

# **RSAC** Studio



Connect **to**  
Protect

## **Hacking Healthcare: Attacks on the Highest Value Asset**

**Paul Dant**

Chief Strategy Officer  
Independent Security Evaluators

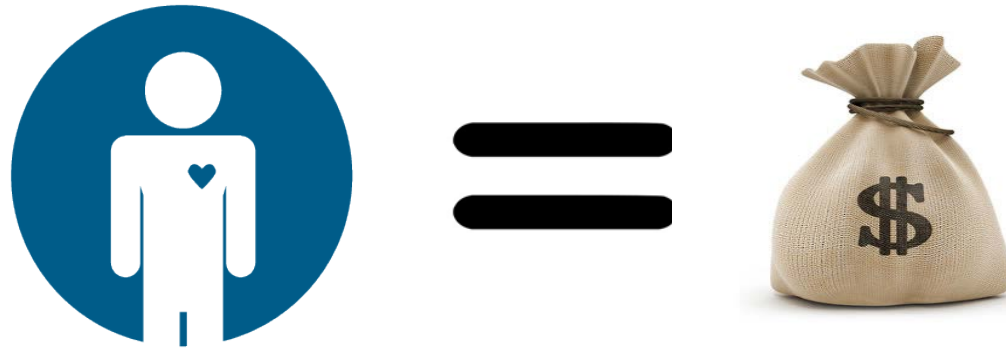


#RSAC

# The Key Takeaway



#RSAC



# Who am I?



#RSAC



**Paul Dant**

**Chief Strategist @ ISE**

9: First digital product

13: First blackhat hack

17: First hacker caught

19: First whitehat hack

# Who is ISE?



#RSAC



# Our Roles for Today



## My Role

Paint a picture...

- What we should be protecting
- Who we are defending against
- How do we fix the problem

## Your Role

Interpret the picture...

- Understand the correct mission
- Understand the right approach
- Realize success

# How Can You Apply in Practice?



#RSAC

- Recognize the high value asset and defend accordingly
- Understand that regulations and compliance should follow, not lead
- Developing and implementing a strategic plan is critical to success

# Why Patient Health?



# Why Patient Health?



#RSAC

We tend to focus on these...





# Why Patient Health?



## Wrong Mission + Outdated Approach = Failure

*Focusing on Patient Records*

*Ignoring Advanced Threats*

*Patients at Risk*

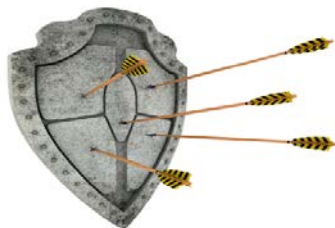
# Why Patient Health?



