Best Practices to Avoid and Handle Income Tax Identity Theft/Refund Fraud

Kenneth K. Dort

Peter W. Baldwin

Jason G. Weiss

February 13, 2020

faegre drinker

Faegre Drinker Biddle & Reath LLP

Overview

- **Current Landscape**
- **Typical Incident**
- **Response Planning**
- **Best Practices/Risk Mitigation**
- **Remediation**
- **Questions**

What Is Tax Refund Identity Theft?

- **When someone criminally assumes the identity of a valid tax payer and uses the tax payer's Personally Identifiable Information (PII) to assume the tax payer's identity and literally steal their current tax refund allocation.**
- **This has become a major problem in recent years – leading to the loss of billions of dollars in fraudulent tax refund payments.**

How Does This Scheme Work?

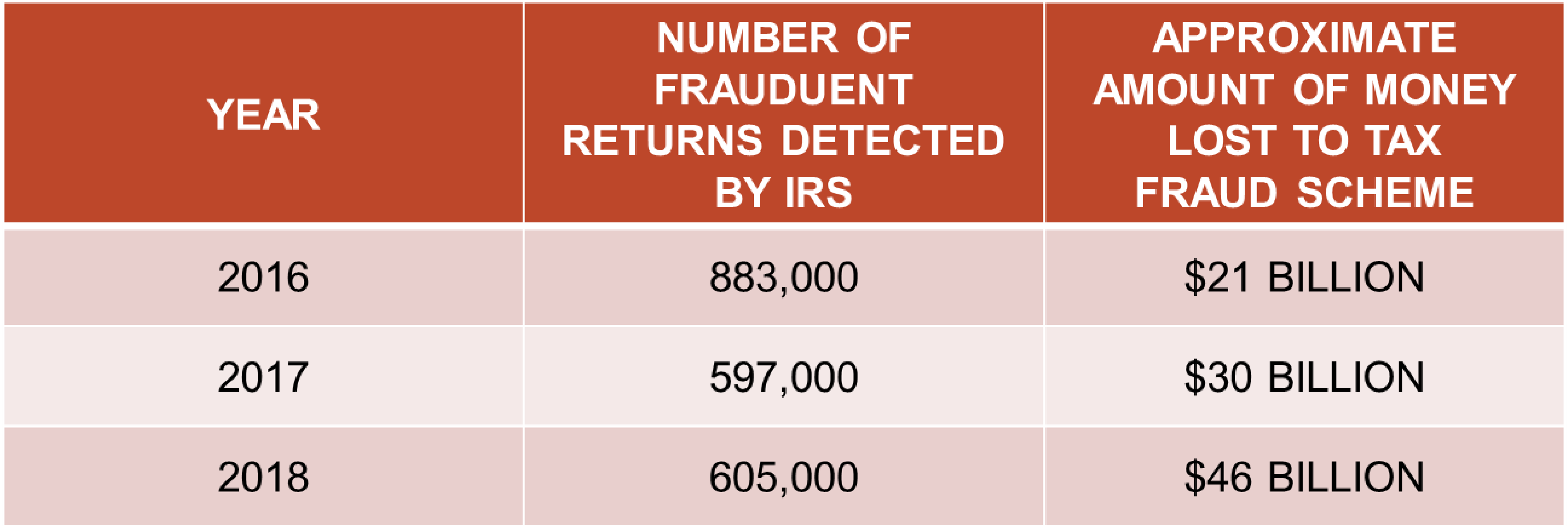
- **Typically, a victim’s employer is contacted by a cyber-criminal, usually via a “phishing” scheme. So, the obvious question is: What is a “phishing” scheme?**
- **Phishing is customarily defined as the fraudulent practice of sending emails “purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.”**
- **You must also be aware of other devastating “social engineering” techniques in addition to Phishing that we will discuss in a moment.**
- **As it relates to Tax Identity theft matters, however, this type of phishing attack is typically focused on obtaining:**
  - Email addresses of victims;
  - Social Security Numbers; and
  - Dates of Birth of victim employees.

