


Center for Agricultural Law & Taxation

Don't Let Disaster Destroy Your Office – Disaster Proof from Cybercrime
 May 4, 2017



Cybercrime

- As the Internal Revenue Service, the state tax agencies and the tax industry make progress combatting identity theft, cybercriminals need more data to impersonate real taxpayers and file fraudulent returns for refunds
- Top Five Crimes
 - Refund Fraud
 - Corporate Account Takeover
 - Identity Theft
 - Theft of Sensitive Data
 - Theft of Intellectual Property

2

Center for Agricultural Law & Taxation

The Crime

- A hacker takes control of your computer network and blocks you from accessing customer accounts, orders and inventories, then demands you pay thousands of dollars for their release
- A hacker steals medical histories of every patient at your practice, then files Medicare claims under those patients' names
- Your bank account password is stolen by someone recording everything you do on your computer, and is then used to withdraw all of your money

3

Center for Agricultural Law & Taxation

You Have a Plan in Place if Disaster Strikes Right?

- There is more than one type of disaster
- We think Katrina or the now named winter storms
- So far in 2017 there have been 15 federally declared disaster areas in 12 different states and 1 Tribal government property
- Severe storm, flooding, tornados, straight-line winds, mudslides and hurricane season has yet to start
- In addition, 1 emergency declaration (Dam), and 10 Fire Management Assistance Declarations have been assigned

4

Center for Agricultural Law & Taxation

The Other Silent Disaster -Cybercrime

- Information is the new currency
- Companies have more personal information about consumers than ever before, and store and transmit it across their own systems as well as the Internet
- Hackers and others seek to:
 - Exploit vulnerabilities
 - Obtain unauthorized access to consumers' sensitive information, and
 - Potentially misuse it in ways that can cause serious harms to consumers as well as businesses

5

Center for Agricultural Law & Taxation

Heads Up!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

- We can evacuate when the hurricane is coming
- We can confine ourselves to a tornado shelter when the weather man gives warning
- We can preparer for a fierce winter storm
- We CAN place certain operations in motion to protect ourselves from Cybercrime

6

Center for Agricultural Law & Taxation

Identity Theft

- The Bureau of Justice Statistics estimates that 16.6 million persons – or 7 percent of all U.S. residents ages 16 and older – were victims of identity theft in 2015
- Average loss \$3,500

7

Center for Agricultural Law & Taxation

Laws on the Books

- The Gramm-Leach-Bliley Act (“GLB Act”), provides data security requirements for non-bank financial institutions – tax professional are included in this law
- The Fair Credit Reporting Act (“FCRA”) requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a purpose for receiving that information, and imposes safe disposal obligations on entities that maintain consumer report information

8

Center for Agricultural Law & Taxation

Laws on the Books

- The Children’s Online Privacy Protection Act (“COPPA”) requires reasonable security for children’s information collected online
- As directed by Congress, the Federal Trade Commission (FTC) maintains the nation’s main repository of identity theft complaints and provides centralized resources for victims of identity theft
- Identity theft has been the top consumer complaint for 13 consecutive years

9

Center for Agricultural Law & Taxation

What the Laws Require?

- Take responsibility or assign an individual to be responsible for the safeguards of the systems
- Do a risk assessment of the computer system and your office
- Make a list of the locations where information is stored and evaluate risks
- Make a plan to safeguard taxpayer data
- Only use service providers who have policies in place to maintain information protection
- Constantly monitor, evaluate and adjust the plan as needed taking into account changes in the business

10

Center for Agricultural Law & Taxation

Safeguard of Taxpayer Data

- Make sure your software is up to date
- Run routine scans of the system to ensure it is not infected
- If a problem is found, disconnect and perform a system restore

11

Center for Agricultural Law & Taxation

It's All About Control – Start with Security

- From personal data on employment applications to network files with customers' credit card numbers, to tax returns, sensitive information is everywhere
- Start with security
 - Factor it into the decision making in every department of the business – personnel, sales, accounting, information technology, etc.
 - Collecting and maintaining information "just because" is **no longer** a sound business strategy
 - Make conscious choices about the kind of information you collect, how long you keep it, and who can access it

12

Center for Agricultural Law & Taxation

Develop a Daily Routine

- Lock doors/files to restrict access to paper and electronic files
- Require strong passwords
- Encrypt data on a regular basis
- Have a back up
- Shred documents
- Do not email PII
- Shut off computers

13

Center for Agricultural Law & Taxation

Center for Agricultural Law & Taxation

Internal Controls



14

Checklist

- Only connect to the internet over secure, password protected networks
- Do not click on pop-ups, open attachments or respond to emails from unknown parties
- Always enter a URL by hand instead of following links if you are unsure of the sender
- Guard the PII (Personal Identifiable Information)
- Limit who you share information with by reviewing your privacy setting on your social media accounts
 - Better yet, do not participate in social media

15

Center for Agricultural Law & Taxation

Checklist

- Trust your instincts – remember if it is too good to be true assume it is a scam
- Password protect all devices that connect to the internet and user accounts with strong passwords
- Do not use the same password twice – change on a regular basis –every three months or more as needed
- Secure passwords

16

Center for Agricultural Law & Taxation

Resources

- U.S. Computer Emergency Readiness Team - <https://www.us-cert.gov/government-users>
 - Provides timely information about current security issues
- Department of Homeland Security – Stop Think Connect Campaign - <https://www.dhs.gov/stopthinkconnect-toolkit>

17

Center for Agricultural Law & Taxation

Privacy - IRS Publication 4299

- Created initially for volunteers
- Contains some good information for all tax professionals just not volunteers

