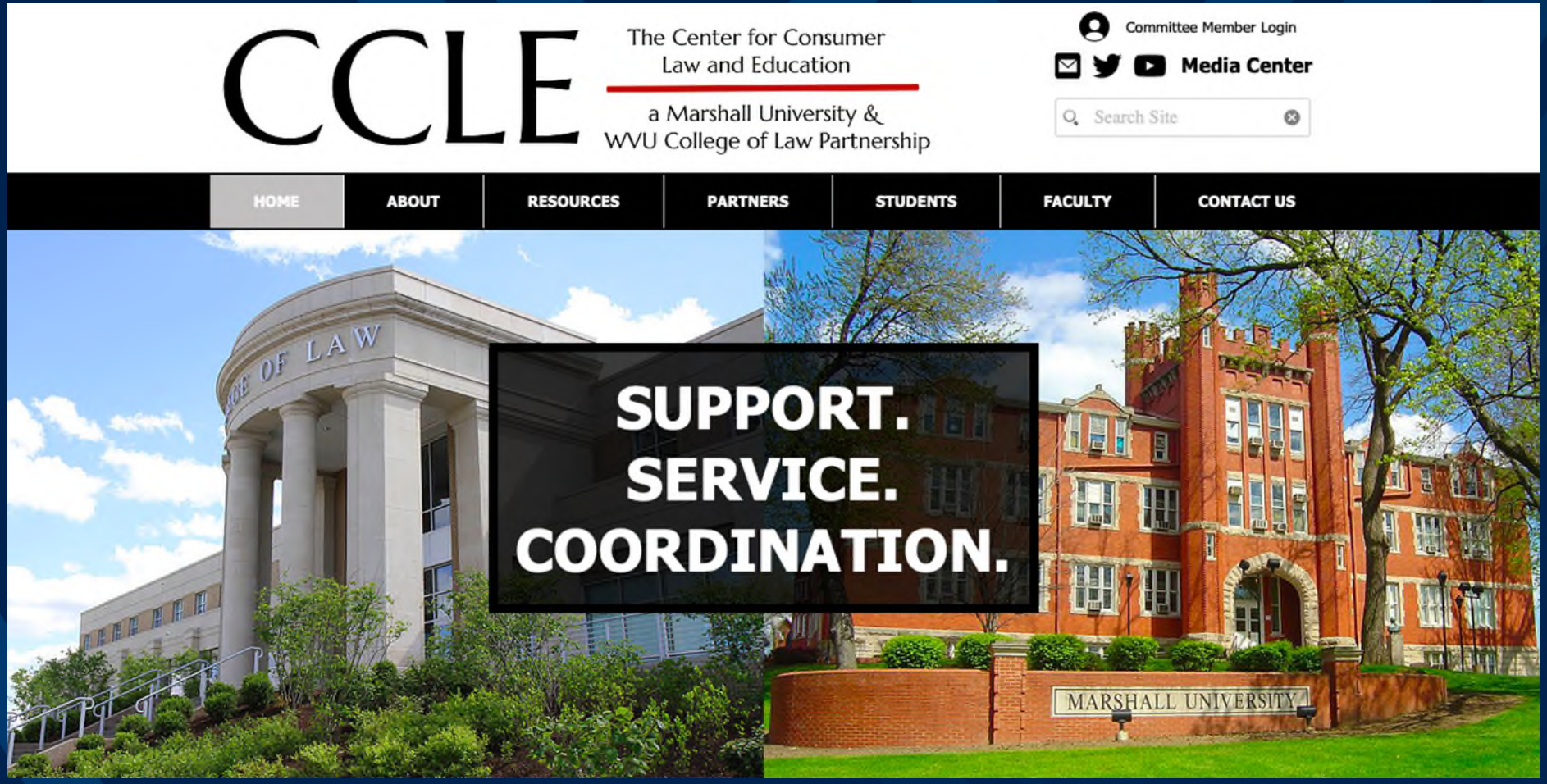
# Ethics: Identity Theft

## Data Privacy, Cybersecurity, Tax-Related Implications and a Discussion with the Director of the Center for Consumer Law and Education


