Electronic Tax Administration Advisory Committee

ANNUAL REPORT TO CONGRESS

June 2019

Publication 3415 (Rev. 6-2019) Catalog Number 28110R Department of the Treasury **Internal Revenue Service** www.irs.gov

ELECTRONIC TAX ADMINISTRATION ADVISORY COMMITTEE

MEMBERS

John Ams

Shannon Bond

John Breyault

Luanne Brown

Angela Camp

John Craig

Jenine Hallings

Michael Jackman

Courtney Kay-Decker

Suzanne Kruger

Kathy Pickering

Phillip Poirier, Jr. (Vice Chair)

Lynnette T. Riley

Gene Salo

John Sapp

Joseph Sica

Mark Steber

Doreen Warren (Chair)

ETAAC member biographies can be found in Appendix B

LETTER FROM THE CHAIR AND VICE CHAIR

The Electronic Tax Administration Advisory Committee (ETAAC) is pleased to deliver its 2019 Annual Report to Congress.

Since the expansion of its Charter in 2016, ETAAC's primary focus continues to be on protecting taxpayers and enhancing their experience. Our 2019 report provides recommendations to identify and prevent Identity Theft Tax Refund Fraud (IDTTRF) and protect and help taxpayers by involving and increasing the awareness of affected stakeholders in our tax system, improving the taxpayer interactions with the IRS and increasing the security of our electronic tax infrastructure.

ETAAC would like to emphasize several key points at the outset of this Report.

1. The Security Summit, under the IRS's leadership, continues to make progress in the fight against IDTTRF. Sustaining the Security Summit's ability to detect and prevent IDTTRF will require continued engagement with existing and new partners from both government (federal, state and local) and industry.
2. Congressional funding and support for the Security Summit and ISAC[1] remain a key enabler to the ongoing success of these initiatives.
3. The IDTTRF threat will be a challenge for some time to come. In fact, nation-states and cybercriminals are becoming more sophisticated and will continue to make it difficult to detect and stop their criminal activities, which will directly impact legitimate taxpayers trying to meet their tax filing obligations.
4. The implementation of new tax laws, such as the Tax Cut and Jobs Act, requires IRS resources both to implement the substantive elements of any new law and also to analyze and prepare for potential new IDTTRF opportunities created by the new law.
5. The commitment and professionalism of the IRS leadership and staff during the government shutdown was exemplary. Notwithstanding the disruption, the IRS prepared and executed contingency plans that minimized the impact of the shutdown on its operations including its efforts to stop IDTTRF.

Our report is organized to provide the reader with the opportunity to review key insights at a glance or to go deeper into the supporting details.

- For a high-level overview, read the Executive Summary following this Letter and the Summary List of ETAAC 2019 Recommendations.
- To understand the details underlying our 2019 recommendations, review the Current Environment for IDTTRF & Cybersecurity and Detailed Support for ETAAC 2019 Recommendations sections. (Page numbers for each area and recommendations are listed in the Table of Contents).

[1] "ISAC" refers to the IDTTRF Information Sharing and Analysis Center, which is further described in the About the Security Summit section of this report.

The eighteen-member ETAAC team spends thousands of volunteer hours to research and consider its recommendations. Our intention is to recognize the remarkable progress of the Security Summit collaborative effort under the IRS's leadership and with the significant support and commitment of states and industry, and to identify potential opportunities to build on its success.

We appreciate the support and interest that Congress has expressed in our work.

Likewise, we appreciate the support of the IRS's employees and leadership, including their responses to our numerous requests and questions. We want to recognize their continued commitment to the Security Summit and the American taxpayer. Through the Security Summit, the IRS has brought together disparate stakeholders to protect the integrity of our tax system. The Security Summit is no small achievement and is a living demonstration of the effectiveness and benefits of taking on common challenges with a collaborative and unified approach.

Finally, the ETAAC Chair has been involved in the Security Summit from its very beginning as a state representative. Over the past several years, she has seen firsthand the steady increase in collaboration, trust and respect of the government and private sector participants involved in this monumental endeavor. She is proud to recognize the solid foundation built by the Security Summit, and believes that the effort to prevent IDTTRF and protect taxpayers will continue to bear fruit so long as all stakeholders continue to collaborate and stay focused on the common objective of maintaining the integrity of our tax system.

Respectfully submitted,

Doreen Warren	Phillip L. Poirier, Jr.
ETAAC Chair	ETAAC Vice Chair

EXECUTIVE SUMMARY

Identity Theft Tax Refund Fraud and Information Security is our primary focus

This report is the third since the ETAAC's charter was extended to include an evaluation of the Security Summit initiative and the prevention of IDTTRF.

The ETAAC 2017 and 2018 Annual Reports to Congress included 22 and 19 recommendations, respectively, concerning IDTTRF and the Security Summit's activities.

For 2019, ETAAC made a conscious decision to narrow its focus to a smaller number of critical recommendations. After considering over 25 potential topics, we arrived at ten recommendations falling under three themes:

- Strengthening the Security Summit and ISAC
- Improving Security
- Protecting and Enabling Taxpayers

Our report also includes an update on the IRS's efforts to increase electronic filing.

The Security Summit continues to make progress against these ongoing risks

IDTTRF threatens the integrity of our voluntary compliance tax system at both the federal and state levels. The wholesale theft of huge volumes of personal information has provided criminals and other bad actors with detailed and accurate taxpayer information. Our sophisticated adversaries can use this information to create and file returns that look almost identical to those of the legitimate taxpayer. Unfortunately, there is no silver bullet that makes it easy for the IRS to spot these fraudulent returns among the hundreds of millions of legitimate returns.

This is a critical time. To protect our tax system, the Security Summit and ISAC must continue to drive progress with a unified and collaborative approach among all of the stakeholders.[2] Fortunately, the IRS, states and private industry have made substantial funding and personnel commitments to the Security Summit and ISAC. Ongoing funding and investment in programs, technology and staff will be critical to the continued maturation, evolution and success of the Security Summit and ISAC.

Focus of ETAAC's 2019 Recommendations

ETAAC's 2019 recommendations fall under three broad themes:

1. Strengthen the Security Summit and ISAC by:
    - Funding the ISAC
    - Enacting an IDTTRF exception to IRC Section 6103
    - Increasing the engagement of ISAC members
    - Integrating the Payroll Community more fully into the Security Summit

[2] The About the IRS Security Summit section of this Report reviews the key accomplishment and current focus/priorities of the Security Summit and ISAC.

- Piloting a Financial Services Company (FSC) Collaboration Space in the ISAC

2. Improve the security in key areas of our tax system by:
   - Assessing the state of information security in the tax professional community
   - Granting the IRS the authority to establish and enforce security standards
3. Protect & enable taxpayers by:
   - Developing and expanding channels for identity proofing
   - Collaborating with Security Summit members to identify and pilot emerging approaches for identity verification
   - Engaging with the Security Summit to improve the IRS Taxpayer Protection Program's taxpayer experience

Congressional support is needed in some key appropriation and policy areas

The ETAAC 2019 Report calls for Congress to take appropriations or policy actions in several key areas to enable the IRS to fight IDTTRF and increase information security.

First, from an appropriations perspective, ETAAC recommends that Congress provide sufficient funding for the IRS to staff and execute IRS, Security Summit and ISAC priorities identified in this report. This request includes our recommendation to fund the ISAC. (See Recommendation #1)

Second, from a policy perspective, ETAAC recommends that Congress take legislative action in two key areas:

- Information Sharing. Congress should create a carefully targeted exception under Internal Revenue Code (IRC) Section 6103 to permit the use and disclosure of federal tax information to enable more effective information sharing to identify and prevent IDTTRF. (See Recommendation #2)
- Security Standards. Congress should grant the IRS the authority to establish and enforce security standards for our tax system. (See Recommendation #7)

Closing Thoughts

Clear IRS ownership and accountability for information security

The IRS continues to demonstrate its commitment to improve information security across our tax system and to fight IDTTRF. The success of these efforts requires effective and efficient management based on clear internal ownership and accountability within the IRS.