18

Center for Agricultural Law & Taxation

Penalty for Unauthorized Disclosures or Uses

- IRC §7216(a) imposes criminal penalties on tax return preparers who knowingly or recklessly make unauthorized disclosures or
- Use of information furnished in connection with the preparation of an income tax return or other uses without permission – violation in some cases
- A violation of IRC §7216 is a misdemeanor, with a maximum penalty of up to one year imprisonment or a fine of not more than \$1,000, or both, together with the cost of prosecution

19

Center for Agricultural Law & Taxation

§ 7216

Using and Disclosing Taxpayer Information for:	Are the two Consents (Use and Disclosure) Required?
Preparing current, prior, or subsequent year tax returns.	No
Purposes other than preparing current, prior, or subsequent year tax return.	Yes
Reporting the number of returns (number of types of return such as Earned Income Tax Credit (EITC), Child Tax Credit (CTC), etc.) prepared to use for fundraising, marketing, publicity or other uses related to the volunteer sites tax return preparation business.	No
Reporting any data containing return dollar amounts for marketing or advertising or any other non-fundraising activities.	Yes
Reporting any data containing return dollar amounts for fundraising activities.	No

20

Center for Agricultural Law & Taxation

Consent - Requirements

- There are two types of consents:
 - 1) Consent to “Disclose”, taxpayer information
 - Disclose means the giving out of information, either voluntarily or to be in compliance with legal regulations or workplace rules, and,
 - 2) Consent to “Use” taxpayer information
 - Use means the act or practice of employing something

21

Center for Agricultural Law & Taxation

Privacy and Confidentiality – Key Principles

- Must keep confidential the information provided for tax return preparation
- Protect physical and electronic data gathered for tax return preparation both during and after filing season
- Secure the taxpayer’s consent to use or disclose their data
- Maintain privacy during the taxpayer interview
- Information provided for tax return preparation should not be shared with anyone who does not have a need to know

22

Center for Agricultural Law & Taxation

Validating Taxpayers – An Issue to Think About

- IRS-tax law certified volunteers preparing tax returns must confirm the identity of each taxpayer signing the tax return to prevent identity theft and tax fraud
- Review an original photo identification (ID) such as:
 - Valid driver’s license (U.S.)
 - Employer ID
 - School ID
 - State ID (U.S.)
 - Military ID
 - National ID
 - Visa, or passport

23

Center for Agricultural Law & Taxation

Validating Taxpayers – An Issue to Think About

- However, judgment should be used to accept any other valid form of identification
- If a taxpayer cannot substantiate a taxpayer’s identity, or if the you are uncomfortable accepting the items presented as proof of identity, the taxpayer should be advised to return with an acceptable form of identification

24

Center for Agricultural Law & Taxation

E Mail

- Both parties should consider using a supplemental program that secures the message with a password
- There are several software programs available
- Before emailing information to taxpayers, a unique set of passwords/identifiers to ensure the secure transmission of information between parties
- Never use public computer to send email
- Sensitive email messages should be deleted from the computer and/or server once they are no longer needed

25

Center for Agricultural Law & Taxation

Center for Agricultural Law & Taxation

Let's Talk Technical Issues



26

Breaking Down the Computer Talk - Router

- You responsible for protecting your clients data
- Part of that is understanding terms and how they operate
 - A router comes configured with many vendor default settings
 - Many of these settings are public knowledge and make the router susceptible to attacks
 - Remember to change the router default log-in password during the initial setup
 - Password should consist of letters, numbers and special characters of at least 14 characters

27

Center for Agricultural Law & Taxation

Breaking Down the Computer Talk - Router

- Change the default SSID: A service set identifier (SSID) is a unique name that identifies a particular wireless local area network (WLAN)
- All wireless devices on a WLAN must use the same SSID to communicate with each other
- Manufacturers set a default SSID at the factory
- An attacker can use the default SSID to identify the device and exploit any of its known vulnerabilities
- Users sometimes set the SSID to a name that reveals their organization, their location, or their own name
- This information makes it easier for the attacker to identify the specific business or home network based upon an SSID that explicitly displays the organization's name, organization's location, or an individual's own name

28

Center for Agricultural Law & Taxation

Breaking Down the Computer Talk - Router

- Don't stay logged into the management website for the router:
 - Routers usually provide a website for users to configure and manage the router
 - Do not stay logged into this website, as a defense against cross-site request forgery (CSRF) attacks
 - In this context, a CSRF attack would transmit unauthorized commands from an attacker to the router's management website

29

Center for Agricultural Law & Taxation

Turn the Network off When Not in Use


- While it may be impractical to turn the devices off and on frequently, consider this approach during travel or extended offline periods
- The ultimate in wireless security measures—shutting down the network—will definitely prevent outside attackers from being able to exploit the WLAN

30

Center for Agricultural Law & Taxation

Center for Agricultural Law & Taxation

Taxes and the Impact of Identity Theft How It All Works



Tax-Refund Fraud

- Cybercriminals first obtain a valid name and Social Security number, preferably from someone who will not be filing a tax return
- That person could be a deceased taxpayer or a minor
- They will obtain this information using social engineering or email phishing, purchasing the data on the black market, or using other avenues
- Sellers on the black market typically have some degree of access to the necessary personally identifiable information — person's name, Social Security number, address and date of birth — from their workplace
- They usually are insiders at high-traffic businesses such as hospitals, doctors' offices or car dealerships that capture such information

32

Center for Agricultural Law & Taxation

Tax-Refund Fraud

- The cybercriminal next makes up wage and withholding information, claims standard deductions or a few itemized deductions, and perhaps tax credits, and completes a return that generates a large refund
- They file the fraudulent tax return electronically, which technically makes it a cybercrime and not ordinary fraud

