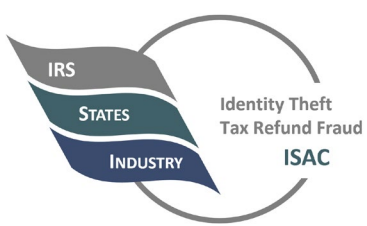


National Association of State Treasurers

Identity Theft Tax Refund Fraud – Information Sharing and Analysis Center (IDTTRF-ISAC) Partnership

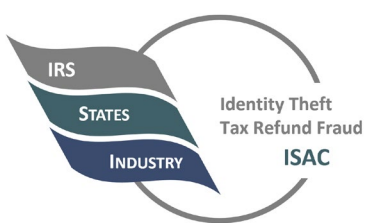
November 7, 2019



Speakers

Lynne Riley – Georgia State Treasurer

Sharonne Bonardi - Deputy Comptroller at
Comptroller of Maryland and President, Federation
of Tax Administrators Board of Trustees



The Identity Theft Threat to Our Nation's Tax System

Over 150 million households file federal and state tax returns each year, amounting to trillions of dollars flowing through the tax ecosystem.



Criminals target the highly sensitive personal information in these returns, threatening the integrity of the nation's tax system.



Nearly 15 billion data records have been lost or stolen since 2013.* Thieves often use the dark web or initiate pay-offs to secure personal data, including stolen Social Security numbers.

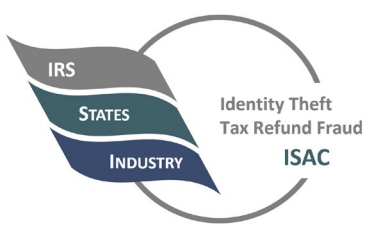
*<https://breachlevelindex.com/>

Looking at the Problem Holistically

Recognizing that the IRS could not fix identity theft tax refund fraud alone, IRS convened the first public-private sector Security Summit in March 2015 to identify cooperative and collaborative steps to protect taxpayers and the integrity of the federal and state tax systems. One of the Summit’s many initiatives was the recommendation to establish the Identity Theft Tax Refund Fraud - Information Sharing and Analysis Center (IDTTRF-ISAC) – an ideal venue for a public/private partnership to resolve the challenges of sharing critical data among stakeholders.

- ISACs facilitate the sharing of information between two or more parties when it would not necessarily happen otherwise.
- ISACs are designed to motivate the private sector to share information with the public sector without fear that the information will be used against them.
- Some ISACs also provide limited liability protection for private sector organizations who share information.





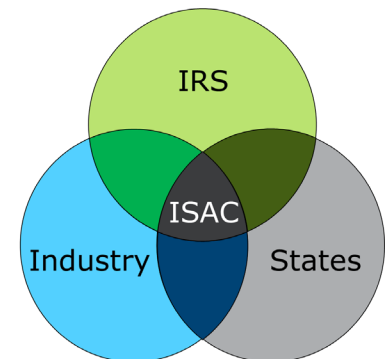
IDTTRF-ISAC – Mission & Vision

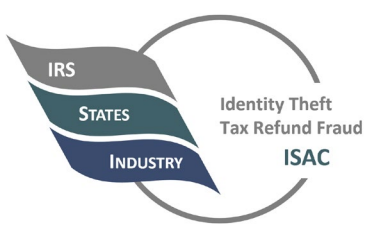
Mission

The mission of the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center is to provide a secure platform via a sustainable public/private partnership, to facilitate information sharing consistent with applicable law, and analytics necessary to detect, prevent, and deter activities related to stolen identity refund fraud.