In the area of information security, the IRS can continue to improve its effectiveness in developing and updating security requirements and providing consistent, clear, concise and actionable guidance to and education for tax professionals and e-file program participants.

As noted in previous recommendations,[3] ETAAC believes that the IRS must have clearer internal ownership and accountability for establishing or enforcing existing or new security standards and programs. This issue is equally present in the IRS's broader management and execution of Security Summit and ISAC initiatives that cross multiple internal IRS businesses, divisions and functions such as the integration of the payroll community into the Security Summit as further described in this Report.

Stakeholder engagement and IRS leadership

The Security Summit's unified and collaborative approach to detect and prevent IDTTRF necessarily involves our entire voluntary compliance tax system.

The success of this approach hinges on fostering a very high-level of engagement with all Security Summit stakeholders. As shared by former Commissioner Koskinen, high engagement in the Security Summit is contingent on the initiative providing value to its members.

The IRS plays the non-delegable leadership role in driving stakeholder engagement and ensuring that value is being delivered. ETAAC is encouraged by Commissioner Rettig's priority to protect taxpayers and the tax system and his recognition that the Security Summit is a terrific example of what the public and private sectors can accomplish when they work together. We look forward to working with Commissioner Rettig and the IRS team in future years.

[3] See ETAAC commentary on its 2018 Recommendation #10 in the Progress on ETAAC 2018 & 2017 Recommendations section of this report.

TABLE OF CONTENTS

PROGRESS TOWARD 80% E-FILE GOAL

Measuring Progress Towards The 80% Electronic Filing Goal

Section 2001(a) of the IRS Restructuring and Reform Act of 1998 (RRA 98)[4] provided that "It is the policy of Congress that -- paperless filing should be the preferred and most convenient means of filing Federal tax and information returns; it should be the goal of the Internal Revenue Service to have at least 80 percent of all such returns filed electronically by the year 2007; and the Internal Revenue Service should cooperate with and encourage the private sector by encouraging competition to increase electronic filing of such returns." Section 2001(b)(2) of the RRA 98 authorized the creation of the ETAAC, whose charter provides that it will research, analyze, consider and make recommendations on the IRS's progress toward achieving its 80% e-file goal.

The IRS interpreted the RRA 98's 80% goal to apply to "major returns,"[5] and ETAAC has generally followed this approach in reviewing the IRS's progress towards the 80% goal for the purposes of the ETAAC's Annual Reports to Congress.[6] (Also see Appendix C)

IRS estimates it has achieved the 80% electronic filing goal for major returns

IRS undertook a collaborative public/private partnership with states and the private sector to achieve its 80% electronic filing goal. This is a momentous achievement not just for this partnership, but also for the American taxpayer because of the increased convenience and speed of refund delivery associated with electronic filing and direct deposit.

Table 1: 2016-2019 Electronic Filing Rate for Major Returns

	2016 (IRS Actual)	**2017 (IRS Actual)**	**2018 (IRS estimated)[7]**	**2019 (IRS projected)**
Electronic Filing Rate	79.2%	80.1%	81.1%	82.1%

Source: IRS Publication 6186 (2017 and 2018 Updates). Also see Appendix C.

Overall e-file rates continue to grow, but more slowly

As shown in Table 2 below, the IRS estimates that individual returns have the highest e-file rate and represent 76% of major returns filed. The relatively low growth rate of individual e-file can be expected as individual return e-file matures.

[4] Pub. L.105–206, 112 Stat. 685, enacted July 22, 1998

[5] Pursuant to its definition of "e-File Rate" in the IRS Strategic Plan 2009-2013 (Pub. 3744, 4-2009), the IRS reported that it would "measure the percentage of all major tax returns filed electronically by individuals, businesses and tax-exempt entities" and that "'Major' tax returns are those in which filers account for income, expenses and/or tax liabilities." IRS has not redefined the term major returns in either of its two subsequent Strategic Plans, i.e., for 2014-2017 or for 2018–2022.

[6] See ETAAC Annual Report to Congress, June 2011, p. 2, Footnote 1.

[7] See IRS Publication 6186 (2018 Update), pps. (1) – (3) for the IRS's explanation of its estimate and projection methodologies.

E-file rates continue to increase for other major return types. It is mildly encouraging that the employment tax return segment[8] continues to increase, albeit the overall rate of e-file for Employment returns remains low.

Table 2: 2018 Projected Electronic Filing Rates

	2018 IRS Estimated			2019 IRS Projected			
	Total	**E-filed**	**E-file Rate**	**Total**	**E-filed**	**E-file Rate**	**Year-over-Year Change**
Individual (Forms 1040, 1040-A, and 1040-EZ)	151,663,800	134,149,000	88.5%	152,911,800	136,184,900	89.1%	.6%
Employment (Form 94X Series)	30,916,100	13,775,500	44.6%	31,033,500	14,601,600	47.1%	2.50%
Corp Income Tax (1120,1120-A,1120-S), etc.	7,170,600	5,808,700	81.0%	7,235,200	5,962,200	82.4%	1.4%
Partnership (Forms 1065/1065-B)	4,135,300	3,610,500	87.3%	4,227,300	3,743,900	88.6%	1.30%
Fiduciary (Form 1041)	3,106,500	2,618,800	84.3%	3,099,800	2,653,600	85.7%	1.40%
Exempt Orgs (Forms 990, 990-EZ, etc.)	1,617,100	1,094,400	67.7%	1,662,100	1,152,700	69.4%	1.70%
Totals	198,609,400	161,056,900	**81.1%**	200,169,700	164,298,900	**82.1%**	1.00%

Source: See Table 2, IRS Publication 6186 (2018 Update)

The 2019 electronic filing rate for individual returns should hit approximately 89%

As of April 19, 2019, the e-file rate for individual returns during the initial part of the 2019 Filing Season increased by 1.07% from the prior year comparable period.[9]

As in the past, ETAAC has a methodology to estimate the current year individual return e-file rate based on the above season-to-date filing information adjusted for changes in historical e-file patterns between May and October (See Appendix C). Based on its methodology, ETAAC estimates that individual returns should achieve an e-file rate of 89% for the 2019 filing season, which is consistent with the IRS's 2019 projection in Publication 6186.

[8] As used in this report, "Form 94X" refers generally to the major employment returns, e.g., Form 940 Employer's Annual Federal Unemployment (FUTA) Tax Return, Form 941 Employer's Quarterly Federal Tax Return, etc.

[9] See https://www.irs.gov/newsroom/filing-season-statistics-for-week-ending-april-19-2019.

Nevertheless, the measures for e-file rates have gaps and the e-file of some return types can be improved

ETAAC has two observations: (i) some return types cannot be e-filed and/or are not included in the IRS's definition of major returns for purposes of measuring its achievement of the 80% rate, and (ii) employment return e-file remains too low. (ETAAC has commented further on both of these issues in the Progress on ETAAC 2018 and 2017 Recommendations section of this report.)

Some returns with sizeable volumes are not being tracked as part of the 80% goal

Certain return types currently cannot be e-filed, most importantly the Amended U.S. Individual Income Tax Return (Form 1040X).

IRS estimates there will be approximately 3.9 million Form 1040Xs filed in 2018 – all on paper. If Form 1040X returns were included in the definition of "major returns," the IRS's overall e-file rate would drop below 80%.