includes



# Why Patient Health?



# What are the Threats?



#RSAC

Casual Hacker



Hacktivist



Corporate Espionage



Organized Crime



Nation State



# What are the Threats?



#RSAC



# A Simple Business Decision



IF

COST

RISK

REWARD

$\$ + \text{skull and crossbones} < \text{money bag} = \text{DO IT!}$

# Attributes of an Attacker



#RSAC



# How Do We Know?





# Medical Device Security Research



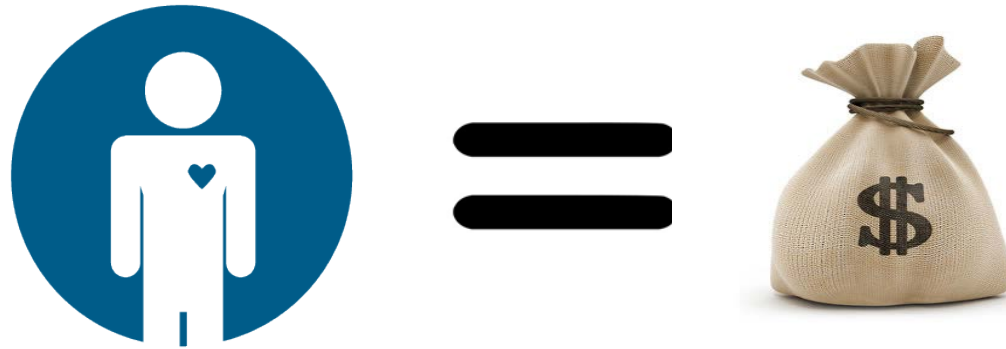
#RSAC



 **HACKED**



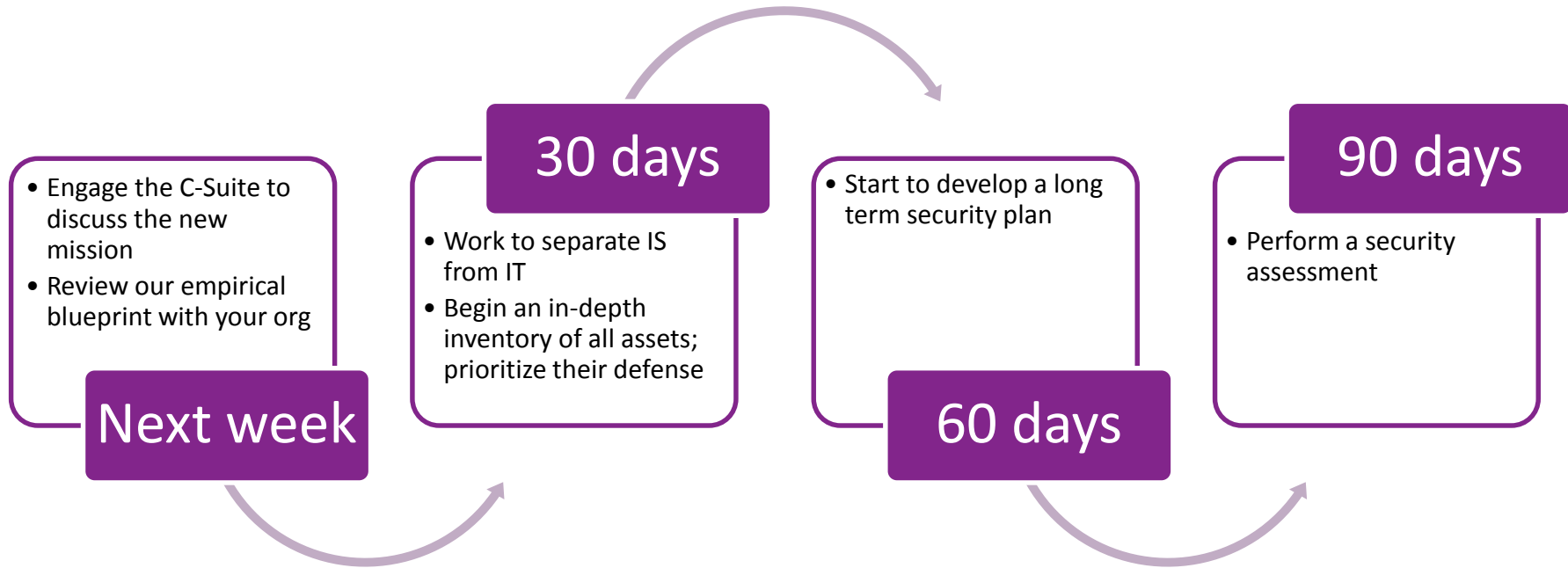
# What's the Solution?

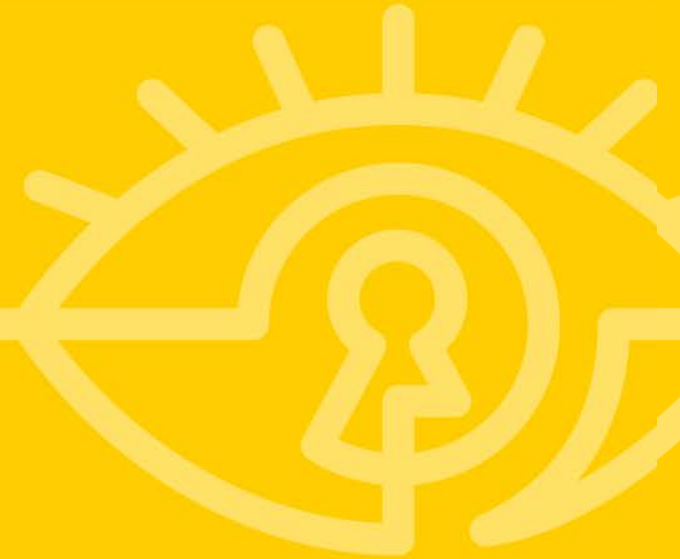


# Call to Action



#RSAC





**Paul Dant**  
**[pdant@securityevaluators.com](mailto:pdant@securityevaluators.com)**

# **RSA**<sup>®</sup>C Studio



Connect **to**  
Protect

## **How'd This Happen? A Journey in PII Pwned Reconciliation**

**Chad Skipper**

Distinguished Engineer  
Dell CTO  
[@chadskipper](#)



#RSAC

# The Date Of Awareness



# The Date Of Awareness



#RSAC

April 13



“What’s mine say?  
Dude!”

“What’s mine say?  
Sweet!”