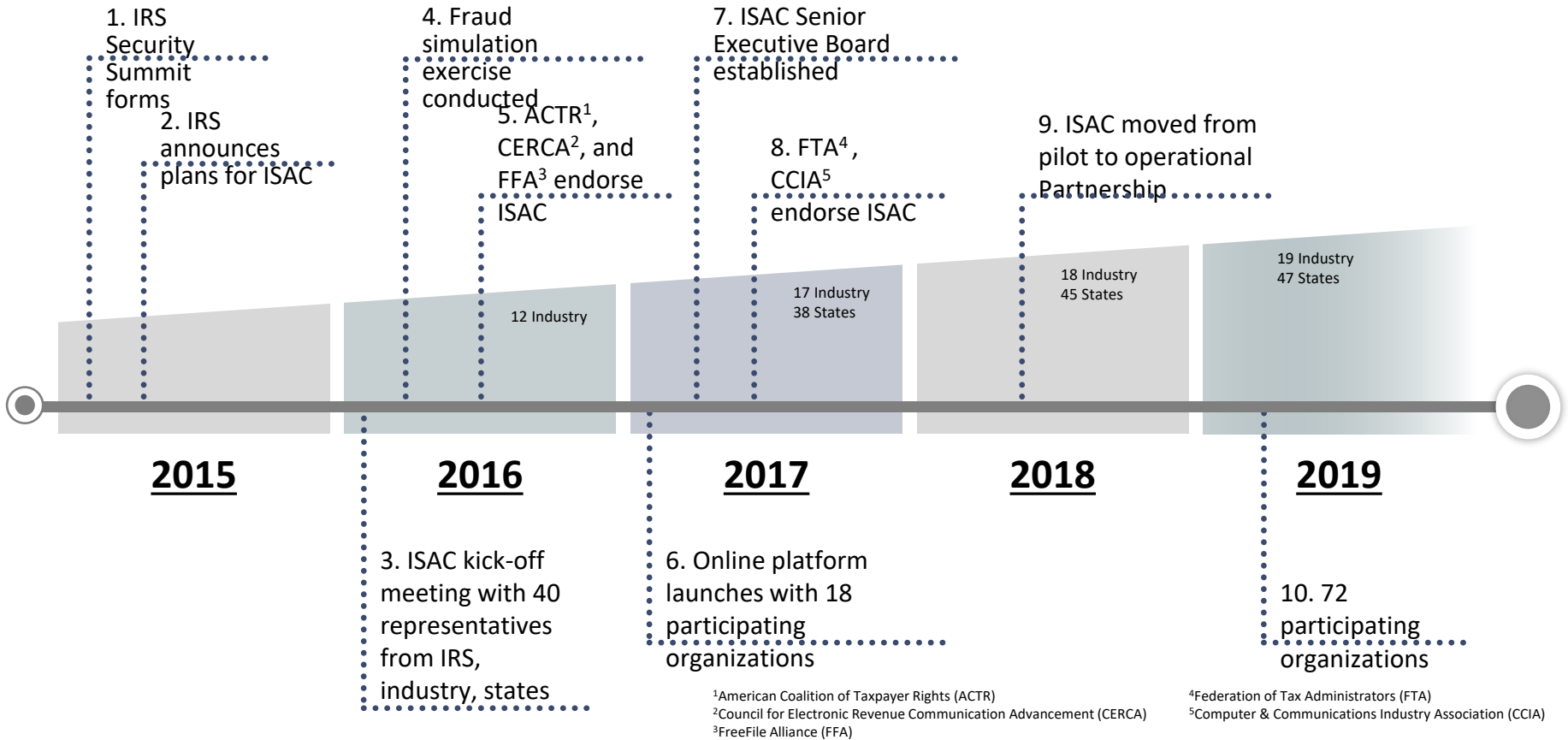
Vision

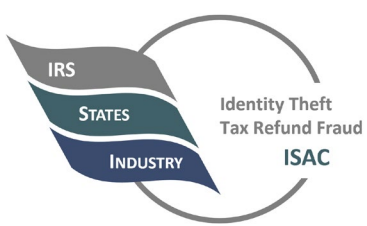
Our vision, as a public/private partnership, is a tax ecosystem where taxpayers can confidently file their taxes safely and securely.