The IRS's Modernized E-File System (MeF) could and should be modified to enable electronic filing of Form 1040X, which would have a positive effect on taxpayers over time by enabling them to file amended returns with the IRS and, through MeF, with states. This would be a much more seamless solution for taxpayers than having to prepare and file amended returns separately for federal and state taxes. ETAAC recommended that the IRS enable electronic filing of Form 1040X through MeF in its 2017 Annual Report to Congress, and again reaffirms its support for this recommendation.

There are other returns with increasingly high volumes that are not included in the IRS's definition of major returns. For example, the Form 4868 Application for Automatic Extension of Time To File U.S. Income Tax Return accounts for approximately 14 million returns in 2018. If both the Form 1040X and Form 4868 were included in the definition of major returns, ETAAC estimates the overall e-file rate would decrease by approximately 2% from 81.1% to 79.1%, which is below the Congressionally established 80% target.

Employment return e-file rates remain too low

Although the e-file rate has increased year-over-year, employment return e-file rates continue to be approximately one-half of the e-file rate of most other major returns. ETAAC has commented on this area for several years, most recently in our 2018 Annual Report to Congress. ETAAC continues to believe there are opportunities to increase the e-file rate in this area.

Caveat: There are Unknown Impacts from Tax Reform on Filing Volume

The IRS has indicated in Publication 6186 that the legislative changes in the Tax Cut and Jobs Act enacted on December 22, 2017 are expected to impact the future tax return volume for many of the individual and business form types. For example, IRS estimates that the changes to the estate tax exclusion will impact e-file rates. However, no further indication is provided in Publication 6186 in regards to this expectation.

CURRENT ENVIRONMENT FOR IDTTRF AND CYBERSECURITY

The tax administration system is comprised of a variety of stakeholders

Every year, the IRS receives almost 200 million tax returns, including approximately 150 million individual income tax returns, 15 million business income tax returns, 30 million employment tax returns and a variety of other return types.

The stakeholder communities involved in these tax systems are as varied as the U.S. population and its economy. The stakeholder communities include and are not limited to:

- Taxpayers: Taxpayers may be individuals, sole proprietors, small business employers or large multinational corporations. They may self-prepare or outsource the preparation and filing of their returns.
- Tax preparation service providers: Tax preparation service providers may engage in any or all of the tax systems – individual income, business income and employment taxes – and vary in size from a solo practitioner to a very large firm with thousands of preparers. In addition, other businesses specialize in specific tax or payroll segments such as payroll service providers and reporting agents.
- Technology stakeholders: Technology stakeholders enable these preparers, including software developers, transmitters and hosting or cloud computing service providers.
- Financial institutions: Financial institutions and other financial service companies enable the payment of taxes and receipt of refunds through the products and services they provide

The size, sophistication, capacity and resources of these stakeholders vary significantly, which present associated risks and challenges.

The IRS has an imperative to develop secure services

Taxpayers engage with the IRS across multiple service delivery channels[10] to meet a variety of needs, including obtaining forms and publications, answering tax questions, requesting the status of tax payments or refunds, obtaining transcripts or understanding IRS letters or notices.[11] They expect (and need) access to the IRS and their tax information in service channels that are accessible, convenient and meet their service preferences. The IRS must ensure that each of its service delivery channels is secure and that sensitive interactions occur only after successful identity verification.[12]

Increasingly, the IRS is expected to deliver on-demand online and mobile services (electronic services) to supplement traditional service channels. Taxpayers expect them – they are available to consumers and businesses from their other financial services

[10] The IRS's primary service channels are telephone, in-person, digital and correspondence.

[11] See National Taxpayer Advocate 2017 Annual Report to Congress, Most Serious Problem #2, p. 27.

[12] See GAO Report "IDENTITY THEFT: IRS Needs to Strengthen Taxpayer Authentication Efforts" (GAO-18-418, June 2018) (GAO Authentication Report).

providers. These electronic services offer convenient 24/7 access, help the IRS reduce its operating costs and, as with its other service delivery channels, must be secure.

Our electronic infrastructure is under attack…stolen information fuels IDTTRF

The United States faces significant cyber threats. The Federal Bureau of Investigation (FBI) reports that it received over 1.4 million cybercrime complaints totaling over $5 billion between 2013 and 2017.[13] A significant portion of these thefts originate through compromises of something as common as business email.[14]

There are well-publicized examples of large scale system breaches or compromises of sensitive personal, family, business, financial and medical information from a variety of government and private sources, including (#'s are approximate):[15]

- 2012: Office of Personnel Management (22 million background investigations)
- 2013: Yahoo! (3 billion email accounts)
- 2014: eBay (145 million merchant accounts)
- 2015: Anthem (80 million health insurance accounts)
- 2017: Equifax (145 million credit reporting accounts)
- 2018: Marriott (500 million lodging accounts)

Stolen information, coupled with other publicly available information (such as social media), can be used to construct and file fraudulent tax returns that mimic legitimate taxpayer returns in nearly every way. Stolen information can also be used in one tax system to facilitate IDTTRF in another tax system, for example, stolen payroll information (e.g., wages, federal withholding and state withholding) can be used to enable IDTTRF on individual income tax returns. Stolen information can also be used to compromise identity verification systems designed to secure electronic services, or to access sensitive information or take other fraudulent actions in other service channels that may have less effective identity verification protocols.

The parties conducting these compromises are nation-states and cybercriminals. They are sophisticated, well-funded, persistent and patient.[16] In response to efforts to protect our tax system, these criminals adjust their tactics to pursue other system and stakeholder vulnerabilities. Their targets are both large and small enterprises, including

[13] See FBI 2017 Internet Crime Report, p.4. (See https://pdf.ic3.gov/2017_IC3Report.pdf).

[14] See https://www.fbi.gov/news/stories/2017-internet-crime-report-released-050718

[15] See https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

[16] See FireEye M-Trends 2019 Report (See https://content.fireeye.com/m-trends).

the hundreds of thousands of tax professionals serving taxpayers[17] as well as service providers in the business, payroll and employment tax areas.[18]

The Government Accountability Office (GAO) and Treasury Inspector General for Tax Administration (TIGTA) have identified IDTTRF and cybersecurity as among the top risks and management challenges facing the federal government and the IRS.[19] The IDTTRF fight will never end.

The IRS has responded to this threat in a variety of ways

The IRS has developed a comprehensive, multi-faceted IDTTRF strategy.

Part of this strategy includes investing in improved IDTTRF detection systems.[20] For example, the IRS's current IDTTRF detection protocols use a sophisticated risk scoring system that relies on identity theft (IDT) models and various IDT fraud indicators (sometimes called fraud filters) to identify suspicious returns. The IRS has steadily increased the number of IDT fraud filters over the past several years, which now number 200.[21]

The IRS also formed the IRS Security Summit, which is described in the About the IRS Security Summit section of this Report.

But, there remain gaps in our security standards and practices

In the face of this threat, the IRS is severely limited in its ability to implement security standards and practices. For example, one court decision has held that the IRS does not have the authority to regulate unenrolled tax return preparers,[22] while another decision restricts the IRS's authority over tax professionals covered by Circular 230.[23] These legal precedents have had a chilling effect on any IRS action to advance tax

---

[17] The IRS's 2018 summertime security awareness campaign reported that "[d]ata thefts at tax professionals' offices continue to rise and result in fraudulent tax returns that can be especially difficult for the IRS and states to detect." (See https://www.irs.gov/newsroom/tax-security-101-irs-security-summit-partners-launch-new-awareness-campaign-urge-tax-professionals-to-step-up-protections-for-client-data).