33

Center for Agricultural Law & Taxation

Tax-Refund Fraud

- Cybercriminals file electronically because W-2s are not included with electronically filed tax returns, and by the time the IRS discovers that the return does not match up with a W-2, the crime is complete and the cybercriminal has absconded with the funds
- The criminal then simply waits for either a check to be mailed, a direct deposit to be made to a "safe" bank account or, most commonly, a credit to be posted to a debit card
- The debit card is bought specifically for accepting the fraudulent refunds and is harder to trace
- Often, multiple refunds are sent to the same address, bank account or debit card because the cybercriminal will complete dozens, if not hundreds, of fraudulent tax returns

34

Center for Agricultural Law & Taxation

Employment Related Identity Theft and the Tax Return

- Employment related identity theft occurs when someone steals another person's Social Security number in order to get a job
- Often this occurs when illegal immigrants use stolen Social Security numbers to get a job because they cannot legitimately obtain their own Social Security number
- The IRS becomes aware of the Social Security number being misused when the income tax returns filed using the Social Security number don't match the W-2s associated with the Social Security number

35

Center for Agricultural Law & Taxation

Employment Related Identity Theft

- If one of the following happens, this may be an indication that the client's Social Security number or other personal information may have been used by another person without their permission for employment purposes
- They receive IRS notice CP01E 'Employment Related Identity Theft', stating they may be the victim of employment-related identity theft
- They receive IRS notice CP2000 'Request for Verification of Unreported Income, Payments, or Credits', listing wages they didn't earn
- They receive IRS notice CP2057 'Check Your Records to Confirm the Income You Received', regarding a potential income discrepancy and the questionable income is directly related to wages that were not earned by them
- They receive a Form W-2 or Form 1099 from an employer for whom they didn't work;
- They receive a notice from the Social Security Administration (SSA) stating that their Social Security benefits have been adjusted/denied because of wages they didn't earn or;
- They receive a Social Security Statement from SSA showing more income than they earned

36

Center for Agricultural Law & Taxation

IRS to Start Notifying Victims of Employment-Related Identity Theft

- IRS began to notify individuals whose social security numbers have been used in employment-related identity theft uncovered by the agency beginning January 1, 2017
- Letter 4491-C, Notice of Employment-Related Identity Theft

37

Center for Agricultural Law & Taxation

What Letter 4991-C says.....

WHY WE ARE SENDING YOU THIS LETTER

We believe your social security number (SSN) was used by another person to obtain employment. The use of your SSN in this instance hasn't affected your tax return or tax account. However, we marked your tax account to indicate that you are a victim of identity theft. This will help us to serve you more effectively and efficiently in the event you should have an identity theft-related tax issue.

Federal law prevents us from providing specific details regarding the identity of the individual who used your SSN for employment purposes. Our purpose in sending this letter is to make you aware of this incident so you can take the appropriate steps to protect yourself from any potential effects of identity theft.

38

Center for Agricultural Law & Taxation

What Letter 4991-C says.....

WHAT YOU SHOULD DO

Again, there is no impact to your tax return or tax account because of this incident. However, you should review your earnings with the Social Security Administration to ensure their records are correct. You may review earnings posted to your record on your Social Security Statement. The Statement is available online to workers age 18 and older. To get your Statement, go to www.socialsecurity.gov/mystatement and create an account.

You should also monitor your credit reports and any financial accounts for further signs of misuse of your personal information. As a precaution, you may want to contact one of the three major credit bureaus to have a fraud alert placed on your account. You only need to contact one of the credit bureaus, as the one you contact is required to contact the other two.

39

Center for Agricultural Law & Taxation

Fact of Life Today

- Tax Professionals may need to counsel clients who receive such a letter about the implications of the letter
- First, the taxpayer should take the steps outlined in the letter to notify credit bureaus and confirm their earnings with social security
- Second, explain that the real threat at this point most likely is not the party that used the identity, but rather the party from whom that data was obtained
- It is very likely that far more than the person's name and social security number is available for sale to the highest bidder—and the party that bought the identity for employment purposes was almost certainly not given those details since the identity can be resold by that party to others for more money
- An unfortunate fact of life today is that significant information (including social security numbers, addresses, employers, etc.) is available for sale—thus it is probably prudent for all individuals to assume their data is available for sale and they could be targeted

40

Center for Agricultural Law & Taxation

Corporate Account Takeover

- It is costly and ranks among the fastest and most stealthy type of attack
- Cybercriminals engaging in this activity surreptitiously obtain an entity's financial banking credentials, use software to hijack one of its computers remotely and steal funds from the entity's bank account
- Although corporate account takeovers can take different forms, the discussion here primarily is limited to electronic funds transfer fraud, such as Automated Clearing House (ACH) or wire transfer

41

Center for Agricultural Law & Taxation

Schemes Involve Three Steps

- Illicitly acquire login credentials
- Gain unauthorized access to the victim's computer to avoid the bank's security features, activated when it does not recognize the login "fingerprint"
- Transfer the victim's bank funds to an account controlled by the cybercriminal
 - The criminal typically transfers the funds to individuals known as money mules, who move the funds to a protected account such as an overseas bank account in a country that is uncooperative with U.S. banking rules and protocols

42

Center for Agricultural Law & Taxation

Corporate Account Takeover

- The specific person targeted often is the person most likely to be conducting online banking transactions for the entity, such as the chief accounting officer, chief financial officer, treasurer or controller, all of whom are relatively easy to identify online
- The cybercriminal also knows the steps that need to be taken to access accounts as well as online banking's typical security features
- There are at least two risk areas for clients of tax professionals

43

Center for Agricultural Law & Taxation

Risks

- First, the CAO, CFO, treasurer or controller often is unaware of corporate account takeovers and the repercussions and liability that can follow
- Second, there is a lack of adequate controls over the online banking process
- However, even fairly stringent controls can be overcome by a cybercriminal's persistent attack, and these controls can create a false sense of security when, in reality, there still is substantial risk

44

Center for Agricultural Law & Taxation

Bank Accounts

- A corporate takeover will wipe out the bank account in seconds and electronically transmit the funds to a criminal secured account generally offshore
- Taxpayers know almost immediately of the theft if they regularly monitor their accounts

45

Center for Agricultural Law & Taxation

Amazingly.....