ISAC Timeline

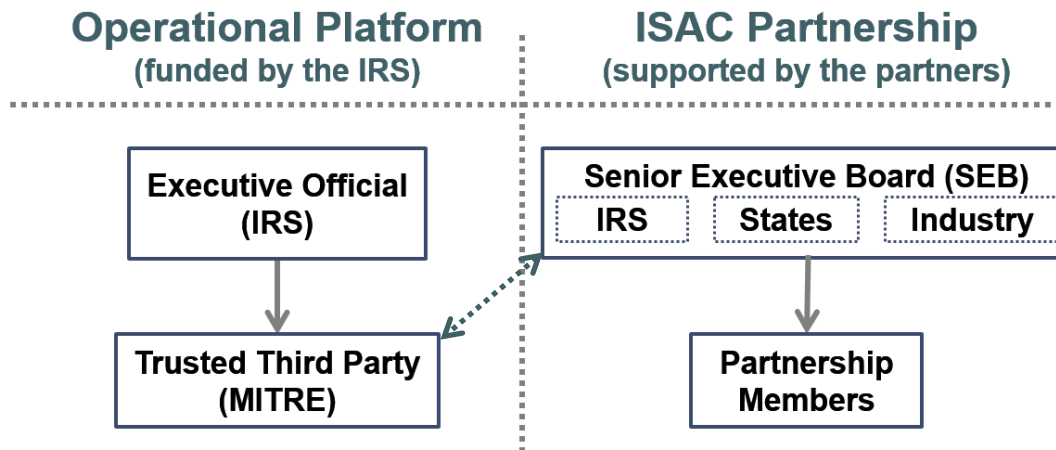




How the IDTTRF-ISAC Works

The IDTTRF-ISAC consists of two parts that operate independently:

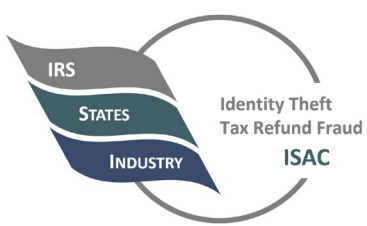
- The **ISAC Operational Platform**, managed by the IRS and operated by MITRE, the Trusted Third Party (TTP), provides the technological mechanism for the ISAC partnership to share information and obtain analysis. The TTP serves as the connecting point between the Operational Platform and the Partnership.
- The **ISAC Partnership** is managed by the Senior Executive Board which consists of equal representation (five members each) from across IRS, States, and the tax industry.



While the technology and analytical services for the ISAC are provided by the Trusted Third Party (TTP) and sponsored by the IRS, the Partnership is independent.

The purpose of the Partnership is to be a vehicle for collaboration among the members of the tax ecosystem to improve our collective ability to prevent identity theft tax refund fraud at the federal, state and local levels.

The role of the TTP is to leverage the collaborative efforts of all ISAC partners to protect taxpayers from identity theft tax refund fraud.



What the ISAC Offers

Post, read and respond to **alerts** – reports of any tax ecosystem threats – in near-real-time within the ISAC's secure* environment.

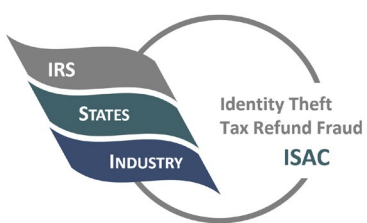
This is like a neighborhood listserv for the tax ecosystem, with immediate reports of breaches, compromised identification numbers, or other suspect data.

Share knowledge, best practices and concerns related to the detection and prevention of IDTTRF through the **Analysts' Community of Practice (ACoP)**.

The ACoP is an active forum of analysts who meet to share techniques and findings in a trusted environment.

Receive **analytics** daily that are tailored to the partner's organization, delivered in digestible formats and easily viewed through visualization tools.

The ISAC conducts analytics on numerous datasets looking for suspicious activity. One dataset is **industry leads** – reports of IDTTRF patterns, suspicious activity, and suspected fraud – which the ISAC aggregates and anonymizes. Dashboard metrics are updated on a live basis as data flows into the ISAC.