[18] The IRS recently warned tax professionals of an uptick in phishing emails targeting them that involve payroll direct deposit and wire transfer scams. See IR-2018-253, December 17, 2018 (See https://www.irs.gov/newsroom/irs-security-summit-partners-warn-tax-professionals-of-fake-payroll-direct-deposit-and-wire-transfer-emails).

[19] GAO High Risk Series Report (GAO-19-157SP, March 2019 (See https://www.gao.gov/assets/700/697245.pdf); and TIGTA Management and Performance Challenges facing the Internal Revenue Service for Fiscal Year 2019, October 15, 2018 (See https://www.treasury.gov/tigta/management/management_fy2019.pdf).

[20] For an overview of one of these systems, see GAO Report: Tax Fraud and Noncompliance: IRS Could Further Leverage the Return Review Program to Strengthen Tax Enforcement (July 2018) (See https://www.gao.gov/assets/700/693374.pdf).

[21] See Highlights section in TIGTA Report: Partnership With State and Industry Leaders Is a Key Focus in Further Reducing Tax-Related Identity Theft (December 27, 2018) (See https://www.treasury.gov/tigta/auditreports/2019reports/201940012fr.pdf).

[22] See Loving v IRS, 742 F.3d 1013 (D.C. Cir. 2014), which addressed issues surrounding the IRS's regulation of non-credentialled (sometimes called unenrolled) preparers not subject to Circular 230.

[23] See Ridgely v. Lew, 55 F. Supp. 3d 89 (D.D.C. 2014).

professional security beyond merely providing information and encouraging compliance.[24]

Moreover, existing laws and regulations mandating security programs have gaps.

Specifically, Section 501(b) of the Gramm-Leach-Bliley Act (GLB)[25] requires that businesses providing financial products and services to individuals for personal, family, or household "protect the security and confidentiality" of nonpublic personal information and directed specified agencies to "establish appropriate standards…relating to administrative, technical, and physical safeguards." Pursuant to this authority, the Federal Trade Commission (FTC) issued the FTC Safeguards Rule (16 CFR 314) in 2002 to establish a standard for financial institutions. The Rule requires a written security plan, designated information security employees and ongoing assessments, implementation and monitoring of safeguards.[26] The FTC extended this regulation to cover tax preparers serving consumers.[27]

The GLB/Safeguards legal structure presents two gaps. First, the FTC's authority under GLB does not extend to tax preparers serving businesses (including the payroll community) because of GLB's limited focus on consumers and households. Second, the IRS has no enforcement authority under the FTC Safeguards Rule.

ETAAC believes that the IRS must have the ability to set tax return information security standards and practices if taxpayers are going to be adequately protected.

The IRS must continue to develop new competencies

The IRS must develop several new competencies as it presses ahead in the IDTTRF and cybersecurity fight. Some of the key competencies include:

- Data analytics capabilities to identify, understand and target specific threats and opportunities.
- Creation of clear, actionable guidance for relatively unsophisticated stakeholders, particularly in the area of cybersecurity.
- Partnering skills with external stakeholders, including the ability to manage independent stakeholders and facilitate disparate interests to reach shared vision on outcomes, priorities and initiatives.
- Organizational ability to innovate quickly, including the responsiveness of the IRS policy and legal functions. Cybercriminals are moving at light speed -- business as usual within the IRS will bring necessary innovation to a standstill.

---

[24] This article discusses the impact of the Loving and Ridgely legal precedents: https://www.forbes.com/sites/jamiehopkins/2014/07/18/the-irs-suffers-a-major-setback-in-its-ability-to-regulate-attorneys-and-cpas/#45792af7beaf.

[25] Also known as the Financial Services Modernization Act of 1999, P.L. 106-102 enacted November 12, 1999.

[26] See https://www.ftc.gov/sites/default/files/documents/federal_register_notices/standards-safeguarding-customer-information-16-cfr-part-314/020523standardsforsafeguardingcustomerinformation.pdf.

[27] See 16 CFR 313.3(k)(2)(viii) and 16 CFR 314.2(a). Given the jurisdictional scope of GLB, this designation is understood to relate to tax preparation firms serving consumers or individuals.

- New ways to anticipate future IDTTRF and cyberthreats proactively. The 2015 Security Summit Report tasked the Strategic Threat Assessment and Response (STAR) Work Group with "looking ahead, to enable the development of proactive, rather than reactive, initiatives and solutions to combat this crime."[28] ETAAC believes that the STAR Work Group and the ISAC should take a more proactive role in identifying the most likely and most damaging courses of action that cybercriminals may take and, then, develop the most effective ways to defend against those IDTTRF and cybersecurity threats. This effort should include the creation of recurring mechanisms to anticipate threats, such as tabletop or Red Team exercises.[29] These mechanisms should bring fresh perspectives from fields outside of tax, including government and industry experts, law enforcement, the financial community and experts in cybercrime.

[28] See https://www.irs.gov/pub/newsroom/2015%20Security%20Summit%20Report.pdf.

[29] ETAAC recognized this need in 2017 when it recommended that "The Security Summit should create mechanisms to enable stakeholders to anticipate future trends in identity theft, refund fraud and cybersecurity and develop proactive responses." ETAAC Annual Report to Congress, June 2017 (ETAAC 2017 Report).

ABOUT THE IRS SECURITY SUMMIT

Security Summit: Formation & Structure

The Security Summit was formed in 2015 and includes representatives from the IRS, state tax revenue agencies, tax professional community, tax preparation firms, software developers, financial service companies, and members of the Payroll Community.[30] Additional background information on the Security Summit can be found on irs.gov.[31]

The Security Summit currently has six Work Groups, each of which has a co-lead from each of the IRS, the states and industry.

The Security Summit initiative also includes an IDTTRF Information Sharing and Analysis Center (ISAC), which consists of the ISAC Platform (funded by IRS) and the ISAC Partnership.[32] The ISAC Platform shifted from pilot into full operational status in October 2018. The ISAC Partnership includes IRS, state and industry representatives and facilitates collaboration in IDTTRF detection and prevention. The ISAC Partnership is separately managed through its Senior Executive Board.

The responsibilities, accomplishments and current focus of each Work Group and the ISAC are further detailed in this section.

Security Summit: Progress From 2015 - 2018

The IRS reports that it has achieved significant progress against IDTTRF since the formation of the Security Summit in 2015.[33]

- Between 2015 and 2018, the number of taxpayers reporting they were identity theft victims fell 71 percent based on the number of identity theft affidavits filed.
    - In 2018, the IRS received 199,000 reports from taxpayers compared to 677,000 in 2015. This was the third consecutive year this number declined. There were 242,000 identity theft affidavits submitted in 2017 and 401,000 in 2016.
- Between 2015 and 2018, the number of confirmed identity theft returns stopped by the IRS declined by 54 percent.
    - For 2018, there was a slight -- 9 percent -- uptick in the number of confirmed identity theft returns (649,000 in 2018 compared to 597,000 in 2017). However, the 2018 count is still significantly below the 883,000 count in 2016 and the 1.4 million count in 2015.

[30] In this report, “Payroll Community” refers broadly to employers, software developers, cloud/hosting service providers, payroll service providers, reporting agents and others engaged in payroll and employment tax, while “Payroll” is used generically to refer to both the payroll and employment tax areas.

[31] See https://www.irs.gov/newsroom/security-summit

[32] The ETAAC Annual Report to Congress, June 2018 (ETAAC 2018 Report), p. 2, provides additional background on the ISAC’s structure and operations (See https://www.irs.gov/pub/irs-pdf/p3415.pdf).