# The Date Of Awareness

#RSAC



Department of Treasury  
Internal Revenue  
PO BOX 249  
Memphis, TN 381

JAMES & KAREN  
22 BOULDER ST  
HANSON, CT 001



Department of Treasury  
Internal Revenue Service  
PO BOX 249  
Memphis, TN 38101-0249

JAMES & KAREN Q. HINDS  
22 BOULDER STREET  
HANSON, CT 00000-7253

Notice CP53

Notice CP53  
Tax year 9999  
Notice date Month 99, 9999  
Social Security number 999-99-9999  
To contact us Phone 1-999-999-9999  
Your Caller ID 1234  
Page 1 of 1

## Message about your 200 Your refund cl

We can't honor requests for i  
refunds for prior year returns  
should receive a refund ched  
3-4 weeks for your 2000 For  
overpayment.

### Additional informati

## Message about your 2000 Form 1040 Your refund check will be sent by mail

We can't honor requests for direct deposit of  
refunds for prior year returns. As a result, you  
should receive a refund check in the mail in  
3-4 weeks for your 2000 Form 1040  
overpayment.

### Additional information

### What you need to do

If you don't receive your refund check  
1-999-999-9999.

- Visit [www.irs.gov/cp53](http://www.irs.gov/cp53).
  - Keep this notice for your records.
- If you need assistance, please don't

April 13





# The Date Of Awareness



April 13



# The Date Of Awareness

#RSAC



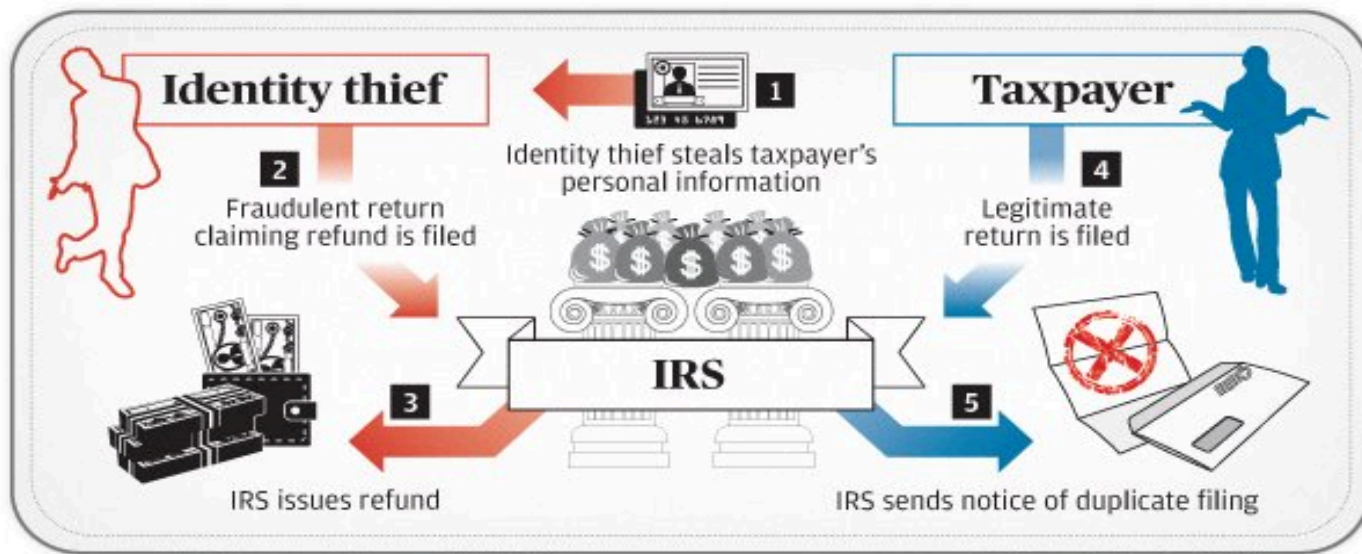
# How Tax Fraud Works



#RSAC

## How identity theft refund fraud works

In refund fraud, an identity thief uses a taxpayer's name and Social Security number to file for a tax refund, which the IRS discovers only after the legitimate taxpayer files.



Source: U.S. Government Accountability Office

Staff graphic by Gerald Fullam

# The Journey of Reconciliation



#RSAC

- Called the IRS Fraud Hotline – 1-800-908-4490

Form 14039  
Rev. February 2014

Department of the Treasury - Internal Revenue Service

**Identity Theft Affidavit**

OMB Number 1545-2139

Complete and submit this form if you are an actual or potential victim of identity theft and would like the IRS to mark your account to identify questionable activity.

Check only one of the following two boxes if they apply to your specific situation. (Optional for all filers.)

☐ I am submitting this form in response to a mailed notice or letter from the IRS.

