Nichols Patrick

A Division of the Loscalzo Institute

Firms Under Attack: Securing Information in Today's CPA Firm

Edward K. Zollars, CPA

www.currentfederaltaxdevelopments.com

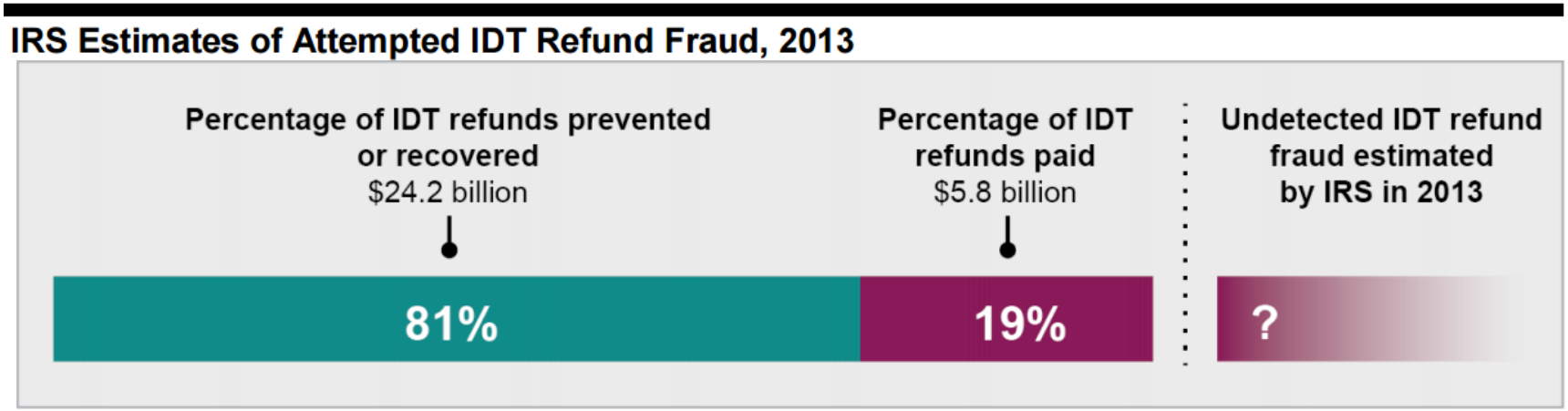
www.cperesources.com

2016 Oklahoma Tax Institute

Nichols Patrick
A Division of the Loscalzo Institute

Tax Related Identity Theft

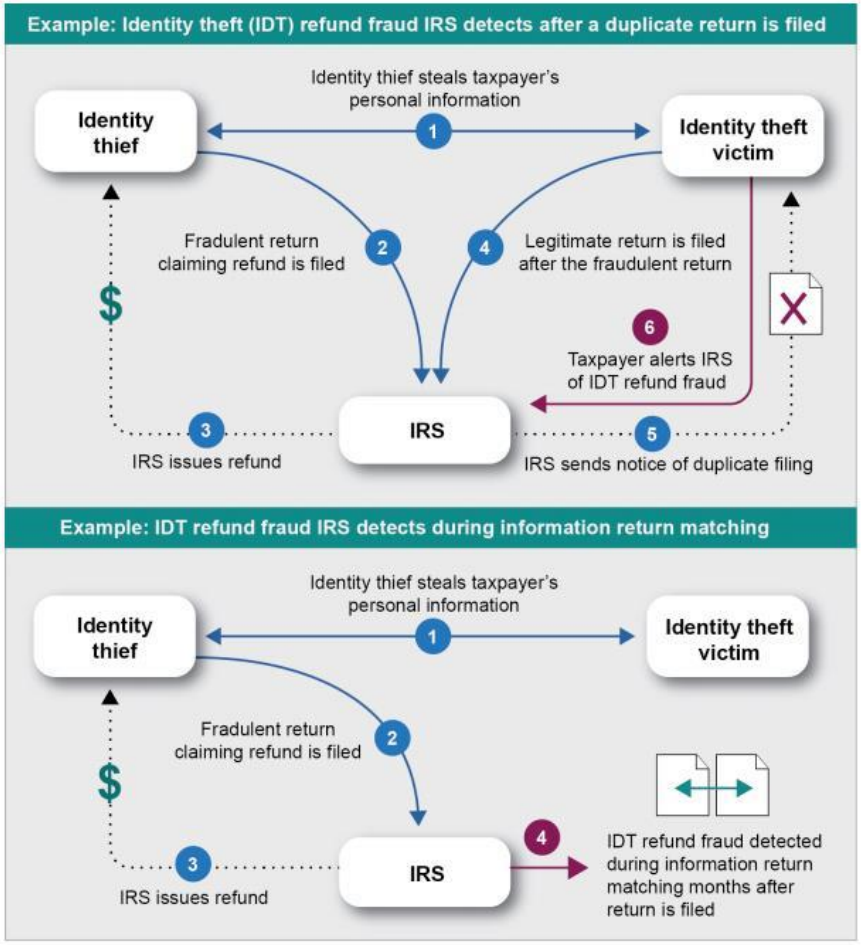