[33] See https://www.irs.gov/newsroom/irs-security-summit-partners-mark-significant-progress-against-identity-theft-key-taxpayer-protection-trends-continue.

- Between 2015 and 2018, the IRS protected a combined $24 billion in fraudulent refunds by stopping confirmed identity theft returns.
    - In 2018, the 649,000 confirmed fraudulent returns asked for $3.1 billion in refunds. The IRS protected $6 billion in 2017, $6.4 billion in 2016 and $8.7 billion in 2015.
- Between 2015 and 2018, financial industry partners recovered an additional $1.4 billion in fraudulent refunds.
    - In 2018, financial institutions recovered 84,000 federal refunds totaling $112 million for the IRS. Institutions recovered 144,000 refunds worth $204 million in 2017, 124,000 refunds worth $281 million in 2016 and 249,000 refunds totaling $852 million in 2015.
    - Note: The financial industry is a key partner in fighting identity theft, helping the IRS and states recover fraudulent refunds that may have been issued. But as fewer fraudulent tax returns enter the system, fewer fraudulent refunds are being issued.

Work Groups & ISAC: Responsibilities, Accomplishments And Focus/Priorities

Authentication Work Group:

- Responsibilities:
    - Identify opportunities for strengthening authentication practices, including new ways to validate taxpayers and tax return information and new techniques for detecting and preventing IDTTRF.
- Accomplishments:
    - Improved schemas and enhanced procedures for reviewing tax returns.
    - Continued to analyze data elements and provided results to industry partners to discuss data quality, completeness and effectiveness in assisting with identity theft detection.
    - Increased the participation of the software industry and provided them with the ability to validate Electronic Filing Identification Numbers (EFINs) via Secure Data Transfer process.
- Focus/Priorities:
    - Analyze additional data elements for reject condition consideration.
    - Continue evaluating EFIN validation, W-2 Verification and Taxpayer Account Lock/Unlock efforts.

Information Sharing Work Group:

- Responsibilities:
    - Identify opportunities for sharing information to improve the collective capabilities for detecting and preventing IDTTRF.

- Accomplishments:
    - Continued leads analysis and sharing with each partner to discuss their uniquely reported leads.
    - Introduced a new lead schema for business-related identity theft for the 2019 filing season.
    - Developed a new alert form that allows ISAC members to notify the Rapid Response Team (RRT) of suspicious activity.
    - Formalized Security Summit membership criteria and standards of conduct and onboarded 5 new members.
- Focus/Priorities:
    - Continue to assess the current leads process for feedback reporting to states and industry.
    - Continue to explore opportunities for information sharing with our partners by enhancing the existing confirmed identity theft file.

Strategic Threat Assessment and Response (STAR) Work Group:

- Responsibilities:
    - Identify points of vulnerability (threats/risks) related to the detection and prevention of IDTTRF, develop a strategy to mitigate or prevent these risks and threats, and review best practices and frameworks used in other industries.
- Accomplishments:
    - Completed year two of a three-year plan implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) for the tax software industry.
    - Established a three-year plan to implement the NIST Cybersecurity Framework (CSF) for the payroll community.
    - Established a three-year “Trusted Customer” plan aligned with NIST, digital identity guidelines.
- Focus/Priorities:
    - Expand the Trusted Customer roadmap for the Payroll community.
    - Continue supporting cybersecurity education.

Financial Services Work Group:

- Responsibilities:
    - Examine and explore additional ways to prevent and deter criminals from accessing tax refunds, tax-related financial products, deposit accounts, and pre-paid debit cards.

- Accomplishments:
    - Continued the pre-validation effort with financial institutions.
    - Launched a pilot project with the Bureau of Fiscal Services (BFS) to support the IRS and Financial Institutions participating in the external leads program for the enhancement of the NACHA reject process.
- Focus/Priorities:
    - Continue evaluating the pre-validation and BFS pilot efforts.
    - Conduct outreach with financial institutions potentially impacted by IDTTRF and expand the external leads process.

Communication and Taxpayer Awareness Work Group:

- Responsibilities:
    - Increase awareness among individuals, businesses and tax professionals on the need to protect sensitive tax and financial information.
- Accomplishments:
    - Continuation of taxpayer-focused awareness campaign, "Taxes.Security.Together" including a new page on IRS.gov Tax Professionals – Protect Client Data, Learn Signs of Data Theft.
    - Conducted expanded tax professional-focused Security Awareness campaign, "Protect Your Client, Protect Yourself" to raise awareness of security risks to tax professionals posed by identity thieves and encourage protection of taxpayer data. These efforts included 10-week "Tax Security 101" campaign to coincide with the Nationwide Tax Forums.
    - Debuted a new IRS Twitter handle @IRSTaxSecurity in November; the IRS Instagram feed launched around the same time to help highlight security issues.
    - Managed its third annual Tax Security Awareness Week in Dec. 2018, which led to 36 press conferences and partner events across the country.
    - Highlighted emerging scams and schemes, including the Dirty Dozen tax scams in March 2019.
- Focus/Priorities:
    - Continue messaging through social media channels, including the new Twitter @IRSTaxSecurity handle.
    - Planning cybersecurity sessions for summer 2019 Nationwide Tax Forums.

Tax Professional Work Group:

- Responsibilities:
    - Examine how new requirements will affect tax preparers, how the preparer community will be affected by the overall data capture and reporting

requirements and how the preparer community can contribute in the prevention of identity theft and IDTTRF.

- Accomplishments:
    - Assisted in the development of content for the IRS's "Protect Your Client, Protect Yourself" and "Tax Security 101" campaigns.
    - Utilized social media and other communication channels to share the availability of continuing education credit for data and information security courses.
    - Modified PTIN registration and renewal letters to provide resource link to e-news subscriptions.
    - Disseminated wallet-sized "what to do in the event of data breach" information cards.
    - Expanded "Returns Per PTIN" functionality allowing all preparers completing a certain number of returns to match the number of returns IRS received with their Preparer Taxpayer Identification Number (PTIN) against the number of returns the preparer completed allowing for earlier identification of PTIN misuse.
- Focus/Priorities:
    - Continue messaging to tax professionals through existing channels.
    - Develop ongoing messages emphasizing a defined area of security planning.

Information Sharing and Analysis Center (ISAC)

- Responsibilities:
    - Centralize, standardize and enhance data compilation and analysis to facilitate sharing actionable data and information.
- Accomplishments:
    - Transitioned the ISAC from a pilot phase to an operational platform to ensure partnership organizations including IRS, States, and Industry work in coordination through a Trusted Third Party to detect and prevent IDTTRF.
    - Increased ISAC membership to 65 member organizations.
- Focus/Priorities:
    - ISAC Senior Executive Board:
        - Pursue legislative changes to allow the IRS to share data into the ISAC.
        - Pursue a solution to share data with financial institution members.
        - Execute the ISAC's Strategic Goals:

- Confidence: Heighten taxpayers' confidence in the nation's tax systems by knowing that we are all working together to fight IDTTRF.
- Integrity: Protect the integrity of the tax ecosystem by preventing and deterring IDTTRF.
- Collaboration: Collaborate with partners, endorsers and stakeholders proactively to improve prevention and detection of IDTTRF.
- Talent Cultivation: Cultivate a well-equipped, diverse, flexible and engaged cross-functional team throughout the tax ecosystem.
- Thought Leadership: Advance data access, usability and analytics to inform decision making and improve operational outcomes.
- Excellence: Drive increased agility, efficiency, effectiveness and security of the tax ecosystem operations.

o <u>ISAC Operational Platform:</u>

- Improve User Experience/Utility with appropriate access on a secure platform.
- Continue efforts to build skills of the community by leveraging the Trusted Third Party, Analyst Community of Practice, endorsing organizations and membership.
- Continue efforts to optimize use of the data currently available to the ISAC membership.
- Continue to monitor metrics and value added of the ISAC to IDTTRF prevention effort.
- Continue collaboration with Security Summit Working Groups on opportunities to provide feedback.
- Continue to explore new information and data sources including other ISACs (Multi-State or National Association of ISACs) or government agencies to improve detection or avoid false detection.