- Fifty percent of identity thefts goes undetected for at least one month and 10 percent remains undetected for two or more years

46

Center for Agricultural Law & Taxation

Identity Theft

- Identity theft typically occurs when a cybercriminal successfully steals a person's personally identifiable information
- This type of cybercriminal does not really benefit unless there is a financial reward for the effort or some type of damage that can be done with the data
- Thus, identity theft serves as a gateway to other cybercrimes such as tax-refund fraud, credit-card fraud, loan fraud and other similar crimes

47

Center for Agricultural Law & Taxation

Examples

- Opening a line of credit
- Purchasing goods or services
- Renting or buying a house or apartment
- Receiving medical care
- Obtaining employment
- Other examples include committing traffic infractions or felonies, auction fraud and wage-related fraud

48

Center for Agricultural Law & Taxation

Identity Theft

- According to the Identity Theft Resource Center (ITRC), identity theft complaints ranked first in 2012 in the Federal Trade Commission's (FTC) list of complaints, with a 32 percent increase over 2011
- A Javelin Strategy & Research survey shows an increase of 13 percent in 2011 compared with 2010, and a total of 11.6 million victims in the United States in 2011

49

Center for Agricultural Law & Taxation

Identity Theft

- Entities need to exercise due diligence to protect personally identifiable information — it is good customer service and helps avoid lawsuits or violations of state or federal laws
- Forty-six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have laws regarding security breaches of personally identifiable information

50

Center for Agricultural Law & Taxation

Identity Theft

- If a breach occurs, costs for failing to comply are high
- For example, the Massachusetts law, known as MASS 201, allows the Massachusetts attorney general to sue any company that has a security breach if the company is found to be noncompliant with the law's requirements
- This law has given rise to audits in Massachusetts, known as MASS 201 audits
- These compliance audits ensure that entities have taken "reasonable" precautions to protect the personally identifiable information of Massachusetts' citizens

51

Center for Agricultural Law & Taxation

Theft of Sensitive Data

- Sensitive data such as unencrypted credit card information stored by a business, personally identifiable information, trade secrets, source code, customer information and employee records all attract the attention of cybercriminals
- This cybercrime overlaps with previous discussions of personally identifiable information, identity theft and security breaches
- The costs to victims of this type of cybercrime can be high, and involve both public-image damage and financial costs related to loss of business, legal fees and increasing security measures

52

Center for Agricultural Law & Taxation

Theft of Intellectual Property

- Intellectual property, including commercial, copyrighted materials — music, movies and books — also is at risk of being stolen
- Although music owners have risen on the list of victims of cybercrime in the past decade, commercial entities that hold copyrights or patents need to remain on guard

53

Center for Agricultural Law & Taxation

Center for Agricultural Law & Taxation

Some Issues to Consider



54

Ask yourself Do I Really need the Information?

- Don't collect personal information you don't need
 - No one can steal what you don't have
 - When does your company ask people for sensitive information?
 - Perhaps when they're registering online or setting up a new account
 - When was the last time you looked at that process to make sure you really need everything asked for

55

Center for Agricultural Law & Taxation

How Long Do I Keep the Information?

- Sometimes it's necessary to collect personal data as part of a transaction
- But once the deal is done, it may be unwise to keep it
- Have you set a time frame of when to shred old clients tax return data or purge it from your systems?
- How long do you keep credit card data once the sale is complete
 - In a recent case, this happened and the FTC determined that the company violate banking rules, by holding on to the information without a legitimate business need, creating an unreasonable risk
 - Ultimately, hackers stole the account data and used it to make counterfeit credit and debit cards
 - The business could have limited its risk by securely disposing of the financial information once it no longer had a legitimate need

56

Center for Agricultural Law & Taxation

What Records Do I Have to Keep?

- EROs must retain some of the following material/documents until the end of the calendar year at the business address or another address that allows access- others like the return itself must be kept longer (3 years)
- The materials must be available at the time of an IRS request
- An ERO may also retain the required records at the business address of the Responsible Official
- The records can be paper or electronic

57

Center for Agricultural Law & Taxation

What Records Do I Have to Keep?

- A copy of Form 8453, U.S. Individual Income Tax Transmittal for an IRS e-file Return, and supporting documents that are not included in the electronic records submitted to the IRS
- Copies of Forms W-2, W-2G and 1099-R
- A copy of signed IRS e-file consent to disclosure forms
- A complete copy of the electronic portion of the return that can be readily and accurately converted into an electronic transmission that the IRS can process and
- The acknowledgement file for IRS accepted returns

58

Center for Agricultural Law & Taxation

What Records Do I Have to Keep?

- Forms 8878 and 8879 must be available to the IRS for three years from the due date of the return or the IRS received date, whichever is later
- The Submission ID must be associated with Form 8878 and 8879
- The Submission ID can be added to the Form 8878 and 8879 or, the acknowledgment containing the Submission ID can be associated with Forms 8878 and 8879

59

Center for Agricultural Law & Taxation

How Long Must You Keep Those Tax Records?