What Is the Short-term Result of a Tax Identity Theft?

- **Once a cyber-criminal obtains the identifying information, the cyber-criminal will submit a fake tax return to the IRS using the victim's identity.**
  - This deprives the victim of their IRS tax refund check.
  - Usually the cyber-criminal declares a modest amount to ensure not attracting attention from either the IRS or law enforcement.

- **Cyber-criminals can then expand this scheme to filing multiple fake tax returns – some statistics have noted cyber-criminals filing as many 15 fraudulent tax returns EVERY DAY.**

Fraudulent Tax Returns Are a Big Financial Problem (Approximate)



YEAR	NUMBER OF FRAUDUENT RETURNS DETECTED BY IRS	APPROXIMATE AMOUNT OF MONEY LOST TO TAX FRAUD SCHEME
2016	883,000	$21 BILLION
2017	597,000	$30 BILLION
2018	605,000	$46 BILLION

So, How Do Cyber-criminals Use Social Engineering?

- **Social Engineering is a multi-faceted attack:**
  - The perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocol needed to proceed with the attack.
  - The attacker then moves to gain the victim’s trust and provides a stimulus for subsequent action that breaks established security practices, such as revealing sensitive information and granting access to critical resources (www.imperva.com).
- **Social Engineering is the most efficient, cost effective and capable tool used by cyber-criminals in a variety of crimes**
  - The original master of social engineering was one of the most famous hackers of our generation, Kevin Mitnick. Many books have been written about him and how he used social engineering to orchestrate his attacks.

Common Social Engineering Attacks

Attack Type	What Happens in the Attack
Phishing	Targeting people through social media ruse
Spear Phishing	Targeting specific group of people
Whaling	Targeting business execs
Watering Hole	Injecting malicious script in public websites
Pretexting	Faking your identity
Tailgating	Piggy-backing into a restricted site
Dumpster Diving	Going through garbage bins for sensitive info
Quid Pro Quo	Hacker offers service in benefit for an exchange
Business E-mail Compromises (BEC)	Faking fraudulent wire transfers - BEC has become the single largest damages claim today for Cyber Insurance

Other Common Social Engineering Attacks

- **Cyber Social Engineering can lead to a variety of problems for any business, financial and otherwise:**
  - RANSOMWARE
  - MALWARE
  - BUSINESS E-MAIL COMPROMISE
  - ECONOMIC ESPIONAGE
  - LOST DATA
  - DATA SNIFFERS
  - KEYBOARD STROKE MONITORS
  - THEFT OF E-MAIL
  - THEFT OF INTELLECTUAL PROPERTY
  - EXORBITANT COSTS TO SECURE NETWORK

What Can Your Organization Do to Prepare For/Mitigate Risks

So, What Can Your Organization Do to Prepare and Protect Your Employees?

- **There are five basic steps your organization can take to better prepare and protect your employees from falling victim to Tax Identity Theft and Refund Fraud:**
  1. Training
  2. W-2 Delivery
  3. Risk Management
  4. Information Sharing
  5. Action Plan

How Can Training Help You Protect Your Employees?

- **There is nothing more important than consistent and effective employee "social awareness" training.**
- **The weakest part of any organization as it relates to falling victim to any type of fraud scheme is PEOPLE.**
- **So, how can you use training as an effective tool?**
  - Conduct (at least) annual training with your HR and accounting departments to make them aware of these type of schemes and any new twists. Knowledge is power!
  - The training MUST include reminding employees to never send social security numbers, W-2s and/or any other sensitive financial or personal information via email or phone to anyone.

How Should You Handle the Delivery of W-2s When Necessary?