ETAAC Integration With The Security Summit

The Security Summit's efforts were first institutionalized through the auspices of the ETAAC in 2016 when an amendment to ETAAC's charter expanded its scope to include researching, studying and making recommendations regarding the prevention of IDTTRF. On an ongoing basis, ETAAC members engage with the IRS, as well as with Security Summit membership, by attending and participating in work group activities. Additionally, ETAAC members proactively engage with the Security Summit by consulting with work group co-leads to keep abreast of Security Summit initiatives and IDTTRF developments.

PROGRESS ON ETAAC 2018 AND 2017 RECOMMENDATIONS

ETAAC recognizes that its recommendations are provided for the IRS's consideration and, ultimately, the IRS must decide whether and how to implement them based on its assessment of benefit/cost and competing priorities. Generally, the IRS agreed with the direction of the nineteen Recommendations included in the ETAAC 2018 Report, and identified their current policies or activities that it believes are consistent with them or reported an intention to evaluate or implement them, as appropriate.

Progress on ETAAC 2018 Recommendations

The IRS has provided ETAAC with periodic updates on its progress, which has been good notwithstanding the impact of implementing the Tax Cuts and Jobs Act and the partial government shutdown. Specific 2018 recommendations on which IRS has made progress include:

- #2: Increase outreach to employers and businesses
- #3: Ensure the effective operation of the Security Summit and ISAC
- #6: Increase participation in Security Summit cybersecurity initiatives
- #7: Communicate and build tax professional awareness
- #12: Improve detection with enhanced business tax schema data elements
- #15: Enhance identity proofing and authentication by extending eligibility to obtain an Identity Protection Personal Identification Number (IP PIN) to all individual taxpayers.

ETAAC recommends continued IRS attention to two of its remaining 2018 recommendations:

- #10: Establish clear IRS internal responsibility.
    - ETAAC continues to believe that the IRS should identify and empower one organization inside the agency with overall responsibility for setting security requirements for tax professionals and coordinating the implementation and education of such requirements across the various internal IRS organizations.
- #17**:** The IRS should prioritize the development of an electronic means to submit and accept powers of attorney.
    - We understand that the IRS has received approval to begin elaboration on a tax professional online capability, which would include electronic means to submit and manage authorizations. IRS advises that this project is included in Phase 1 of the IRS Integrated Modernization Business Plan.[34]

[34] See https://www.irs.gov/pub/irs-utl/irs_2019_integrated_modernization_business_plan.pdf.

Additionally, ETAAC has made recommendations in its 2019 Report that relate to, reinforce or update our perspective on several 2018 recommendations:

2018 Recommendation	Related 2019 Reco. #
#1: Integrate the payroll community more broadly into the Security Summit and the ISAC	# 4
#5: Establish a common security standard and the IRS's enforcement authority; and, #8: Require security continuing education	#7
#11: Enact an IRC Section 6103 IDTTRF exception	#2
#14: Investigate the use of Trusted Third Parties, such as appropriately screened and trained tax professionals, as an alternative to conduct in-person identity proofing to enable taxpayers to ultimately gain remote secure access to their information.	#8

Progress on selected ETAAC 2017 Recommendations

The ETAAC 2018 Report highlighted three 2017 recommendations as requiring more or continued attention. The IRS continues to work on these recommendations and they are mentioned here to emphasize their continued importance.

Recommendation #3: Given its associated exceptionally high e-file rejects, the IRS should analyze the effectiveness of the Prior Year Adjusted Gross Income/Self-Select PIN taxpayer signature verification model, and work collaboratively within the Security Summit to identify options to replace this model, preferably with one that could be used by both the IRS and States.

> ETAAC Updated Observations: The IRS studied this issue and provided ETAAC with an overview of the taxpayers' ability to successfully e-file even though the first attempt may fail.

Recommendation #11: The Security Summit should create mechanisms to enable stakeholders to anticipate future trends in identity theft, refund fraud and cybersecurity and develop proactive responses. One example of such a mechanism would be a day-long "Red Team" working session where Security Summit stakeholders brainstorm IDTTRF and security trends to anticipate where threats might be in future years and, then, determine potential responses that could be undertaken now.

> ETAAC Updated Observations: IRS has provided updated information concerning its proactive approach to anticipate future IDTTRF threats. However, ETAAC believes there are opportunities to conduct these types of forward-looking activities in the cybersecurity area through the STAR Work Group or ISAC.

Recommendation #17: The IRS should thoroughly review and update the key IRS publications for the IRS e-file Program (e.g., Publication 1345, Handbook for Authorized IRS e-file Providers for Individual Income Tax Returns, and Publication 3112, IRS e-file Application and Participation) and the IRS publications outlining security practices (e.g.,

Publication 4557, Safeguarding Taxpayer Data) to accomplish the following: Ensure the e-file program publications educate Electronic Return Originators (EROs) on the cyber and physical security risks facing them; Provide a clear and full statement of the security regulations, standards and requirements applicable to a tax professional's participation in IRS e-file, and the potential consequences of failing to comply; Provide simple, clear and actionable guidance on how to implement a security program, preferably consolidated into a single source publication; and, Review, update and improve such content on a regular basis.

> ETAAC Updated Observations: Some progress has been made, but ETAAC continues to be concerned about the lack of a single IRS "owner" for security standards and practices across the tax ecosystem. ETAAC's 2018 Recommendation #10 articulated our concerns and suggested actions.

Progress on ETAAC 2017 and 2018 Electronic Filing Recommendations

ETAAC's charter includes researching, analyzing, considering and making recommendations on the IRS's progress toward the Congressional policy goal of achieving an 80% e-file rate. To that end, ETAAC made specific recommendations in each of 2017 and 2018 to increase electronic filing.

First, the IRS annually receives almost 4 million amended tax returns on IRS Form 1040X, which must currently be filed on paper. Recommendation #22 in ETAAC's 2017 Report[35] recommended that the IRS change this situation and enable taxpayers to electronically file amended individual tax returns through the IRS:

> *The IRS should implement the ability for taxpayers to electronically file amended returns on Form 1040X, Amended U.S Individual Income Tax Return, through the IRS Modernized e-file (MeF) System.*

As noted in its 2017 Report, this action would have several benefits. It would avoid the need for paper and manual processes, help to achieve the Congressionally-mandated target of achieving 80% electronic filing rates and provide a seamless transmission channel for both federal and state amended returns by leveraging the existing electronic filing network consisting of MeF and the hundreds of software packages already designed to connect with MeF in stark contrast to a stove-piped federal only solution. Additionally, the electronic filing of Form 1040X through MeF would ensure that the IRS receives more attributes associated with tax returns that could assist in identifying IDTTRF.

Second, as ETAAC has repeatedly noted, the Form 94X employment tax return series has the second highest volume of tax return series and the lowest e-file rates – by far. Recommendation #19 in ETAAC's 2018 Report[36] recommended that IRS undertake a collaborative approach to increase the electronic filing of employment returns:

> *The IRS should leverage its public/private partnerships to establish a collaborative undertaking with all key stakeholders focused on a two phase approach to increase electronic filing rates for the Form 94X series: Phase One*

[35] ETAAC 2017 Report, pps. 45 – 46.