- If the acknowledgement is used to identify the Submission ID, the acknowledgement must be kept in accordance with published retention requirements for Forms 8878 and 8879
- The acknowledgement is not required to be physically attached to Form 8878 and 8879; it can be electronically stored
- EROs may electronically image and store all paper records they are required to retain for IRS e-file
- This includes Forms 8453 and paper copies of Forms W-2, W-2G and 1099 R as well as any supporting documents not included in the electronic record and Forms 8878 and 8879

60

Center for Agricultural Law & Taxation

How Long Must You Keep Those Tax Records?

- The storage system must satisfy the requirements of Revenue Procedure 97-22, 1997-1, Retention of Books and Records
- In brief, the electronic storage system must ensure an accurate and complete transfer of the hard copy to the electronic storage media
- The ERO must be able to reproduce all records with a high degree of legibility and readability (including the taxpayers' signatures) when displayed on a video terminal and when reproduced in hard copy

61

Center for Agricultural Law & Taxation

Legal Code Section

- Reg. 1.6107-1(b)(iii)(2) – retain for 3 years

62

Center for Agricultural Law & Taxation

Don't Use Personal Information When it's Not Necessary

- Do not use personal information in a context that create unnecessary risks
 - Example: A company used real people's personal information in employee training sessions, and then failed to remove the information from employees' computers after the sessions were over
 - Example: A company gave access to sensitive consumer data to service providers who were developing applications for the company
- In both cases, the risk could have been avoided by using fictitious information for training or development purposes

63

Center for Agricultural Law & Taxation

Control Access to Data

- Take reasonable steps to keep data secure
- Restrict access to sensitive data
- Does everyone on staff need unrestricted access to the network and the information stored
- Place controls on access to make sure employees have access only on a "need to know" basis
- For the network, consider steps such as separate user accounts to limit access to the places where personal data is stored or to control who can use particular databases
- For paper files, external drives, disks, etc., an access control could be as simple as a locked file cabinet

64

Center for Agricultural Law & Taxation

Control Access to Data

- Limit administrative access
- Administrative access allows a user to make system-wide changes to a system
- Access should be limited to the employees tasked to do that job
- Administrative control systems include the ability to reset user account and passwords
- Ensure that employees' access to the system's administrative controls was tailored to their job needs

65

Center for Agricultural Law & Taxation

Require Secure Passwords and Authentication

- Insist on complex and unique passwords
- Store passwords securely – not on computers
- Guard against brute force attacks
 - Hackers use automated programs that perform a similar function
 - These brute force attacks work by typing endless combinations of characters until hackers luck into someone's password
 - Making passwords more complex helps
 - Don't forget to implement a suspend or disable user credentials program after a certain number of unsuccessful login attempts
 - Implementing a policy to suspend or disable accounts after repeated login attempts helps eliminate risk

66

Center for Agricultural Law & Taxation

Protect Against Authentication Bypass

- Locking the front door doesn't offer much protection if the back door is left open
- In a recent FTC case, a business failed to adequately test its web application for widely-known security flaws, including one called "predictable resource location"
- As a result, a hacker could easily predict patterns and manipulate URLs to bypass the web app's authentication screen and gain unauthorized access to the company's databases
- The company could have improved the security of its authentication mechanism by testing for common vulnerabilities

67

Center for Agricultural Law & Taxation

Store Sensitive Personal Information Securely and Protect it during Transmission

- For many companies, storing sensitive data is a business necessity
- Even if you take appropriate steps to secure the network, sometimes you have to send that data elsewhere
- Use strong cryptography to secure confidential material during storage and transmission
- The method will depend on the types of information the business collects, how it is collected and how it is processed
- Explore possibilities
- Given the nature of the business, some possibilities may include:
 - Transport Layer Security/Secure Sockets Layer (TLS/SSL) encryption
 - Data-at-rest encryption, or
 - An iterative cryptographic hash

68

Center for Agricultural Law & Taxation

Store Sensitive Personal Information Securely and Protect it during Transmission

- Regardless of the method, it's only as good as the personnel who implement it
- Make sure the people designated to do the job understand how the company uses sensitive data and have the know-how to determine what's appropriate for each situation
 - Keep sensitive information secure throughout its lifecycle
 - Use industry-tested and accepted methods
 - Ensure proper configuration

69

Center for Agricultural Law & Taxation

Segment Your Network and Monitor Who's Trying to Get In and Out

- When designing the network, consider using tools like firewalls to segment the network, thereby limiting access between computers on the network and between each computer and the internet
 - Not every computer in the system needs to be able to communicate with every other one
 - Help protect particularly sensitive data by housing it in a separate secure place on the network

70

Center for Agricultural Law & Taxation

Segment Your Network and Monitor Who's Trying to Get In and Out

- Another useful safeguard: intrusion detection and prevention tools to monitor the network for malicious activity

71

Center for Agricultural Law & Taxation

The Plan – Ideas in Putting Together Your Plan

- Business Name, address, etc
- Alternate location where operations can be conducted
- Emergency Contact Information
- Non-emergency contacts
- Insurance provider(s)
- Key Crisis Managers and contact information
- Identify potential disasters that could impact the business
- Appoint an emergency planning team

72

Center for Agricultural Law & Taxation

The Plan

- Team should coordinate with other businesses as needed
 - Many small business work in same general location – coordination may be necessary
- Prioritize what operations are critical, establish a person in charge and develop an action plan in case of an emergency
- Don't forget the day to day suppliers or other businesses you depend on to operate
 - Establish a list of contacts that need to be made

73

Center for Agricultural Law & Taxation

The Plan

- Develop a plan for quick evacuation and a more leisure evacuation
 - What records need to be secured or moved
 - What security needs to be in place if records are moved or downloaded
 - What back-up's need to be made and how will they be stored
 - Conduct at least one meeting per year to review the evacuation plan and the responsibilities of each persons assigned duties

74

Center for Agricultural Law & Taxation

The Plan

- Make sure all in office are aware of the emergency plan
- Determine how will the staff communicate if a disaster occurs

75

Center for Agricultural Law & Taxation

The Plan- Computer Security

- Protect hardware, software and back-ups

76

Center for Agricultural Law & Taxation

Data Back-Up

- Who backs up data?
- How often is it backed up?
- Records that should always remain handy
 - Insurance policies
 - Bank account records
 - Computer backups

77

Center for Agricultural Law & Taxation

Data Loss

- Business name
- Business employer identification number (EIN) associated with the data loss
- Contact name
- Contact phone number
- Summary of how the data loss occurred
- Volume of records impacted

78

Center for Agricultural Law & Taxation

What To Do?