CCLE
The Center for Consumer Law and Education
a Marshall University & WVU College of Law Partnership
Committee Member Login
Media Center
Search Site
HOME
ABOUT
RESOURCES
PARTNERS
STUDENTS
FACULTY
CONTACT US
SUPPORT.
SERVICE.
COORDINATION.
MARSHALL UNIVERSITY

# Consumer Protection

"Consumers, by definition, include us all. They are the largest economic group in the economy, affecting and affected by almost every public and private economic decision. Two-thirds of all spending in the economy is by consumers. But they are the only important group in the economy who are not effectively organized, whose views are often not heard."

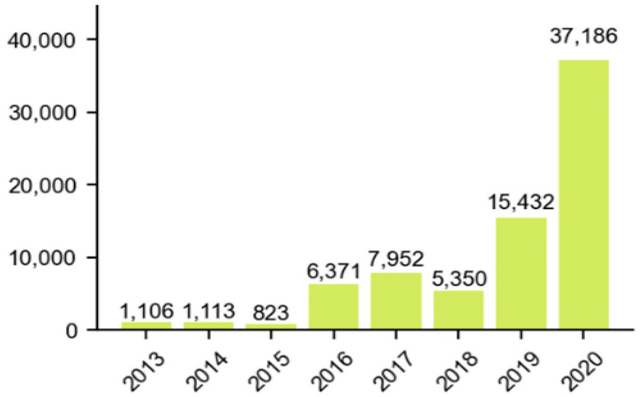
*President Kennedy: Consumer Bill of Rights, March 15, 1962*

# THE TRENDS

Data breach cases, fintech litigation, privacy and cybersecurity compliance/litigation

→ all increasing markets

**Figure 2:** Number of records lost each year (in millions) for the last eight years




**>50%**

feel more exposed to cybersecurity and data protection issues, 11% feel less exposed

**38%**

feel regulators are becoming more interventionist, 17% felt they were less interventionist

**35%**

expect volume of disputes to rise moving forward, only 9% expect volume to decrease


# Privacy


- European Union General Data Protection Regulation (GDPR)
- Congress Seven Bills+++
- California Consumer Privacy Act
- City of Chicago

# LAWS IMPACTING DATA PRIVACY AND SECURITY

- Federal and 50 State Laws Governing:
  - What information can be collected
  - How it must be stored and secured
  - Under what circumstances it can be shared
  - Under what circumstances it can be disclosed
  - Requirements for responding to data breaches and data losses
  - Penalties for data breaches and data losses

- This does not account for international laws . . .

# DATA BREACHES… CONGRESS IS CONCERNED

- ***From a Congressional Technology Working Group***:

***Protect the U.S. from Cyber Attacks***

"Cyber attacks have the potential to bring down our nation's economy, expose our most sensitive information, and even seriously injure or kill American citizens. We will work to enact strong cyber-security protections this Congress that focus on increasing protections in an innovative manner that allows for dynamic solutions to this dynamic problem."

# Moving Forward: Consumer *Privacy* Bill of Rights

A CONSUMER INTERNET PRIVACY

BILL of RIGHTS

The Obama Administration believes America must apply our timeless privacy values to the new technologies and circumstances of our times. Citizens are entitled to have their personal data handled according to these principles.

**Individual Control**
Consumers have a right to exercise control over what personal data companies collect from them and how they use it.

**Access and Accuracy**
Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity and risk associated with the data.

**Transparency**
Consumers have a right to easily understandable and accessible information about privacy and security practices.

**Focused Collection**
Consumers have a right to reasonable limits on the personal data that companies collect and retain.

**Respect for Context**
Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent.

**Accountability**
Companies should be accountable to enforcement authorities and consumers for adhering to these principles.