GAO Report



Source: GAO analysis of IRS data. | GAO-15-119

GAO Report

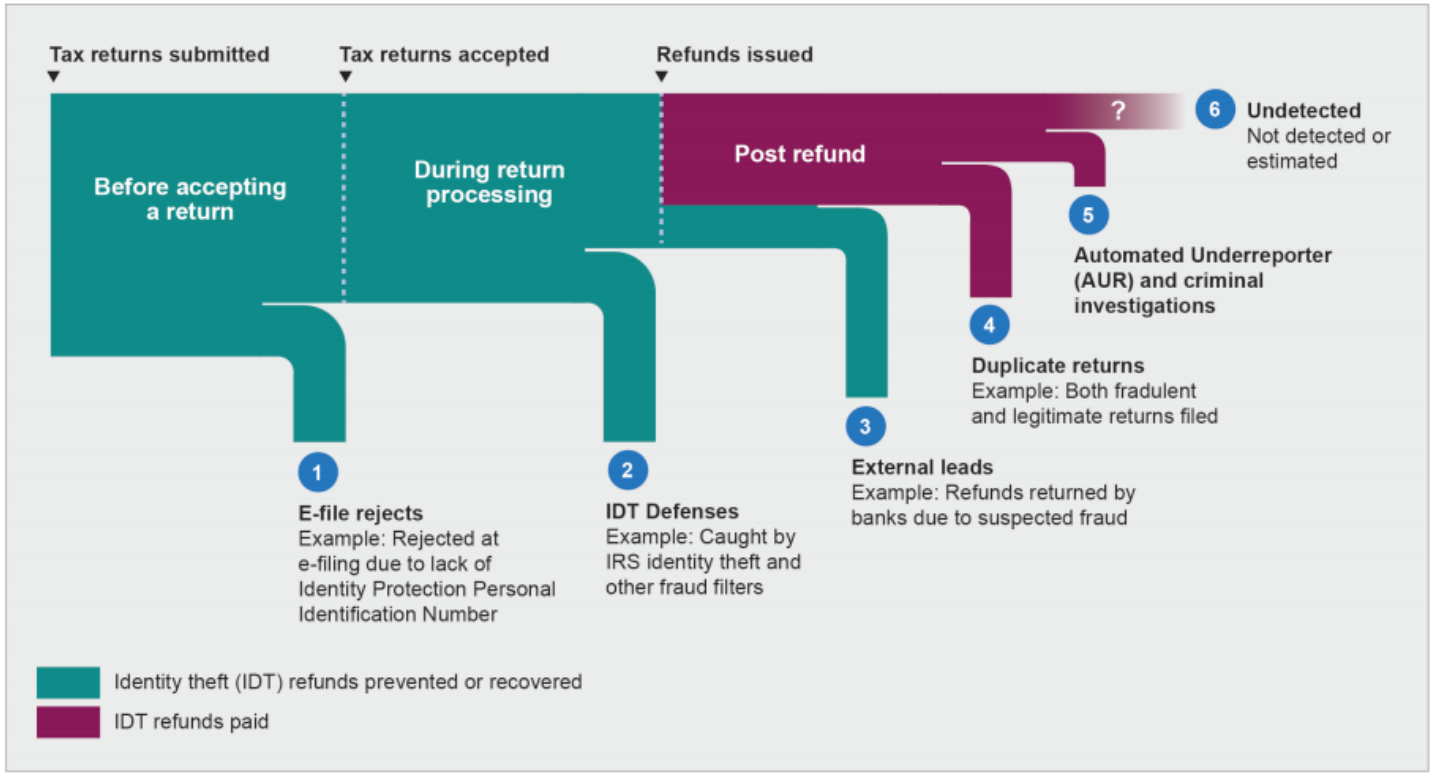
Figure 1: Detecting IDT After Refunds are Issued: Two Examples



Source: GAO analysis of IRS documents. | GAO-15-119

GAO Report

Figure 2: Illustration of IRS *Identity Theft Taxonomy*



Source: GAO analysis of *IRS Taxonomy.* | GAO-15-119

Why Does Identity Theft Exist?