- Review Taxpayer Guide to Identity Theft
- Share IRS Publication 5027, Identity Theft Information for Taxpayers, with employees and direct them to the "Steps for Identity Theft Victims" which includes:
 - Contacting one of the three credit bureaus to place a "fraud alert" on their account
 - The taxpayer may consider placing a "credit freeze" which offers more protection
 - File a complaint with the Federal Trade Commission
 - Review FTC www.identitytheft.gov information for additional steps to recover from identity theft
 - The FTC also offers guidance to businesses on how to inform employees of the incident and additional steps businesses may take

79

Center for Agricultural Law & Taxation

Data Breach Response

- Data Breach Response: A Guide for Business
- Share IRS Publication 4524, Security Awareness for Taxpayers, with your employees

80

Center for Agricultural Law & Taxation

Remember

- The IRS doesn't initiate contact with taxpayers by email, text messages or social media channels to request personal or financial information
- Any contact from the IRS will be in response to a contact initiated by you
- Cybercriminals, when they learn of a new IRS process, often create false IRS web sites and IRS impersonation emails

81

Center for Agricultural Law & Taxation

Common Sense

- Always use robust security software for all computers and devices, and routinely perform deep scans often to identify any malware/virus infections
- Use strong password to access computers and client files
- Learn to recognize and avoid phishing email schemes

82

Center for Agricultural Law & Taxation

The Data Has Been Breached

- Should you experience a data compromise – whether by cybercriminals, theft or accident – there are certain basic steps you should take
- Preliminary steps include:
 - Contacting the IRS and law enforcement:
 - Contact your software provider
 - If reported quickly, the IRS can take steps to block fraudulent returns in your clients' names
 - Federal Bureau of Investigation, your local office
 - Secret Service, your local office (if directed).
 - Local police – To file a police report on the data breach

83

Center for Agricultural Law & Taxation

State Contacts

- Any breach of personal information could have an effect on the victim's tax accounts with the states as well as the IRS
- You should email the Federation of Tax Administrators at StateAlert@taxadmin.org to get information on how to report victim information to the states
- State Attorneys General for each state in which you prepare returns
- Most states require that the attorney general be notified of data breaches
- This notification process may involve multiple offices

84

Center for Agricultural Law & Taxation

Contacting Clients and Other Services

- Federal Trade Commission
- If you would like more individualized guidance, you may contact the FTC at idt-brt@ftc.gov
- Credit / ID theft protection agency- certain states require offering credit monitoring / ID theft protection to victims of ID theft
- Credit bureaus – to notify them if there is a compromise and clients may seek their services

85

Center for Agricultural Law & Taxation

Contacting Clients and Other Services

- Clients – Send an individual letter to all victims to inform them of the breach but work with law enforcement on timing
- Clients should complete IRS Form 14039, Identity Theft Affidavit, only if they receive a notice/letter from the IRS or their e-filed return is rejected because of a duplicate Social Security number

86

Center for Agricultural Law & Taxation

Requesting a Copy of a Fraudulent Return

- Form 4506-F, Request for a Copy of a Fraudulent Tax Return, and mail along the required documentation to the following address:
- IRS, Fresno, CA 93888-0025

Return Information	Redaction
Names of the primary taxpayer, secondary taxpayer, and dependents (or children reported for other tax benefits)	Entire name except the first four letters of the last name (if the last name is four letters or less, then fewer than four letters of the last name will remain visible.)
Address of the primary and secondary taxpayers	Entire address except the street name
Names and address of all other persons or entities on return	Entire name and address
Taxpayer identification numbers (SSN/ITIN) and employer identification numbers (EIN)	Entire number except the last four digits
Personally identifiable numbers, such as Designee's Personal Identification Number (DPIN), Preparer's Tax Identification Number (PTIN), etc.	Entire number
IP address and names of software companies	Entire name and address
Telephone number(s)	Entire number except the last four digits
Bank routing and account number(s)	Entire number except the last four digits
Signature	Entire signature

1

Center for Agricultural Law & Taxation

Form 4506-F

Form 4506-F <small>(July 2016)</small>	Department of the Treasury - Internal Revenue Service Request for Copy of Fraudulent Tax Return <small>Do not sign this form unless all applicable fees have been completed. Request may be rejected if the form is incomplete or illegible. For more information about Form 4506-F, visit www.irs.gov/form4506-F.</small>	OMB Number 1545-0429
--	---	-------------------------

Read this information first

When should I complete this form? You should use this form if you are the person whose name and Social Security Number (SSN) was used to file a fraudulent tax return. Due to federal privacy laws, the victim's name and SSN must be listed as either primary or secondary taxpayer on the fraudulent return; otherwise the IRS cannot disclose the return information. For this reason, the IRS cannot disclose return information to any person listed only as a dependent.