☐ I am completing this form on behalf of another person, such as a deceased spouse or other deceased relative. You should provide information for the actual or potential victim in Sections A, B, & D.

**Note to all filers:** Failure to provide required information on **BOTH** sides of this form **AND** clear and legible documentation will delay processing.

**THIS FORM MUST BE SIGNED ON THE REVERSE SIDE (SECTION F).**

**Section A - Reason For Filing This Form** (Required for all filers)

Check only **ONE** of the following two boxes. You **MUST** provide the requested description or explanation in the lined area below.

1 ☐ I am a victim of identity theft **AND** it is affecting my federal tax records.

You should check this box if, for example, your attempt to file electronically was rejected because someone had already filed using your Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN), or if you received a notice or correspondence from the IRS indicating someone was otherwise using your number.

Provide a short explanation of the problem and how you were made aware of it.

2 ☐ I have experienced an event involving my personal information that may at some future time affect my federal tax records.

You should check this box if you are the victim of non-federal tax related identity theft, such as the misuse of your personal identity information to obtain credit. You should also check this box if no identity theft violation has occurred, but you have experienced an event that could result in identity theft, such as a lost/broken purse or wallet, home robbery, etc.

Briefly describe the identity theft violation(s) and/or the event(s) of concern. Include the date(s) of the incident(s).

**Section B - Taxpayer Information** (Required for all filers)

Taxpayer's last name	First name	Middle initial	The last 4 digits of the taxpayer's SSN or the taxpayer's complete individual Taxpayer Identification Number (ITIN)

# The Journey of Reconciliation



#RSAC

- Called the IRS Fraud Hotline – 1-800-908-4490
- Verified that a fraudulent tax refund was submitted for 2014

Form 14039  
Rev. February 2014

Department of the Treasury - Internal Revenue Service

**Identity Theft Affidavit**

OMB Number 1545-2139

Complete and submit this form if you are an actual or potential victim of identity theft and would like the IRS to mark your account to identify questionable activity.

Check only one of the following two boxes if they apply to your specific situation. (Optional for all filers.)

☐ I am submitting this form in response to a mailed notice or letter from the IRS.

☐ I am completing this form on behalf of another person, such as a deceased spouse or other deceased relative. You should provide information for the actual or potential victim in Sections A, B, & D.

**Note to all filers:** Failure to provide required information on BOTH sides of this form AND clear and legible documentation will delay processing.

**THIS FORM MUST BE SIGNED ON THE REVERSE SIDE (SECTION F).**

**Section A - Reason For Filing This Form** (Required for all filers)

Check only **ONE** of the following two boxes. You **MUST** provide the requested description or explanation in the lined area below.

**1** ☐ I am a victim of identity theft AND it is affecting my federal tax records.

**2** ☐ I have experienced an event involving my personal information that may at some future time affect my federal tax records.

You should check this box if, for example, your attempt to file electronically was rejected because someone had already filed using your Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN), or if you received a notice or correspondence from the IRS indicating someone was otherwise using your number.

You should check this box if you are the victim of non-federal tax related identity theft, such as the misuse of your personal identity information to obtain credit. You should also check this box if no identity theft violation has occurred, but you have experienced an event that could result in identity theft, such as a lost/broken purse or wallet, home robbery, etc.

**Provide a short explanation of the problem and how you were made aware of it.**

**Briefly describe the identity theft violation(s) and/or the event(s) of concern. Include the date(s) of the incident(s).**

**Section B - Taxpayer Information** (Required for all filers)

Taxpayer's last name	First name	Middle initial	The last 4 digits of the taxpayer's SSN or the taxpayer's complete individual Taxpayer Identification Number (ITIN)



# The Journey of Reconciliation



#RSAC

- Called the IRS Fraud Hotline – 1-800-908-4490
- Verified that a fraudulent tax refund was submitted for 2014
- IRS received fraudulent tax return on March 19th 10:24:09 EST - submitted electronically

**Form 14039**  
Rev. February 2014

Department of the Treasury - Internal Revenue Service  
**Identity Theft Affidavit**

OMB Number  
1545-2139

Complete and submit this form if you are an actual or potential victim of identity theft and would like the IRS to mark your account to identify questionable activity.

Check only one of the following two boxes if they apply to your specific situation. (Optional for all filers.)

☐ I am submitting this form in response to a mailed notice or letter from the IRS.

☐ I am completing this form on behalf of another person, such as a deceased spouse or other deceased relative. You should provide information for the actual or potential victim in Sections A, B, & D.

**Note to all filers:** Failure to provide required information on **BOTH** sides of this form **AND** clear and legible documentation will delay processing.

