# Protect Your Clients; Protect Yourself from Data Theft

August 17, 2016

**The information contained in this presentation is current as of the date it was presented. It should not be considered official guidance.**

# Protect Your Clients; Protect Yourself from Data Theft

"Combatting identity theft is going to take a concerted effort by all of us – working together – and I look forward to working with all of you in the tax community." -

IRS Commissioner John A. Koskinen

# Webinar Agenda

- Explain next steps for Security Summit Initiatives and your role in it
- Increase awareness about data loss threats and the “Protect Your Clients; Protect Yourself” campaign
- Discuss how to get started and where to find information on safeguarding taxpayer data

## Do you have a question?

Select the “Ask a Question” link under the PowerPoint window and click the submit button.

# Data Thefts and Protecting Client Tax Information

**Ken Corbin**
**Director, Return Integrity and Compliance Services**
**W&I Division**

**Carol Campbell**
**Director, IRS Return Preparer Office**

**Mark Kahler**
**Senior Analyst, Criminal Investigation**

**David P. Lyons**
**President, Lyons & Lyons, PC**

## Ken Corbin – RICS Director; Security Summit Lead

# IRS Actions in Recent Years:

- Improved identity theft screening filters
- Limit direct deposits to three refunds in single account
- Locked accounts of nearly 30 million deceased taxpayers
- Curtailed prisoner fraud
- Established relationships with financial institutions
- Created identity theft markers and Identity Protection PIN

# Ken Corbin – RICS Director; Security Summit Lead

## Real Progress Made

- Stopped 1.4 million confirmed identity theft returns in calendar year 2015
- Protected $8.7 billion in identity theft refund fraud
- Stopped $3.1 billion in other types of fraud
- Reduced case resolution time to 120 days from 300 days
- Issued 2. 7 million IP PINs for 2016 filing season

## Ken Corbin – RICS Director; Security Summit Lead

# Security Summit Initiative 2016:

- Shared more than 20 new data elements from returns
- Enhanced password standards for customer software accounts
- Strengthen validation standards for returning customers
- Improve information sharing
- Strengthen cybersecurity framework

## Ken Corbin – RICS Director; Security Summit Lead

# **Security Summit Initiative 2017**:

- 16-digit Form W2 Verification Code on 50 million W-2s
- Sharing additional data elements from individual returns
- Sharing data elements from business returns
- Creating external leads program for states
- Launching Information Sharing and Analysis Center

# Carol Campbell – Return Preparer Office Director

## Tax Professional Work Group

- Protect Your Clients; Protect Yourself
  - Raise awareness on need for security
  - Identify common sense steps
  - New IRS.gov page
- Connect with IRS
  - E-News for Tax Professionals
  - Twitter.com/irstaxpros
  - Facebook.com/irstaxpros
  - Quick Alert

# Carol Campbell – Return Preparer Office Director

## Getting Started

- Assign someone responsible for safeguards
- Assess risks to taxpayer information; list all locations where taxpayer information stored
- Create and enact plan to safeguard taxpayer data
- Use only service providers who have safeguards in place
- Monitor and evaluate security plan as circumstances change

## Carol Campbell – Return Preparer Office Director

## Publication 4557 – Safeguarding Taxpayer Data

- Covers seven topic areas:
  - Administrative Activities
  - Facilities Security
  - Personal Security
  - Information Systems Security
  - Computer Systems Security
  - Media Security
  - Certifying Information Systems for Use

## Carol Campbell – Return Preparer Office Director

### Data Loss: Steps for Tax Professionals

- Contact the IRS and Law Enforcement
  - IRS Stakeholder Liaisons
- Contact states in which you file returns
- Contact experts
- Contact clients and other services
- Information for preparers available on IRS.gov/identitytheft

# Carol Campbell – Return Preparer Office Director

## Track returns filed with your PTIN/EFIN

- Access your PTIN account
  - Select “Additional Activities” from Menu;
  - Select “View Returns Filed Per PTIN”
  - Shows returns for preparers who filed 50 or more returns
- Access your e-services account
  - View returns filed per EFIN