Step 1 - Provide Taxpayer Information

1 Social Security Number (SSN) used on fraudulent return 2 Name used on fraudulent return
 3 SSN owner's current street address 3a SSN owner's current city, state, and ZIP
 4 SSN owner's complete address shown on last return if different from above

Step 2 - Provide Requestor Information

5 What is your relationship to the taxpayer named in Step 1?
 Check the box that best applies.
 Self (you are the taxpayer)
 Parent or guardian of a minor child
 Representative named on Form 2848, Power of Attorney
 Guardian, executor, or representative named on court documents

NOTE: The person making this request must provide a copy of a government-issued identification and, if you are not the taxpayer, documents demonstrating your authority to receive the requested tax information. See instructions.

Center for Agricultural Law & Taxation

Form 14039

Form 14039 <small>(April 2017)</small>	Department of the Treasury - Internal Revenue Service Identity Theft Affidavit	OMB Number 1545-2139
--	--	-------------------------

Complete this form if you need the IRS to mark an account to identify questionable activity.

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

- 1. I am submitting this Form 14039 for myself.
- 2. This Form 14039 is submitted in response to a "Notice" or "Letter" received from the IRS.
 - Please provide "Notice" or "Letter" number(s) on the line to the right.
 - Please check box 1 in **Section B** and see special mailing and timing instructions on reverse side of this form.
- 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 C** 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 C** 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.

Center for Agricultural Law & Taxation

Form 14039

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

Victim's last name	First name	Middle initial	Taxpayer Identification Number (Please provide 9-digit Social Security Number)
--------------------	------------	----------------	--

Current mailing address (apartment or suite number and street, or P.O. Box) If deceased, please provide last known address.

Current city State ZIP code

Tax Year(s) 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") **Names 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"

Home telephone number Cell phone number Best time(s) to call

Language in which you would like to be contacted English Spanish

Section D - Penalty of 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 Date signed

Submit this completed form to either the mailing address or the FAX number provided on the reverse side of this form.

Catalog Number 52526A www.irs.gov Form **14039** (Rev. 4-2017) 90

Center for Agricultural Law & Taxation

Form 14039

Section E -- Representative, Conservator, Parent or Guardian Information (Required if completing Form 14039 on someone else's behalf)

Check only ONE of the following five boxes next to the reason you are submitting this form.

- 1. The taxpayer is deceased and I am the surviving spouse
 - No attachments are required, including death certificate.
- 2. The taxpayer is deceased and I am the court-appointed or certified personal representative
 - Attach a copy of the court certificate showing your appointment.
- 3. The taxpayer is deceased and a court-appointed or certified personal representative has not been appointed
 - Attach copy of death certificate or formal notification from a government office informing next of kin of the decedent's death.
 - Indicate your relationship to decedent: Child Parent/Legal Guardian Other
- 4. The taxpayer is unable to complete this form and I am the appointed conservator or have Power of Attorney/Declaration of Representative authorization per IRS Form 2848
 - Attach a copy of documentation showing your appointment as conservator or POA authorization.
 - If you have an IRS issued Centralized Authorization File (CAF) number, enter the nine-digit number: _____
- 5. The person is my dependent child or my dependent relative
 - By checking this box and signing below you are indicating that you are an authorized representative, as parent, guardian or legal guardian, to file a legal document on the dependent's behalf.
 - Indicate your relationship to person: Parent/Legal Guardian Fiduciary Relationship per IRS Form 56 Power of Attorney Other

Representative's name _____
 Last name _____ First name _____ Middle initial _____
 Representative's current mailing address (City, town or post office, state, and ZIP code) _____
 Representative's telephone number _____

Center for Agricultural Law & Taxation

Form 14039

Instructions for Submitting this Form

Submit this completed and signed form to the IRS via **Mail** or **FAX** to specialized IRS processing areas dedicated to assist you in **Section C** of this form, be sure to include the Social Security Number in the 'Taxpayer Identification Number' field.

Help us avoid delays:

- Choose one method of submitting this form either by Mail or by FAX, not both.
- Please provide clear and readable photocopies of any additional information you may choose to provide.
- Note that tax returns may not be submitted to either the mailing address or FAX number.

Submitting by Mail

- If you checked **Box 1** in **Section B** in response to a notice or letter received from the IRS, return this form and, if possible, a copy of the notice or letter to the address contained in the notice or letter.
- If you checked **Box 1** in **Section B** of **Form 14039**, are unable to file your tax return electronically because the primary and/or secondary SSN was misused, attach this **Form 14039** to the back of your paper tax return and submit to the IRS location where you normally file your tax return.
- If you've already filed your paper return, please submit this **Form 14039** to the IRS location where you normally file. Refer to the 'Where Do You File' section of your return instructions or visit IRS.gov and input the search term 'Where to File'.
- If you checked **Box 2** in **Section B** of **Form 14039** (no current tax-related issue), mail this form to:

Department of the Treasury
 Internal Revenue Service
 Fresno, CA 93888-0025

Submitting by FAX

- If you checked **Box 1** in **Section B** of **Form 14039** and are submitting this form in response to a notice or letter received from the IRS, if it provides a FAX number, you should send there.
- If no FAX number is shown on the notice or letter, please follow the mailing instructions on the notice or letter.
- Include a cover sheet marked "Confidential".
- If you checked **Box 2** in **Section B** of **Form 14039** (no current tax-related issue), FAX this form toll-free to:
855-807-5720

Center for Agricultural Law & Taxation

Center for Agricultural Law & Taxation

Insurance



Data Breach Insurance Coverage – Cyber Liability

- When a data breach occurs, quick action is important to help restore the public's confidence if your a business victimized by a cyber attack
- Cyber liability insurance and data breach insurance helps cover costs like notification, identity protection solutions, public relations, legal, liability and more depending on the coverage chosen
- To mitigate the risk of civil litigation and other penalties when a data loss or theft occurs, a cyber liability or data breach insurance policy can provide access to professional assistance to help businesses comply with applicable laws and regulations