**THIS FORM MUST BE SIGNED ON THE REVERSE SIDE (SECTION F).**

**Section A - Reason For Filing This Form** (Required for all filers)

Check only **ONE** of the following two boxes. You **MUST** provide the requested description or explanation in the lined area below.

**1** ☐ I am a victim of identity theft **AND** it is affecting my federal tax records.

**2** ☐ I have experienced an event involving my personal information that may at some future time affect my federal tax records.

*You should check this box if, for example, your attempt to file electronically was rejected because someone had already filed using your Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN), or if you received a notice or correspondence from the IRS indicating someone was otherwise using your number.*

*You should check this box if you are the victim of non-federal tax related identity theft, such as the misuse of your personal identity information to obtain credit. You should also check this box if no identity theft violation has occurred, but you have experienced an event that could result in identity theft, such as a lost/broken purse or wallet, home robbery, etc.*

Provide a short explanation of the problem and how you were made aware of it.

Briefly describe the identity theft violation(s) and/or the event(s) of concern. Include the date(s) of the incident(s).

**Section B - Taxpayer Information** (Required for all filers)

Taxpayer's last name	First name	Middle initial	The last 4 digits of the taxpayer's SSN or the taxpayer's complete individual Taxpayer Identification Number (ITIN)

# The Journey of Reconciliation



#RSAC

- Called the IRS Fraud Hotline – 1-800-908-4490
- Verified that a fraudulent tax refund was submitted for 2014
- IRS received fraudulent tax return on March 19th 10:24:09 EST – submitted electronically
- Action – Return Check and submit Identity Theft Affidavit Form 14039 for each person

**Form 14039**  
Rev. February 2014

Department of the Treasury • Internal Revenue Service  
**Identity Theft Affidavit**

OMB Number  
1545-2139

Complete and submit this form if you are an actual or potential victim of identity theft and would like the IRS to mark your account to identify questionable activity.

Check only one of the following two boxes if they apply to your specific situation. (Optional for all filers.)

☐ I am submitting this form in response to a mailed notice or letter from the IRS.

☐ I am completing this form on behalf of another person, such as a deceased spouse or other deceased relative. You should provide information for the actual or potential victim in Sections A, B, & D.

**Note to all filers:** Failure to provide required information on **BOTH** sides of this form **AND** clear and legible documentation will delay processing.

**THIS FORM MUST BE SIGNED ON THE REVERSE SIDE (SECTION F).**

**Section A – Reason For Filing This Form** (Required for all filers)

Check only **ONE** of the following two boxes. You **MUST** provide the requested description or explanation in the lined area below.

**1** ☐ I am a victim of identity theft **AND** it is affecting my federal tax records.

**2** ☐ I have experienced an event involving my personal information that may at some future time affect my federal tax records.

*You should check this box if, for example, your attempt to file electronically was rejected because someone had already filed using your Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN), or if you received a notice or correspondence from the IRS indicating someone was otherwise using your number.*

*You should check this box if you are the victim of non-federal tax related identity theft, such as the misuse of your personal identity information to obtain credit. You should also check this box if no identity theft violation has occurred, but you have experienced an event that could result in identity theft, such as a lost/broken purse or wallet, home robbery, etc.*

Provide a short explanation of the problem and how you were made aware of it.

Briefly describe the identity theft violation(s) and/or the event(s) of concern. Include the date(s) of the incident(s).

**Section B – Taxpayer Information** (Required for all filers)

Taxpayer's last name	First name	Middle initial	The last 4 digits of the taxpayer's SSN or the taxpayer's complete individual Taxpayer Identification Number (ITIN)
----------------------	------------	----------------	---

# The Journey of Reconciliation



#RSAC

- Fraudster has more rights than victim

**Form 14039**  
Rev. February 2014  
Department of the Treasury - Internal Revenue Service  
**Identity Theft Affidavit**  
OMB Number 1545-2139

Complete and submit this form if you are an actual or potential victim of identity theft and would like the IRS to mark your account to identify questionable activity.

Check only one of the following two boxes if they apply to your specific situation. (Optional for all filers)

☐ I am submitting this form in response to a mailed notice or letter from the IRS.

☐ I am completing this form on behalf of another person, such as a deceased spouse or other deceased relative. You should provide information for the actual or potential victim in Sections A, B, & C.

**Note to all filers:** Failure to provide requested information on BOTH sides of this form AND clear and legible documentation will delay processing.

**THIS FORM MUST BE SIGNED ON THE REVERSE SIDE (SECTION F).**

**Section A - Reason For Filing This Form (Required for all filers)**

Check only ONE of the following two boxes. You MUST provide the requested description or explanation in the lined area below.