[36] ETAAC 2018 Report, pps. 48 – 50.

should focus on improving the IRS' content and communications regarding Form 94X electronic filing, and Phase Two should focus on streamlining IRS policies and procedures that create unnecessary barriers to increased e-file for Form 94X series.

The IRS should pursue both of these recommendations through a public/private partnership with states and industry. These partnerships have demonstrated their effectiveness, both in providing integrated and seamless federal and state electronic filing experiences to taxpayers and tax professionals and in fighting IDTTRF.

SUMMARY LIST OF ETAAC 2019 RECOMMENDATIONS

Below are ETAAC's 2019 recommendations organized into three specific areas. Our detailed analysis and explanation of each recommendation is found in the "Detailed Support for ETAAC 2019 Recommendations" section of this Report. These recommendations are not listed in priority order.

I: STRENGTHEN THE SECURITY SUMMIT: ENABLE & EXPAND

RECOMMENDATION #1: *Fund the ISAC*

Congress should appropriate funds for the IRS's requested budget program increases for IDTTRF prevention including approximately $7 million to enable contractor support for the ISAC.

RECOMMENDATION #2: *Enact an IDTTRF exception to IRC Section 6103*

Congress and the Department of the Treasury should make targeted legislative and regulatory changes, respectively, to permit appropriate uses and disclosures by the IRS under Internal Revenue Code Section 6103 for IDTTRF detection and prevention purposes.

RECOMMENDATION #3: *Increase the engagement of ISAC members*

The IRS and ISAC should increase the engagement of ISAC members by (i) using the ISAC Strategic Plan's Engagement Model to illustrate and encourage higher levels of participation, and (ii) leveraging state and industry endorsing organizations to provide guidance and support to improve performance quality.

RECOMMENDATION #4: *Integrate the Payroll Community more fully into the Security Summit*

The IRS should, in collaboration with Security Summit members, conduct a prompt review of the Payroll Community and develop a plan for the Community's full integration into the Security Summit and ISAC on an accelerated basis.

RECOMMENDATION #5: *Pilot a Financial Services Company (FSC) Collaboration Space in the ISAC*

The IRS should pilot a dedicated Financial Services Company (FSC) Collaboration Space in the ISAC to facilitate FSC information sharing in order to leverage their unique insights in identifying and preventing IDTTRF.

II: IMPROVE SECURITY IN KEY AREAS OF OUR TAX SYSTEM

RECOMMENDATION #6: *Assess the state of information security practices in the tax professional community*

In collaboration with the Security Summit, the IRS should develop and execute a plan for ongoing research on the state of information security practices and vulnerabilities in the tax professional community.

RECOMMENDATION #7: *Grant the IRS the authority to establish and enforce security standards*

Congress should grant IRS clear legal authority to develop, implement and enforce appropriate information security standards and practices in the area of tax administration, which would include establishing administrative, technical, and physical safeguards, implementing required education and training, and providing ongoing guidance.

III: PROTECT & ENABLE TAXPAYERS

RECOMMENDATION #8: *Develop and expand channels for identity proofing*

The IRS should (i) continue its current efforts to implement digital identity proofing protocols compliant with NIST Special Publication 800-63-3 Digital Identity Guidelines, and (ii) identify and develop opportunities to expand the availability of identity proofing mechanisms in other channels including the implementation of an IRS trusted third-party identity verification program.

RECOMMENDATION #9: *Collaborate with Security Summit members to identify and pilot emerging approaches for identity verification*

The IRS should engage regularly with subject matter experts from Security Summit members to identify and potentially pilot emerging technologies or approaches to verify identities across all channels.

RECOMMENDATION #10: *Engage with the Security Summit to improve the Taxpayer Protection Program's taxpayer experience*

The IRS should collaborate with Security Summit and ISAC members to identify actions to increase the number of legitimate taxpayers timely responding to Taxpayer Protection Program communications.

DETAILED SUPPORT FOR ETAAC 2019 RECOMMENDATIONS

Below are ETAAC's 2019 recommendations and supporting analysis, which provides important context and elaboration for each recommendation.

I. STRENGTHEN THE SECURITY SUMMIT: ENABLE & EXPAND

INTRODUCTION

The recommendations in Part I strengthen the Security Summit in several ways. Recommendations #1, #2 and #3 enable the Identity Theft Tax Refund Fraud (IDTTRF) Information Sharing and Analysis Center (ISAC) by:

- Funding ISAC operations,
- Enabling the ISAC's information sharing capabilities by creating an IDTTRF exception to Internal Revenue Code (IRC) Section 6103, and
- Improving the ISAC's ability to detect and analyze fraudulent schemes by promoting the use of the ISAC Strategic Plan's Engagement Model and leveraging state and industry endorsing organizations[37] to provide guidance and support.

Recommendations #4 and #5 expand the capabilities of the Security Summit and ISAC by fully integrating the Payroll Community and piloting a Financial Services Company Collaboration Space.

ISSUES & RECOMMENDATIONS

……

ISSUE: The current model for funding the ISAC creates uncertainty about its continuing operations. Congress has an opportunity to strengthen the Security Summit by authorizing funding for the ISAC as a permanent component of the Security Summit.

RECOMMENDATION #1: ***Fund the ISAC***

Congress should appropriate funds for the IRS's requested budget program increases for IDTTRF prevention including approximately $7 million to enable contractor support for the ISAC.

Support for Recommendation:

Partnering with external stakeholders is a key element of the IRS Strategic Plan

One of the IRS's six strategic goals is to "Collaborate with external partners proactively to improve tax administration."[38] The IRS recognizes that such collaborations help it

[37] Although they do not have statutory authority to administer state or federal taxes, "endorsing organizations" support tax administration through the collective activities and commitments of their members. They are not "parties" to the Security Summit MOU but do support this public/private initiative.

[38] IRS Strategic Plan FY 2018-2022 (IRS Strategic Plan), page 15 (See https://www.irs.gov/pub/irs-pdf/p3744.pdf).

find innovative solutions, tackle common challenges and enhance its ability to serve taxpayers and operate efficiently.

The IRS Strategic Plan identifies several types of collaborative activities with external stakeholders that benefit the IRS and taxpayers, and align with the Security Summit initiative:

- Incorporating insights from partners into IRS service and outreach channels.
- Enhancing monitoring of the tax ecosystem to combat abusive behavior.
- Expanding interagency and private sector working groups to collaborate on areas of mutual interest, building on successes like the Security Summit.
- Consulting with the private sector to integrate industry-leading practices into IRS operations, particularly around customer service, analytics and cybersecurity.

ISAC participation and usage is increasing

The ISAC is a notable illustration of the IRS's partnership strategy in action. It is the IRS's most significant IDTTRF collaborative platform and enables the IRS, state revenue agencies and industry to identify, report, analyze, distribute and act on IDTTRF activity in real time.

A recent TIGTA report noted the ISAC's growing participation, including an increase in participating organizations from 18 in 2017 to more than 60 in 2018, as well as an increase in registered users from 264 in 2017 to 426 in 2018.[39] The report further notes that "alert and data contributions by participating organizations have increased by more than six times since January 2017, which has increased the volume of data sharing as well as the quality of the ISAC's data analytics."

ISAC funding needs to be stable

In its recently submitted Congressional Budget Justification and Annual Performance Report and Plan Fiscal Year 2020 dated March 18, 2019, the IRS has requested $22 million for additional identity theft prevention resources including approximately $7 million for the ISAC.[40]

ETAAC supports this request and notes that additional funding may be required in future years as ISAC further expands its membership, usage and operations.