- Identity theft is simply very profitable – see the "First Lady of Tax Fraud"
- Information Leakage makes it easy
  - Many entities have been compromised
  - Organizations begin building databases of such information
- Note that a CPA firm's servers contain a wealth of extraordinarily sensitive and valuable information
  - Can be used to steal identities for other purposes
  - Also looking to take over systems to use firm's software to file fraudulent returns

Nichols Patrick
A Division of the Loscalzo Institute

Assisting the Victim of Tax Related Identity Theft

Refunds Due to Taxpayers

- Identity theft causes return processing to stop
- Will create various issues
  - Cash flow problems for taxpayer that has plans for the refund
  - May block
    - Purchase of real estate
    - Refinancing
  - Might get some help from taxpayer advocate—but don't count on it

Obtaining Copies of Fraudulent Returns

- IRS procedures on providing copies to fraudulent returns to affected taxpayers
- Can be useful to see extent of information held by ID thieves
- May indicate other areas where taxpayer may run into identity theft
- But is not a fast process…

Nichols Patrick
A Division of the Loscalzo Institute

The IP-PIN Program

The IP PIN Program in Operation

- Meant to give protection to taxpayers victimized by ID theft
- However, ran into problem (instructive for any sort of solution)
  - Taxpayers lost IP PINs and wanted them reissued quickly
  - IRS established a system to recover IP-PIN using “out of wallet” questions (“Knowledge Based Authentication”)
- KBA’s problem—ID thieves have access to databases of combined information from leaks

CPA's Responsibilities with Client Data

Preparer's Responsibilities

- Fact Sheet (FS-2015-24) and Publication 4557 outline steps that should be taken
  - Security software
  - Education program for all employees
  - Strong passwords changed periodically
  - Secure wireless connections
  - Backups
  - Secure paper files
  - Access e-services weekly to look for unusual activity
- FTC guidance for businesses that have a breach

IRS Warning to Preparers

- IRS has specifically warned preparers that ID thieves are after the data
- Protection will involve
  - Technology (security software)
  - System design issues (configuration of firewalls, establishing limits on data access, etc.)
  - Individual training (recognizing how attacks will come in)

Remote Computer Takeovers

- Want access to the computer system in order to use apparently legitimate system to file fraudulent returns
- Ways of gaining access
  - Remote access software
    - Can be accounts of members of the firm or your IT support vendor
    - Reused password attacks based on large site breaches
    - Should consider
      - Two factor authentication
      - Review logs of use
      - Don't use standard ports
  - Installation of remote access software via phishing, "drive by" sites, etc.
- Will be a targeted attack because want your system

Phishing

- Send an email to get authorized user to do something to help ID thief
  - May be install software
  - May be to provide information
- Microsoft Office attachments
  - Presume will use Office
  - Sends file that seems to “make sense” and will be opened
    - May trick the user into turning on macros for downloaded files
    - May exploit a vulnerability in Office
      - Unknown vulnerability
      - Unpatched version of Office

Critical Steps to Be Taken (per IRS)

- Never leave taxpayer data unsecured
- Securely dispose of taxpayer information
- Require strong passwords
- Require password changes
- Store data in secure systems and encrypt in transit
- Secure all data in all forms and limit to users that need it
- Take great care in granting remote access
- Terminate accounts of former employees
- Create security requirements for staff
- Train staff
- Protect facility
- Create plan on what to do if breach occurs

Additional Considerations

- Complete risk assessment
- Write and follow an Information Security Plan
- Perform background checks

EFIN Number Check

- Update information within 30 days of change
- Insure proper person listed as authorized
- Run regular check of status

Takeover Warning

- Run deep scan on your system
- Strengthen passwords
- Be alert for phishing scams
- Educate staff on scams

Actions a Firm May Take to Protect Client Data

Training All Employees

- IT experts cannot provide 100% security—user education is necessary
- Phishing Education
- HMTL Lies
- Website Security Certificates
- Malicious Attachments
- Drive-by Malware

Software Updates

- Whenever software is updated, changes are reverse engineered to figure out “what was broken”
- Exploits are then developed to go after unpatched systems—often within 24 hours of release of patch
- Users often don’t apply patches
  - Don’t want to take the time—especially if it demands a reboot
  - Afraid will introduce instability (and sometimes it does)
  - Malware may stop patch checking as part of its infection

Password Managers

- Does introduce risks
  - One point of failure
  - If really secure, forgetting that single password may cause loss of access to all accounts
- But the risk of not using them are higher
  - Passwords will be reused
  - Bad passwords will be used
  - Passwords will be kept near the computer—or on it in an unencrypted form

Encrypting Drives

- Full drive encryption should be used on every drive—including backup drives
- Included with operating system
  - Windows
    - 10, 8.1 – Professional
    - 7 – Enterprise and ultimate (new machines downgraded to 7 won't have access)
  - Mac OSX in all recent versions
  - Linux distributions have had this for a while
- Windows 7 solutions
  - Symantec PGP Full Disk Encryption
  - Veracrypt (recently completed independent security audit)