1 ☐ I am a victim of identity theft AND it is affecting my federal tax records.

2 ☐ I have experienced an event involving my personal information that may at some future time affect my federal tax records.

You should check this box if, for example, your attempt to file electronically was rejected because someone had already filed using your Social Security Number (SSN) or individual Taxpayer Identification Number (ITIN), or if you received a notice or correspondence from the IRS indicating someone was otherwise using your number.

Provide a short explanation of the problem and how you were made aware of it.

**Section B - Taxpayer Information (Required for all filers)**

Taxpayer's last name First name Middle initial The last 4 digits of the taxpayer's SSN or the taxpayer's complete individual Taxpayer Identification Number (ITIN)



# The Journey of Reconciliation



#RSAC

- Fraudster has more rights than victim
- Can no longer file refund electronically for 3 years

The image displays three overlapping copies of Form 14039, "Identity Theft Affidavit," from the Department of the Treasury, Internal Revenue Service. The forms are dated February 2014 and have OMB Number 1545-2139. The forms are designed to be completed by victims of identity theft to report the crime to the IRS. Key sections include:

- Section A - Reason For Filing This Form (Required for all filers):** This section requires the filer to check one of two boxes: "I am a victim of identity theft AND it is affecting my federal tax records" or "I have experienced an event involving my personal information that may at some future time affect my federal tax records." It also includes a note to provide information for the actual or potential victim in Sections A, B, & D.
- Section B - Taxpayer Information (Required for all filers):** This section requires the filer to provide their name, address, and Social Security Number (SSN) or Taxpayer Identification Number (TIN).
- Section C - Taxpayer's last name:** This section requires the filer to provide their last name.
- Section D - Taxpayer's last name:** This section requires the filer to provide their last name.

The forms are presented in a way that shows the layout of the document, including the "THIS FORM MUST BE SIGNED ON THE REVERSE SIDE (SECTION F)" instruction and the "Section B - Taxpayer Information" section.

# The Journey of Reconciliation



#RSAC

- Fraudster has more rights than victim
- Can no longer file refund electronically for 3 years
- Will cause 180 day delay upon tax return filed

Form 14039  
Rev. February 2014  
Department of the Treasury - Internal Revenue Service  
Identity Theft Affidavit  
OMB Number 1545-2139

Complete and submit this form if you are an actual or potential victim of identity theft and would like the IRS to mark your account to identify questionable activity.

Check only one of the following two boxes if they apply to your specific situation. (Optional for all filers)

☐ I am submitting this form in response to a mailed notice or letter from the IRS.

☐ I am completing this form on behalf of another person, such as a deceased spouse or other deceased relative. You should provide information for the actual or potential victim in Sections A, B, & C.

**Note to all filers:** Failure to provide requested information on BOTH sides of this form AND clear and legible documentation will delay processing.

**THIS FORM MUST BE SIGNED ON THE REVERSE SIDE (SECTION F).**

Check only ONE of the following two boxes. You MUST provide the requested description or explanation in the lined area below.

1 ☐ I am a victim of identity theft AND it is affecting my federal tax records.

2 ☐ I have experienced an event involving my personal information that may at some future time affect my federal tax records.

You should check this box if, for example, your attempt to file electronically was rejected because someone had already filed using your Social Security Number (SSN) or individual Taxpayer Identification Number (ITIN), or if you received a notice or correspondence from the IRS indicating someone was otherwise using your number.

Provide a short explanation of the problem and how you were made aware of it.

You should check this box if you are the victim of non-federal tax related identity theft, such as the misuse of your personal identity information to obtain credit. You should also check this box if no identity theft violation has occurred, but you have experienced an event that could result in identity theft, such as a lost purse or wallet, home robbery, etc.

Briefly describe the identity theft violation(s) and/or the event(s) of concern. Include the date(s) of the incident(s).

**Section B - Taxpayer Information (required for all filers)**

Taxpayer's last name	First name	Middle initial	The last 4 digits of the taxpayer's SSN or the taxpayer's complete individual Taxpayer Identification Number (ITIN)

# The Journey of Reconciliation



#RSAC

- Fraudster has more rights than victim
- Can no longer file refund electronically for 3 years
- Will cause 180 day delay upon tax return filed
- Additional details from IRS will be sent by mail

Form 14039  
Rev. February 2014  
Department of the Treasury - Internal Revenue Service  
**Identity Theft Affidavit**  
OMB Number 1545-2139

Complete and submit this form if you are an actual or potential victim of identity theft and would like the IRS to mark your account to identify questionable activity.