- **One of the most important documents sought in these types of Tax Identity Theft fraud schemes is the W-2**
- **Consider a secure and well-documented method for sending W-2s to employees**
- **There are secure ways to do this in our digital age:**
  - Consider investing in a secure file sharing portal with Multifactor Authentication
  - Use an encrypted PDF file for which the document and the password are provided separately (usually by E-mail) to provide more secure E-mail transmission of such an important document
  - Try to avoid U.S. mail. This is neither safe nor secure and there is always the risk of mail theft since so few people use locking mailboxes

Start Using and Leveraging “Risk Management” Techniques

- **Risk Management is critical to safeguarding any type of business against almost every type of fraud scheme**
- **Here are a few Risk Management techniques to consider to protect employee W-2s and Personally Identifiable Information from various social engineering attacks:**
  - Consider requiring Human Resources and Accounting teams to forward information about suspicious communications to management for a “second set of eyes”; trust your instincts
  - Consider requiring supervisor and/or management approval before responding to any request for PII information or W-2 information requested by e-mail or phone

When Information Sharing Is a Good Thing

- **Information sharing can be a powerful tool when used correctly. Here are a few ways to ensure that information can be used as a powerful tool to deflect and prevent any type of fraud scheme, including Tax Identify Theft and Refund schemes:**
  - Download and provide current alerts and updates to your individual departments when potential incidents are discovered; use these alerts as a learning tool to ensure that your workplace does not fall for the same scam or scheme – many of these protection-oriented websites will even notify you by text or e-mail when updates are available.
  - Regularly monitor the IRS website for new scam-oriented alerts and distribute these alerts as quickly as possible to your teams.

A Call to Action – or at Least an Action Plan

- **Important question – if something goes wrong, do you know what to do?**
- **That is why having an up-to-date "Action Plan" is a good idea. These plans could/should include:**
  - Important Points of Contact for security, HR, management and anyone else in the company who can provide quick and effective assistance.
  - A "How To Guide" to instruct a victim on the quickest way to handle whatever problems befall them in a simple and easy-to-understand way.
  - Phone numbers of law enforcement.

Some Important General Tips About the IRS

faegre drinker

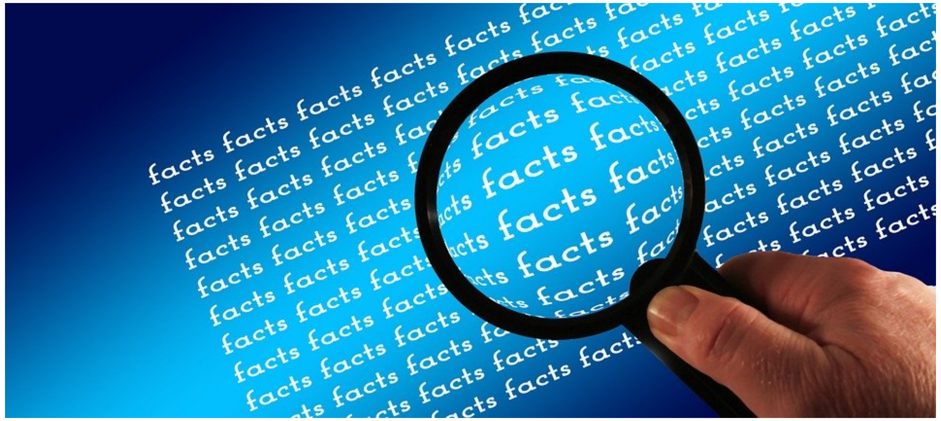
Some Additional Important Tips to Remember

- **The IRS does not initiate contact with a taxpayer by using:**
  - E-mail
  - Text Messages
  - Social Media (No need to check your Instagram to find out about your refund or audit)
- **Also, be VERY wary of phone calls or messages telling you that you owe money; usually, if the IRS wants to talk to you it will be by letter or search warrant**
- **If you do receive an unsolicited E-mail from what appears to be the IRS or a group linked to the IRS – report it to the IRS at phishing@irs.gov.**

How to Respond and Remediate

Immediate Response Efforts

- **Initiate an Internal Review**
  - What happened?
  - Contact and interview relevant players
  - Contact applicable response team
  - Do you need forensics assistance?
- **External Assistance**
  - Internal Revenue Service
  - State agencies
  - FBI
  - Secret Service
  - Local police