**Security**
Consumers have a right to secure and responsible handling of personal data.

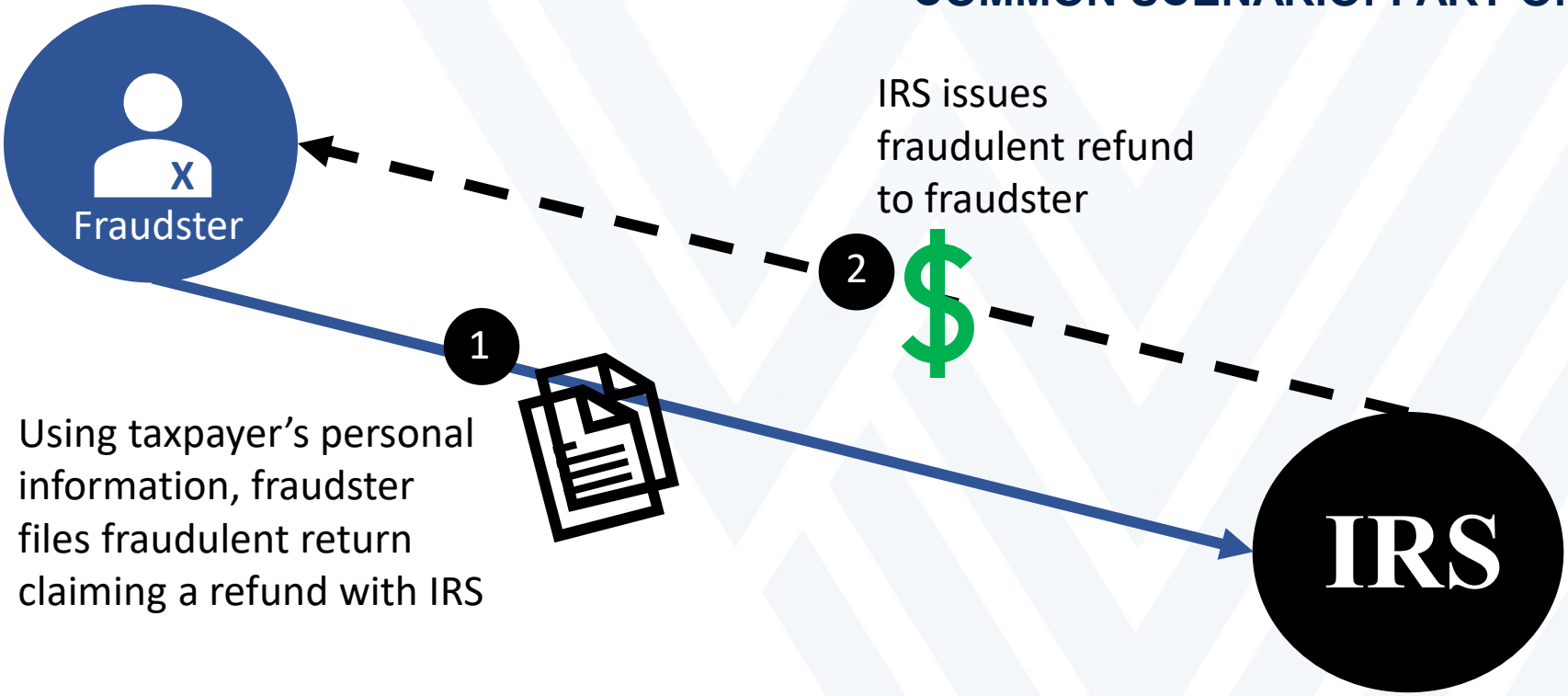
LEARN MORE AT WHITEHOUSE.GOV

# Tax-Related Identity Theft

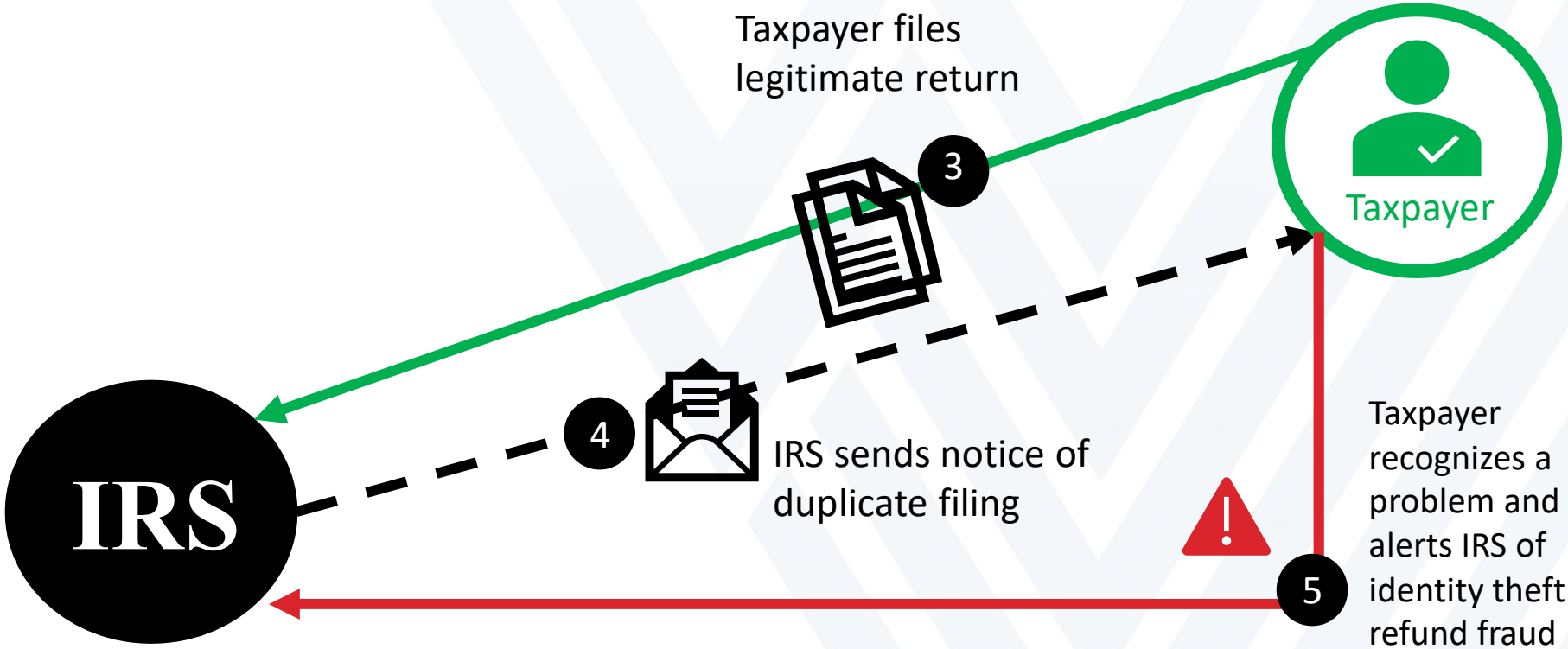
*Common Issues, What to Look For,*

*Protecting Clients and Professional Organizations*

# COMMON SCENARIO: PART ONE



# COMMON SCENARIO: PART TWO



# Security Summit

- Internal Revenue Service, state tax authorities, tax professionals
- Created in 2015
- Works in connection with the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC)

# Security Summit

- **The purpose is to protect the American taxpayer by combating identity theft tax refund fraud** through enhanced communication and information sharing between and among the parties involved in the electronic transmission and processing of federal and state income tax return filings;
- **maintain taxpayer trust** in the administration of the federal and state tax systems;
- **ensure confidence** in the integrity of the voluntary tax compliance system.


# ISAC

- **Purpose**: Facilitate information exchange for tax administration purposes related to identity theft tax refund fraud.
- **Provide a forum** for participants to discuss real-time responses to such fraud schemes.
- **Promote** the advancement of data analysis, capabilities, methodologies and strategies to detect, reduce, and prevent this type of fraud.