Check only one of the following two boxes if they apply to your specific situation. (Optional for all filers)

☐ I am submitting this form in response to a mailed notice or letter from the IRS.

☐ I am completing this form on behalf of another person, such as a deceased spouse or other deceased relative. You should provide information for the actual or potential victim in Sections A, B, & C.

**Note to all filers:** Failure to provide requested information on BOTH sides of this form AND clear and legible documentation will delay processing.

**THIS FORM MUST BE SIGNED ON THE REVERSE SIDE (SECTION F).**

**Section A - Reason For Filing This Form (Required for all filers)**

Check only ONE of the following two boxes if they apply to your specific situation. (Optional for all filers)

☐ I am a victim of identity theft AND it is affecting my federal tax records.

☐ I have experienced an event involving my personal information that may at some future time affect my federal tax records.

**Section B - Taxpayer Information (Required for all filers)**

Taxpayer's last name First name Middle initial The last 4 digits of the taxpayer's SSN or the taxpayer's complete individual Taxpayer Identification Number (ITIN)

# The Journey of Reconciliation



#RSAC

- IC3 – Filed 4/14/15  
<http://www.ic3.gov/complaint/default.aspx>
- FTC – Filed 4/15/15  
<http://www.consumer.ftc.gov/articles/0277-create-identity-theft-report>
- SS Office – Stated to submit to FTC  
<http://www.socialsecurity.gov/myaccount/>



# The Journey of Reconciliation



- [www.transunion.com](http://www.transunion.com) - Added Fraud Alert that will be added to all 3 credit agencies - Equifax / Experian which stays on for 90 days

**EQUIFAX**®

 **Experian**™

 **TransUnion**®

# The Journey of Reconciliation



#RSAC

- [www.transunion.com](http://www.transunion.com) - Added Fraud Alert that will be added to all 3 credit agencies - Equifax / Experian which stays on for 90 days
- Call Banks

**EQUIFAX**®

 **Experian**™

 **TransUnion**®

# The Journey of Reconciliation



#RSAC

- [www.transunion.com](http://www.transunion.com) - Added Fraud Alert that will be added to all 3 credit agencies - Equifax / Experian which stays on for 90 days
- Call Banks
- Submit FTC report to local police

**EQUIFAX**®

 **Experian**™

 **TransUnion**®

# The Journey of Reconciliation



#RSAC

- [www.transunion.com](http://www.transunion.com) - Added Fraud Alert that will be added to all 3 credit agencies - Equifax / Experian which stays on for 90 days
- Call Banks
- Submit FTC report to local police
- Submit FTC report to State Attorney General

**EQUIFAX**®

 **Experian**™

 **TransUnion**®



# Who's Watching Who?



#RSAC



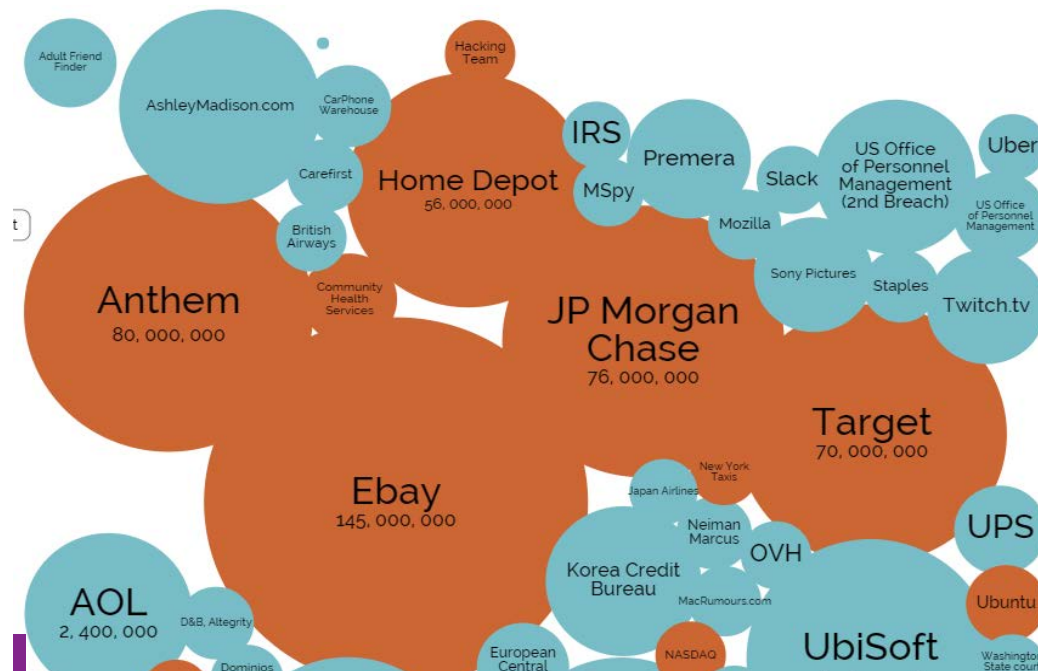
# Who Had It?