Measuring Success

From the proof of concept in 2016 to today as an operational platform, the ISAC’s key accomplishments are highlighted across three measures:

- Levels of industry and state participation in the ISAC
- Volume and quality of alert and data contributions that identify ecosystem threats
- Volume and quality of ISAC’s data analysis to identify suspected fraud

>400% increase in membership since January 2017

A Total of 72 Participating Organizations with 457 Users

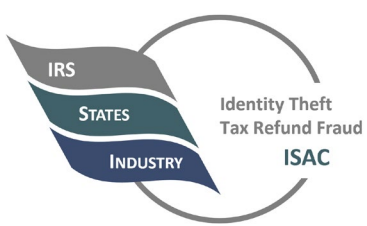
Organizations	Users
47 States*	269
15 Industry	71
4 Financial Institutions	17
5 Endorsing Organizations	10
IRS	90

*31 States have joined as full participants – sharing and receiving alerts as well as sharing and receiving data and analytics
 15 States have joined the Collaboration Site – sharing and receiving alerts.

	2019 Jan Sep	2018 All	2017 All
Alerts Posted	167	145	71
Industry Leads Submitted	1.1M	1.5M	2M

During the 2019 filing season, partner organizations accessed datasets analyzed by the ISAC more than 1200 times.

Of the 167 alerts posted in 2019, 70 alerts were related to previously identified alerts/schemes.



How Members Use the ISAC

1. Obtaining analyzed leads and alerts

Members download analytics including aggregated data (leads, alerts and other sources). They are notified immediately when an ISAC partner posts an alert on the portal reporting known or suspicious fraudulent activity.

“It was gratifying to get a lot of responses to a posted alert. It just always makes you feel good that you’ve contributed.”

“We’ve been able to set more flags based on what we’ve learned. We usually haven’t looked at zero refund returns, but learned from other states these could be compromised, with the fraudster setting up accounts so they could come back later asking for large refunds.”

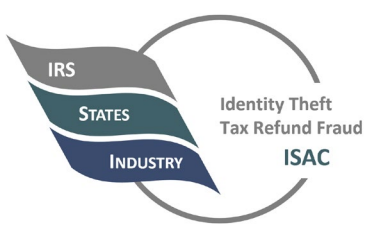
2. Validating fraud detection filters

Members compare leads data to their own to see if their filters are catching the same issues and whether refinements are needed.

“Its unique value is allowing us to engage with other states and industry and see what they’re doing. We can share common points of view as well as differing ones, which helps us think outside the box of what we’re currently doing.”

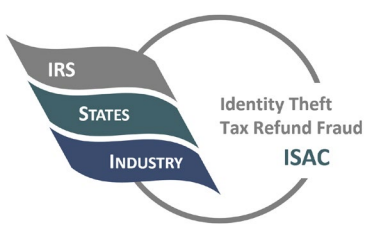
3. Collaborating and sharing information

Members view the ISAC as an opportunity to expand their network while sharing knowledge and best practices in a trusted environment.



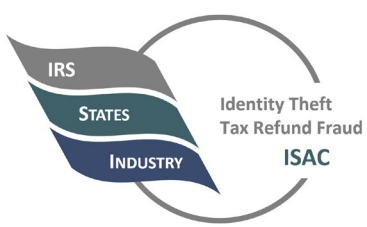
What makes us unique

- We are a Public-Private Partnership with government membership
- We have sensitive data sharing agreements
- We curate our data into consumable formats
- We are fighting fraud/sharing at the entity level
- Inherently governmental activities are owned by some members
- We work at multiple levels within our partner organizations