## Key Characteristics

- **Strategic planning**
- **Program development**
- **Monitoring and analysis**

## Focus and Structure

### Areas of Expertise:

- Identity theft strategy
- Revenue protection
- Updates to policy
- Schema development and analysis
- New data field creation
- NIST Security Standards
- Public facing or external stakeholder
- Process and policy implementation and analysis

### Security Summit Working Groups:

- Information Sharing
  - Rapid Response Team
- Financial Services
- Communications
- Tax Professionals
- Strategic Threat and Response (STAR)
- Authentication


## Key Characteristics

- **Issuance of IDT alerts**
- **Analysis of suspicious IDT activity**
- **Near real-time sharing**

## Focus and Structure

### Areas of Expertise:

- Threats to the tax ecosystem
- Sharing alerts with members
- Analysis of leads and shared information
- Internal stakeholder communications

### ISAC Senior Executive Board (SEB) and Committees:

- Executive Committee
- Community and Outreach Committee
  - Analysts Community of Practice Steering Committee
- Governance Committee
- Metrics Committee

# Protecting Your Clients

- **Federal law requires** you to create, implement and maintain an **information security plan** to protect client data, no matter the size of your firm.
- IRS recommends **Publication 4557, Safeguarding Taxpayer Data**, as a guide for reviewing current security measures and creating or updating security plans
- Use **multi-factor authentication** to login to online management products

# TIPS FOR PROFESSIONAL ORGANIZATIONS

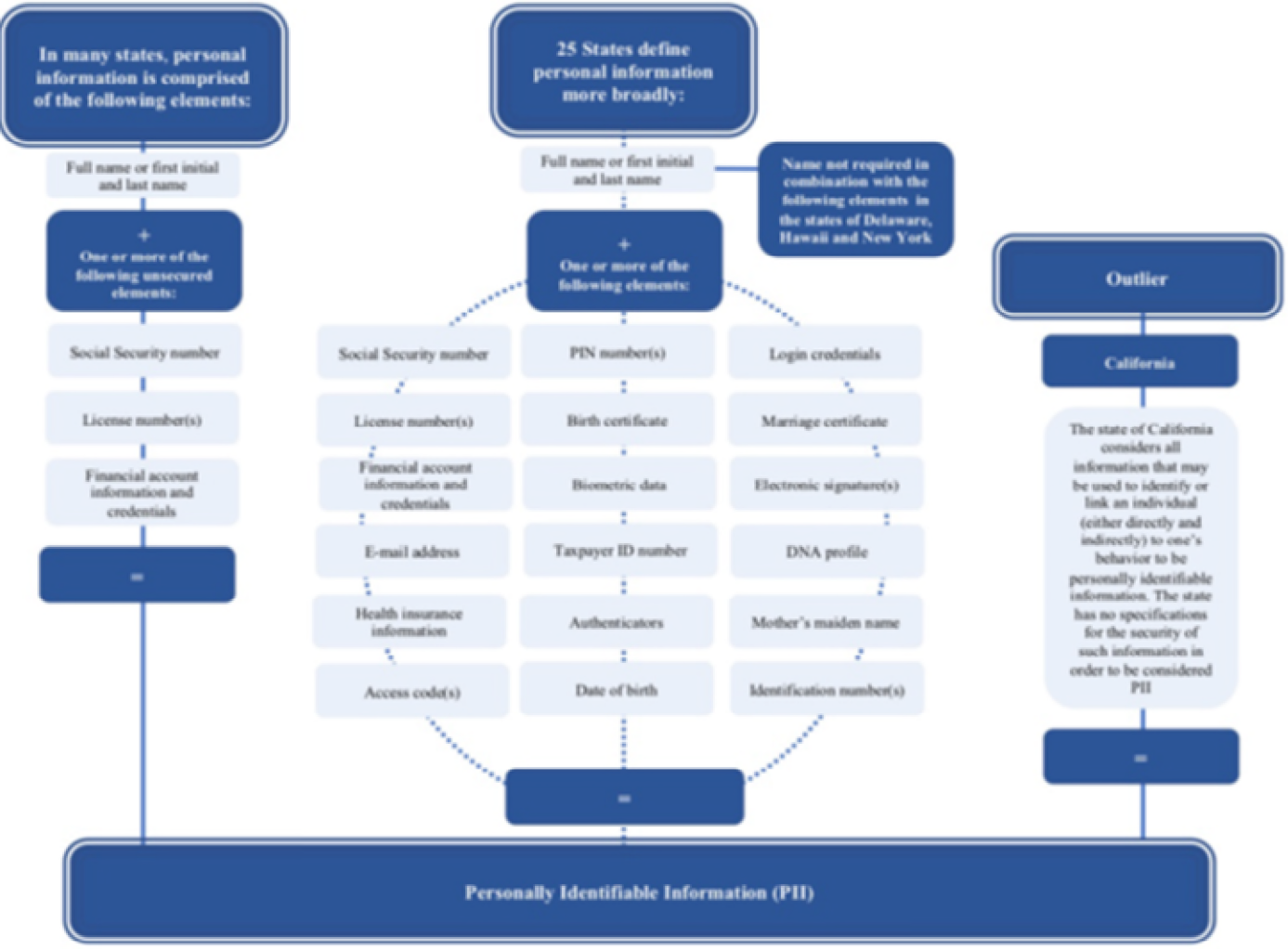
- **Collect** only needed information
- **Retain** only as long as necessary
- **Provide access** only to those with a legitimate business purpose
- **Implement** administrative, physical and electronic **security measures**
  - Multi-Factor Authentication
  - Cyber Insurance
- **Encrypt** data and other sensitive information
- **De-identification** of stored data