94

Center for Agricultural Law & Taxation

Should You Buy Identity Theft Insurance - Individual

- The National Association of Insurance Commissioners says the typical cost of identity theft insurance ranges from \$25 to \$60 per year
- The insurance may include credit alerts, account and credit monitoring, and reimbursement for the costs associated with repairing credit history if you become a victim
- The insurance does not protect you from identity theft – nothing can really do that – and the policy certainly does not cover monetary losses
- Most policies typically have benefit limits ranging from \$10,000 to \$15,000
- Many have deductibles requiring you to pay the first \$100 to \$500 of costs required to restore your financial good name

95

Center for Agricultural Law & Taxation

What Insurance Can Do

- Here are the kinds of things that a case manager could help your client with when they have a claim They could:
- Contact the fraud departments of the three major credit bureaus to place a fraud alert on your credit file
- This alert requires creditors to contact them before opening any new accounts or making any changes to existing accounts
- Order copies of the credit report from all three major credit bureaus to review recent activity
- Close accounts that the client believed were tampered with or opened fraudulently
- Write letters on your behalf to the Social Security Administration, the Department of Motor Vehicles or other agencies
- Provide legal referrals for assistance with court appearances or other legal situations.
- Keep detailed records of the steps taken and remaining to restore identity

96

Center for Agricultural Law & Taxation

The Scoop – Upcoming Dates

- May 17
- May 31
- June 7
- June 21
- July 5
- July 19
- August 2
- August 16
- August 30
- Held at 8:00 am and 12:00 pm Central time

97

Center for Agricultural Law & Taxation

Upcoming Seminars – Mark Your Calendar – Final Dates

- May 11-12, 2017 Back to the Basics: A Foundational Income Tax Return Preparation Course – Live and Webinar
- September 21, 2017 Ag Law Seminar, Live and Webinar
- September 22, 2017 Farm and Estate Tax Review, Live and Webinar
- S Corporation and Entity Review – July 20-21, 2017, Live and Webinar
- Retirement and Social Security Issues(Webinar) = October 10-11, 2017

98

Center for Agricultural Law & Taxation

Back to the Basics: A Foundational Income Tax Return Preparation Course – Live and Webinar

- May 11-12
- Live and Online
- As new income tax return preparers enter the profession, they must quickly build a solid foundation of basic skills
- Some experienced tax preparers—driven by a need to continually produce—may also wonder if they have some holes in this all-important foundation
- In response to this need, CALT is offering a new two-day introductory course focused on teaching the basics of federal income tax return preparation
- Our “Back to the Basics: A Foundational Income Tax Preparation Course” will teach basic tax return preparation skills all tax return preparers must know

99

Center for Agricultural Law & Taxation

Back to the Basics: A Foundational Income Tax Return Preparation Course – Live and Webinar

- Attendees will receive two days of federal individual income tax return preparation training, as well as the opportunity to complete a comprehensive return from beginning to end
- Whether you're new to the profession or simply looking for a comprehensive refresher, we think this course will be of value.
- You'll experience personal interaction with knowledgeable instructors excited about the material and willing to field all types of questions
- This is a great program for new employees needing training in first and second-year tax law and procedures
- It should also serve as an excellent comprehensive refresher for others

100

Center for Agricultural Law & Taxation

Back to the Basics: A Foundational Income Tax Return Preparation Course – Live and Webinar

The interview process and tips for conducting an interview	Who must file
Determination of filing status, including a review of advantages and disadvantages of each	Exemptions/Dependents rules and changes
Taxable and nontaxable income - where to report	Form 1040, line by line
Adjustments to Income	Domestic Production Activity Deduction
Standard Deduction vs. Itemized Deduction	Itemized Deductions
Various Tax Credits Including Child Tax Credit, Earned Income Tax Credit and the American Opportunity Tax Credit, along with associated forms.	Due Diligence Requirements for Credits
Child and Dependent Care Credit	Premium Tax Credit Overview
Schedule C	Depreciation
Schedule E	Business Expenses
Schedule F	Standard Mileage vs. Actual Expenses
Bonus Depreciation	Form 4562
Sale of Business Assets and Form 4797	Capital Gains and Losses, including Schedule D and Form 8949
Casualty Loss	Comprehensive Hands-On Problem

101

Center for Agricultural Law & Taxation

The Schedule is Finalized for the 44th Annual Federal Income Tax Schools



- November 2-3, 2017 – Maquoketa, Iowa – Centerstone Inn and Suites
- November 6-7, 2017 – Le Mars, Iowa – Le Mars Convention Center
- November 8-9, 2017 – Atlantic, Iowa – Cass County Community Center
- November 9-10, 2017 – Mason City, Iowa – North Iowa Area Community College
- November 16-17, 2017 – Ottumwa, Iowa – Indian Hills Community College
- November 20-21, 2017 – Waterloo, Iowa – Hawkeye Community College
- December 11-12, 2017 – Ames, Iowa and Live Webinar – Quality Inn and Suites

Center for Agricultural Law & Taxation

Center for Agricultural Law & Taxation

The CALT Staff

Kristine A. Tidgren
Assistant Director
E-mail: ktidgren@iastate.edu
Phone: (515) 294-6365
Fax: (515) 294-0700



The CALT Staff

<p>Kristy S. Maitre Tax Specialist E-mail: ksmaitre@iastate.edu Phone: (515) 296-3810 Fax: (515) 294-0700</p> 	<p>Tiffany L. Kayser Program Administrator E-mail: tlkayser@iastate.edu Phone: (515) 294-5217 Fax: (515) 294-0700</p> 
--	--

Center for Agricultural Law & Taxation