Consider Informing the Affected Persons Informally

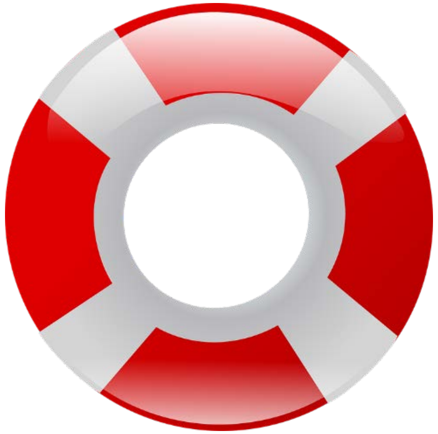
- **Have the Basic Facts First!!**
- **Select the Most Effective Mode**
  - E-mail
  - In-person – possibly by teams
- **Speed Is Essential Given Tax Context**
  - Be prepared for hostility/anger
  - Need to place employees in best position to act

Possible Responses/Remedies

- **Keep Your Formal Breach Notification Obligations in Mind**
- **Credit Monitoring Services (Assuming SSNs Involved)**
  - Provide for at least one year
  - Mitigates risk for affected employees
- **Part of a Proactive Approach**
- **Assist with Filings of IRS Form 14039**
  - https://www.irs.gov/pub/irs-pdf/f14039.pdf
  - This will notify IRS of the problem
- **Note That Refunds Will Be Delayed**
  - Several months

Possible Responses/Remedies, Part II

- **Consider Short-term Loans to Employees**
  - Affected persons submit copy of refund return
  - Enter into a loan agreement:
    - For amount of refund
    - No interest
  - Repayment upon earlier of:
    - Receipt of refund from IRS
    - Departure from employer
- **Current vs. Former Employees**



Breach Notification Compliance

- **Recall that We Still Have a "Breach"**
  - Triggering relevant state breach notification laws
  - Apart from tax ramifications, we still have a breach
- **Activate Relevant Incident Response Plan**
  - Contact law enforcement authorities
  - Pull in key corporate officers
  - Contact cyber counsel
  - Establish compliance schedule/timeline
  - Insurance notifications (if applicable)

Breach Notification Compliance (cont'd)

- **Prepare Compliant Notification Letter**
  - Should address applicable state requirements
- **Set Up Call Center (if Applicable)**
- **Set Up Credit Monitoring (if Applicable)**
- **Notify Applicable State Officials**
  - Be ready for series of communications and follow-ups
- **Notify IRS (Keep in Loop)**

Best Practices for Avoiding Tax Identity Theft and How to Remediate When Disaster Strikes

faegre drinker

Practice Points

- **Know Your Risks/Vulnerabilities**
- **Train Your Employees**
- **Do Not Transfer Tax Information w/o Senior Approval**
- **Prepare/Implement Incident Response Plan**
- **Practice That Plan (Tabletops)**
- **Have Your Appropriate Players in Place**

TOP 10 TIPS AND TRICKS TO KEEP SAFE FROM TAX IDENTITY THEFT AND REFUND FRAUD

1. Do train employees on cyber scheme awareness
2. Don’t (ever) give out PII
3. Don’t click on links from strangers
4. Don’t throw away PII – shred it
5. Do independently look up phone numbers from people requesting PII
6. Do make sure network devices are from trusted sources and have antivirus software
7. Do implement better training, safe W-2 delivery, risk management, information sharing and a robust action plan
8. Do institute Multi-Factor Authentication
9. Do encrypt your data at rest & in motion
10. Do remember – the IRS does not contact people via email, text or social media

Questions?

Kenneth K. Dort
Partner

kenneth.dort@faegredrinker.com
312-569-1458

Peter W. Baldwin
Partner

peter.baldwin@faegredrinker.com
212-248-3147

Jason G. Weiss
Counsel

jason.weiss@faegredrinker.com
310-203-4062