,
• You owe additional tax, have a refund offset or have had collection actions taken against you for a year you did not file a tax return, or
• IRS records indicate you received wages or other income from an employer for whom you did not work.

Steps for victims of identity theft
If you are a victim of identity theft, the Federal Trade Commission recommends these steps:

• File a complaint with the FTC at identitytheft.gov.
• Contact one of the three major credit bureaus to place a ‘fraud alert’ on your credit records:
  - www.Equifax.com 1-888-766-0008
  - www.Experian.com 1-888-397-3742
  - www.TransUnion.com 1-800-680-7289
• Close any financial or credit accounts opened by identity thieves

If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these additional steps:

• Respond immediately to any IRS notice; call the number provided.
• Complete IRS Form 14039, Identity Theft Affidavit, if your e-file return rejects because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach form to your paper return and mail according to instructions.

• Continue to pay your taxes and file your tax return, even if you must do so by paper.
• If you previously contacted the IRS and did not have a resolution, contact us for specialized assistance at 1-800-908-4490. We have teams available to assist.

More information is available at: IRS.gov/identitytheft or FTC’s identitytheft.gov.

About data breaches and your taxes
Not all data breaches or computer hacks result in tax-related identity theft. It’s important to know what type of personal information was stolen.

If you’ve been a victim of a data breach, keep in touch with the company to learn what it is doing to protect you and follow the “Steps for victims of identity theft.” Data breach victims should submit a Form 14039, Identity Theft Affidavit, only if your Social Security number has been compromised and IRS has informed you that you may be a victim of tax-related identity theft or your e-file return was rejected as a duplicate.

How you can reduce your risk
Join efforts by the IRS, states and tax industry to protect your data. Taxes. Security. Together. We all have a role to play. Here’s how you can help:

• Always use security software with firewall and anti-virus protections. Use strong passwords.
• Learn to recognize and avoid phishing emails, threatening calls and texts from thieves posing as legitimate organizations such as your bank, credit card companies and even the IRS.
• Do not click on links or download attachments from unknown or suspicious emails.
• Protect your personal data. Don’t routinely carry your Social Security card, and make sure your tax records are secure.

See Publication 4524, Security Awareness for Taxpayers to learn more.

NOTE: The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.
TAXES. SECURITY. TOGETHER.

The IRS, the states and the tax industry are committed to protecting you from identity theft. We’ve strengthened our partnership to fight a common enemy – the criminals – and to devote ourselves to a common goal – serving you. Working together, we’ve made many changes to combat identity theft, and we are making progress. However, cybercriminals are constantly evolving, and so must we. The IRS is working hand-in-hand with your state revenue officials, your tax software provider and your tax preparer. But, we need your help. We need you to join with us. By taking a few simple steps, you can better protect your personal and financial data online and at home.

Please consider these steps to protect yourselves from identity thieves:

Keep Your Computer Secure

- Use security software and make sure it updates automatically; essential tools include:
  - Firewall
  - Virus/malware protection
  - File encryption for sensitive data
- Treat your personal information like cash, don’t leave it lying around
- Check out companies to find out who you’re really dealing with
- Give personal information only over encrypted websites – look for “https” addresses.
- Use strong passwords and protect them
- Back up your files

Avoid Phishing and Malware

- Avoid phishing emails, texts or calls that appear to be from the IRS and companies you know and trust, go directly to their websites instead
- Don’t open attachments in emails unless you know who sent it and what it is
- Download and install software only from websites you know and trust
- Use a pop-up blocker
- Talk to your family about safe computing

Protect Personal Information

Don’t routinely carry your social security card or documents with your SSN. Do not overshare personal information on social media. Information about past addresses, a new car, a new home and your children help identity thieves pose as you. Keep old tax returns and tax records under lock and key or encrypted if electronic. Shred tax documents before trashing.

Avoid IRS Impersonators. The IRS will not call you with threats of jail or lawsuits. The IRS will not send you an unsolicited email suggesting you have a refund or that you need to update your account. The IRS will not request any sensitive information online. These are all scams, and they are persistent. Don’t fall for them. Forward IRS-related scam emails to phishing@irs.gov. Report IRS-impersonation telephone calls at www.tigta.gov.

Additional steps:

- Check your credit report annually; check your bank and credit card statements often;
- If you are an identity theft victim whose tax account is affected, review www.irs.gov/identitytheft for details.