## David Lyons, CPA – Data breach

Let my experience serve as a lesson

- Never thought could happen; Limited exposure to identity theft prior to 2013
- Clients began receiving IRS notices
- Notified insurance carrier of possible data breach
- Contacted Connecticut State Society of CPAs
- Learned Department of Homeland Security was investigating

## David Lyons, CPA – Data breach

### Dealing with the theft

- Hiring additional staff
- Notifying customers
- Obtaining credit protection services for clients
- IRS ID Protection Unit /Taxpayer Advocate

## David Lyons, CPA – Data breach

### Actions taken to prevent future thefts

- Passwords minimum 12 characters long
- Computer shuts down after 3 unsuccessful password entries
- Password protected each client's tax file
- Computer passwords changed every 90 days
- Firewall/antivirus/malware protects updated regularly
- Install motion detector and new locks at office

## David Lyons, CPA – Data breach

### Actions taken to prevent future thefts

- Encrypt all client information sent over internet
- Completely shut down computers during off hours
- Block access to certain websites from office computers
- Train all employees on security and scams
- Because of Ransom Ware concerns, installed new back-up system

## Mark Kahler – IRS Criminal Investigation

How the cybercriminal network operates:

- Cybercriminal #1
  - Establishes a botnet, infecting computers of unsuspecting owners and gaining control
  - Computers can be in multiple countries
  - Uses hijacked computers to send malware, phishing emails, viruses to U.S.-based computer
  - Places stolen identities on the “Dark Net” for sale to….

## Mark Kahler – IRS Criminal Investigation

How the cybercriminal network operates:

- Cybercriminal #2
  - Buys stolen identities from Dark Net
  - Hires people to create fraudulent tax returns
  - IRS stops majority of fraudulent returns
  - Refunds that do through go to U.S. based accounts or debit cards
  - Hired U.S. “mules” convert the refunds into wire transfers to foreign countries
  - Hired foreign “mules” recover wire transfers and hand over to Cybercriminal #2

## Don’t take the bait

IRS alert reported 400 percent increase in scams related to IRS or tax software products

- Phishing - a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly.
- Malware – shorthand for malicious software - intended to damage a computer, mobile device, computer system, or computer network, or to take partial control over its operation.

# Mark Kahler – IRS Criminal Investigation

## Hot scams for 2016

- Phishing email pretending to be from new client sharing tax data via an attachment
- Phishing email asking tax professionals to update their e-services accounts
- Malware that captures all data and charges a ransom for its return
- Malware that gives criminals remote control of preparers' computers and access to client data

# Mark Kahler – IRS Criminal Investigation

Questions to ask yourself?

- Does your tax software have built-in security measures?
- Are you familiar with the tax software capabilities regarding usernames and passwords as well as data protection options?
- Do you know if your computer has software to protect it from malware and other intrusions?

# Protect Your Clients; Protect Yourself

Few simple steps:

- Never leave any taxpayer information unsecured
- Securely dispose of taxpayer information
- Require strong passwords (numbers, symbols, upper & lowercase) on all computers and tax software programs
- Change those passwords  every 60 – 90 days
- Store taxpayer data in secure systems and encrypt information when transmitting across networks

# Protect Your Clients; Protect Yourself

Few simple steps:

- Ensure that e-mail being sent or received, that contains taxpayer data, is encrypted and secure
- Make sure paper documents, computer disks, flash drives and other media are kept in a secure location and restrict access to authorized users only
- Use caution when allowing or granting remote access to internal networks

# Data Thefts and Protecting Client Tax Information Q&A Session

**Ken Corbin**
**Director, Return Integrity and Compliance Services**
**W&I Division**

**Carol Campbell**
**Director, IRS Return Preparer Office**

**Mark Kahler**
**Senior Analyst, Criminal Investigation**

**David P. Lyons**
**President, Lyons & Lyons, PC**

## IRS Video Portal

Go to: www.irsvideos.gov
and click the "All Webinars" tab
to view IRS Webinar Archives.