#RSAC

Who Had?  
Names  
DOBs  
Current Address  
SSNs

## Recent Large Breaches



# Who Had It?



#RSAC

Who Had?

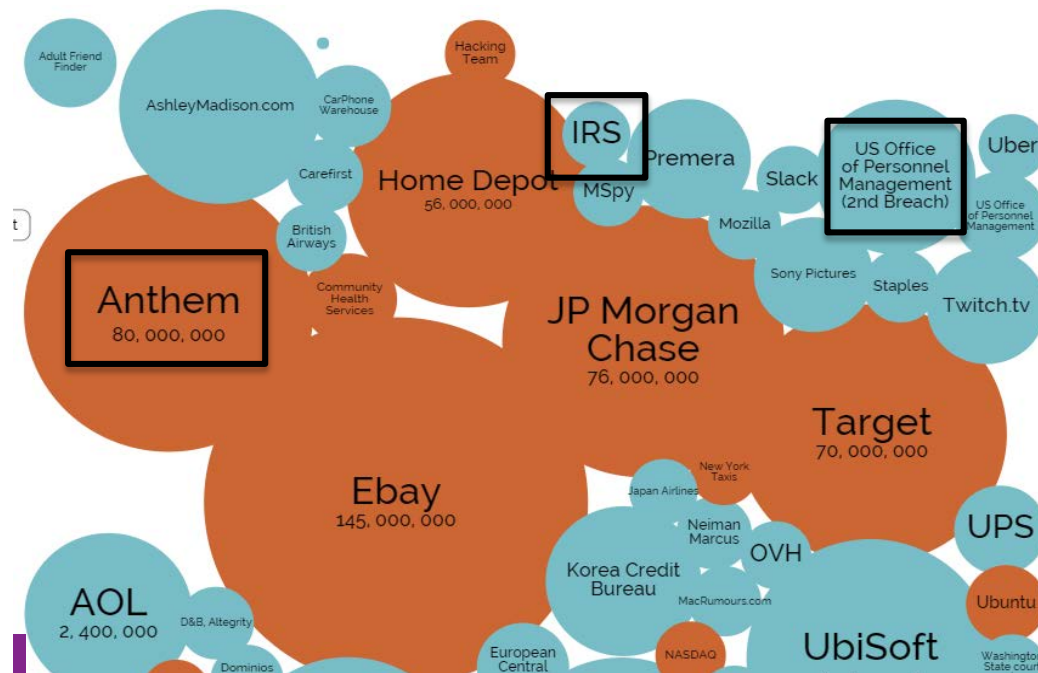
Names

DOBs

Current Address

SSNs

## Recent Large Breaches



# Who Lost It?



#RSAC



IRS denies that I was personally impacted

**Anthem**<sup>®</sup>

Anthem has verified our PII was stolen



OPM  
declined to  
verify if I was  
personally  
impacted

# Who Done It and Why?



#RSAC

- IRS Fraud is its own animal and different beast than credit fraud



# Who Done It and Why?



#RSAC

- IRS Fraud is its own animal and different beast than credit fraud
- Fraudster submits 100s of fraudulent tax returns to deposit in various accounts



# Who Done It and Why?



#RSAC

- IRS Fraud is its own animal and different beast than credit fraud
- Fraudster submits 100s of fraudulent tax returns to deposit in various accounts
- Individuals in Eastern Europe are most suspect





# What To Do?



#RSAC

- Since this was IRS Fraud – Who is watching the IRS?
  - Inspector General
  - No Accountability
- Suspect someone stole your identity and used your SSN for employment purposes or could use your SSN to file a tax return?
  - Complete online form 14039





# How to Reduce Your Risk



#RSAC

- Don't carry your SSN card or any document with your SSN.
- Don't give a business your SSN just because they ask – only when absolutely necessary.
- Check your credit report quarterly.
- Check your Social Security Administration earnings statement annually.
- Protect your personal computers by using firewalls, anti-spam/virus software, update security patches and change passwords for Internet accounts.
- Don't give personal information over the phone, through the mail or the Internet unless you have either initiated the contact or are sure you know who is asking.

# RSA®C Studio



Connect **to**  
Protect

## Thank You

**Chad Skipper**

Distinguished Engineer  
Dell CTO  
@chadskipper



#RSAC