Looking Ahead

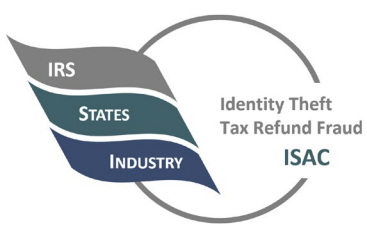
- **Grow breadth and depth of membership and participation**
The ISAC will continue to grow member participation from private sector and other government agencies and provide opportunities to deepen members' participation with clear guidelines and an easy-to-use system.
- **Build member capabilities and deepen engagement**
The ISAC will develop more opportunities through the Analysts' Community of Practice to teach fraud analysts new methods of fighting fraud and how to improve their own analysis.
- **Improve technical capabilities**
The ISAC will continue building analytical capabilities within the ISAC portal, improve ease of use, and create a full circle of feedback for members.
- **Partner with other entities that identify ecosystem threats**
The ISAC will investigate new opportunities for partnership and build engagement with other threat-monitoring organizations to deepen threat intelligence.
- **Improve threat identification and sharing**
Legal and regulatory developments may increase the ISAC's capability to seamlessly share aggregated information.



Secretary of State & Department of Revenue – Business Identity Theft

A group of state revenue departments and Secretary of State (SOS) agencies are working together with the ISAC Trusted Third Party to determine if there is value in an ongoing exchange of information to help detect and prevent business identity theft. The goals of the pilot include:

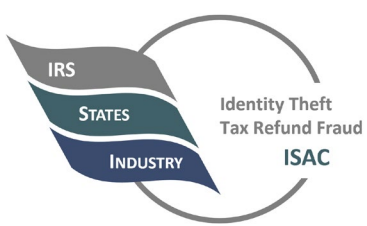
- Identifying data elements that may be valuable to exchange for the detection and prevention of identity theft.
- Conducting analysis on those data elements to determine if they provide value and assist with the detection and prevention of identity theft.
- Develop procedures for an ongoing exchange of data if the pilot outcome results in a determination to expand and continue a partnership.



Deposit Verification (Pre-verification)

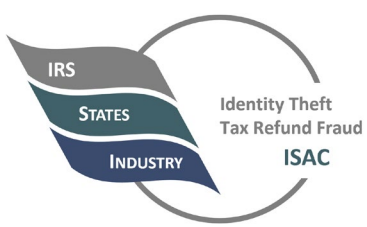
This collaboration between industry, states, and the IRS allows participants to pre-verify deposit eligibility in real time prior to sending the refund through the ACH system. Deposit eligibility is a direct deposit pre-verification and account scoring service.

In this pilot, the ISAC serves as the hub for the shared pre-verification data. In addition to the data going from point to point, it will be analyzed and shared in aggregate with authorized partners.



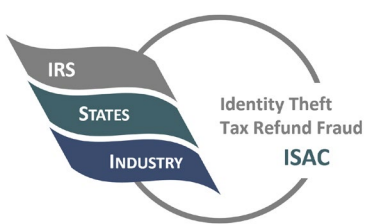
Breach Data

- FTA is partnering with the ISAC on the process of secure data transfer and storage of breach data from business or tax professionals.
- When a business or tax professional has been the victim of some type of data breach, they are directed by IRS.gov to report this information to the state revenue agencies through the Federation of Tax Administrators (FTA).
- By using the ISAC's secure file transfer process states are able to access breach data securely and quickly. In addition, the ISAC analytics team will include the de-identified, aggregated breach data in its analysis and reports for State ISAC users, as appropriate.



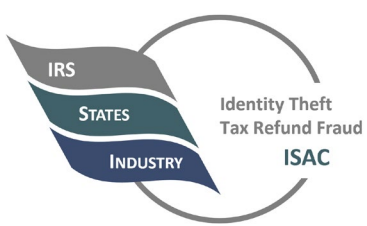
Unclaimed Property Risks

- Data breaches provide criminals with identity information that will allow them to search state unclaimed property websites and submit claim requests to state treasury departments.
- Victims of Individual or Business Identity Theft are likely targets of unclaimed property impersonation.
- State Treasurers are encouraged to consider opportunities to protect their citizens from fraudulent property claims.
- The ISAC Senior Executive Board welcomes State Treasurers to express their interest in exploring the value of an information sharing relationship similar to the Secretary of States pilot project.



Questions?





Contact Information

Lynne Riley - lynne.riley@treasury.ga.gov

Sharonne Bonardi - sbonardi@comp.state.md.us

Andy Dziewulski – IDTTRF@mitre.org