# Protecting Your Organization

- If you or your firm are the victim of data theft, immediately:
  - **Report it** to your local stakeholder liaison
  - **Liaisons will notify IRS Criminal Investigation and others**
- **Speed is critical**
  - If reported quickly, the **IRS can take steps to block fraudulent returns** in your clients' names and will assist you through the process.

# Protecting Your Organization

- **Email** the Federation of Tax Administrators at StateAlert@taxadmin.org
- Notify **Affected Person (always & Reporting Agencies (1000+)**
- **Contact Experts**




## West Virginia

Compared to the broader definitions of personally identifiable information (PII) held by 25 states, West Virginia defines PII considering a relatively narrow range of elements- an approach taken by many states. West Virginia regards PII to be a combination of an individual's name and one or more of the following unsecured elements:

- Social Security Number
- Driver's License Number or State Identification Number
- Financial Account Information and Credentials

Biometric Litigation:
(fingerprint, retinal scan, iris scan, face geometry, hand geometry, voice print, etc.)

*Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186*
Illinois Supreme Court

Fingerprint for amusement park pass (36M settlement)

*Cothron v. White Castle System, Inc.*, No. 20-3202,
(pending in 7CA)

White Castle required employee to submit her fingerprint to access computers and her paystub at work. Cothron alleges that White Castle did not receive BIPA-required consent to collect her fingerprints.

Other States:
Texas, Washington, California, Illinois, NY, Arkansas, several AG's.
(UDAP cases trigger nationwide settlement)

# Cyber Insurance

- Recent increase in claims related to **ransomware** and **extortion** attempts
- **56% of businesses last year** reported ransomware attacks
- **Average extortion payout** last year was **$1M**
- **Ransomware recovery cost for financial services is higher** than the global average ($2.10 million vs. $1.85 million)
- Look for **First- and Third-Party Coverage**
- **Underwriting Requirements** can include strengthening security systems in place

CCLE

The Center for Consumer Law and Education

a Marshall University & WVU College of Law Partnership

## Our Mission

The CCLE coordinates the development of consumer law, policy, and education research to support and serve consumers. Our unique partnership brings together scholars, practitioners, and students at the CCLE to empower, lead, and transform our communities.

## Our Vision

The Center for Consumer Law and Education (CCLE) at Marshall University and WVU College of Law strives to be the leading research and educative consumer rights and development Center in the nation.

# THANK YOU

# Questions?


Jonathan Marshall, Director of CCLE

JMarshall@mail.wvu.edu