---

[39] TIGTA Report "Partnership With State and Industry Leaders Is a Key Focus in Further Reducing Tax-Related Identity Theft" (Ref. No. 2019-40-012, December 27, 2018), pps. 6-7 (See https://www.treasury.gov/tigta/auditreports/2019reports/201940012fr.pdf).

[40] IRS Congressional Justification, pps. IRS-15 to IRS-16 (See https://home.treasury.gov/system/files/266/02.-IRS-FY-2020-CJ.pdf).

……

ISSUE: The IRS is prohibited from sharing valuable IDTTRF-related information within the ISAC because of restrictions under IRC Section 6103. Congress has an opportunity to enable the sharing of this information to improve ISAC's ability to detect and prevent IDTTRF returns while still protecting taxpayer privacy.

RECOMMENDATION #2: ***Enact an IDTTRF exception to IRC Section 6103***

Congress and the Department of the Treasury should make targeted legislative and regulatory changes, respectively, to permit appropriate uses and disclosures by the IRS under Internal Revenue Code Section 6103 for IDTTRF detection and prevention purposes.

Support for Recommendation:

Appropriate and principled changes can be made to IRC Section 6103 that both protect taxpayer privacy and enable IDTTRF prevention

IDTTRF and its related prevention efforts affect millions of taxpayers as noted in this (and past) ETAAC reports. Victimized taxpayers are subjected to lengthy processes to prove their identity, which may delay their refunds for months -- a serious financial burden on families living paycheck-to-paycheck and relying on tax refunds to make ends meet. This situation can be alleviated by the sharing of targeted data elements about suspicious returns between Security Summit stakeholders in ways that help identify and prevent IDTTRF schemes and patterns.

In its 2018 Report, ETAAC explained how IRC Section 6103 is designed to protect taxpayers but also creates barriers to information sharing vital to IDTTRF detection and prevention. At that time, ETAAC recommended that Congress amend IRC Section 6103 to enable narrowly crafted uses and disclosures of tax information to fight IDTTRF. ETAAC provided a full analysis for its recommendation, including guiding principles to ensure continued taxpayer privacy and protection.[41]

In 2019, ETAAC reaffirms its support for this recommended legislative action. As necessary, IRS Legislative Affairs should work directly with the ISAC to obtain specific illustrations and use cases concerning the information currently unable to be shared and identify the associated IDTTRF prevention impact.[42]

[41] ETAAC 2018 Report, Rec. #11, pps. 34 – 37.

[42] ETAAC illustrated the impact of IRC Section 6103 in the ETAAC 2018 Report (See p. 35).

……

ISSUE: ISAC's effectiveness rests on the level and quality of its members' participation. The IRS and ISAC have an opportunity to continue maturing the ISAC's IDTTRF detection and prevention capabilities by promoting the ISAC engagement model and leveraging the guidance and support of the ISAC's endorsing organizations.

RECOMMENDATION #3: ***Increase the engagement of ISAC members***

The IRS and ISAC should increase the engagement of ISAC members by (i) using the ISAC Strategic Plan's Engagement Model to illustrate and encourage higher levels of participation, and (ii) leveraging state and industry endorsing organizations to provide guidance and support to improve performance quality.

Support for Recommendation:

The ISAC plays a key role in identifying and stopping IDTTRF schemes

The ISAC includes the IRS, state and industry membership,[43] which provides it with unique visibility across the tax ecosystem and broad analytical capabilities.

The ISAC's primary advantage is its ability to share threat and scheme information with tax system stakeholders quickly (and within legally permissible parameters) so they can take action to protect taxpayers and tax revenue.

In preparation for the 2019 filing season, the ISAC took a number of steps to improve information sharing including:

- enhancing the alerts reporting process and refining collaboration tools;
- improving the way information is analyzed and shared by creating visualization dashboards and adding performance metrics;
- enhancing the security of ISAC systems through training, audits and testing; and
- providing pre-filing season training in numerous areas including leads and alerts reporting, data analysis and data usage.

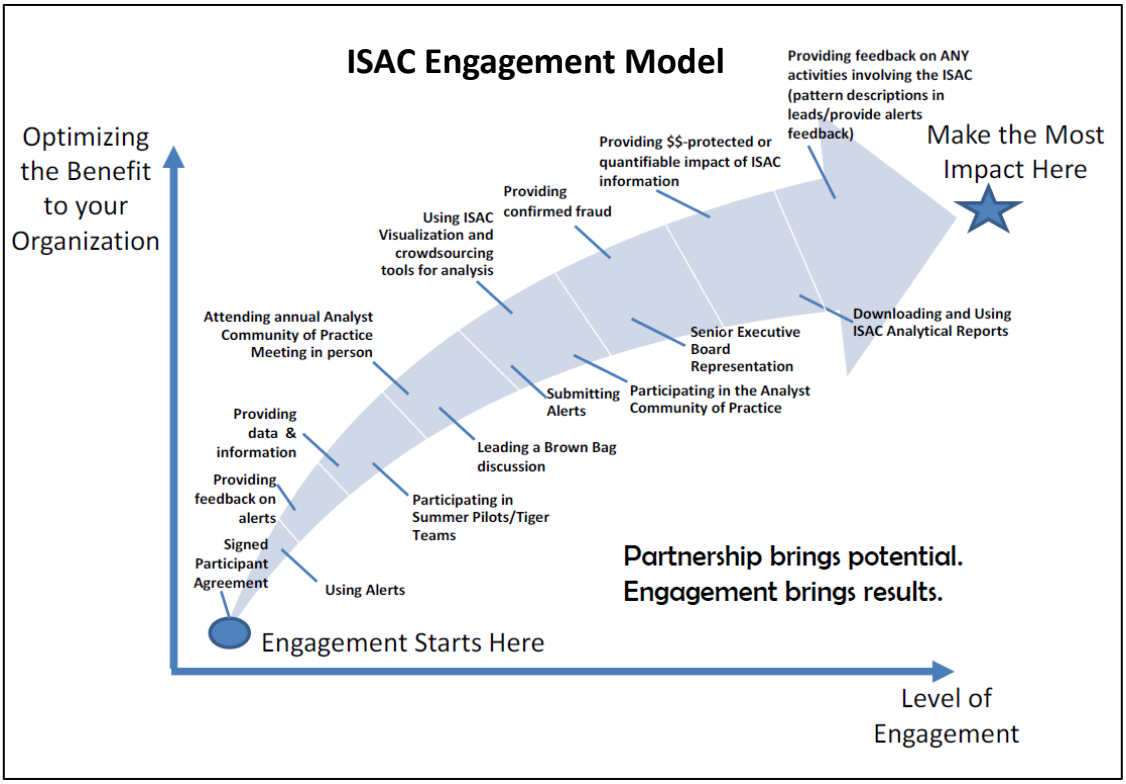
Ultimately, the ISAC's effectiveness rests on the level and quality of its members' participation.

[43] Currently, IRS, all states and a majority of industry members participate in the ISAC. The ISAC's structure is described in the About the IRS Security Summit section of this Report.

The ISAC Engagement Model provides a framework to increase the level of ISAC member participation

In January 2019, the ISAC issued its first Strategic Plan, which provides specific goals[44] aligned with the IRS's overarching strategic goals. The plan presents an "Engagement Model" to guide ISAC members along the continuum of potential ISAC activities that enable the ISAC's fight against IDTTRF (see below graphic).

The opportunities to increase one's level of participation may not be self-evident to ISAC members, especially new members or their analysts. For that reason, the ISAC should actively promote the Engagement Model to educate its members on how they can more broadly participate in the ISAC in order to add value to their organization's and to the ISAC's IDTTRF efforts.



Endorsing organizations can help improve the quality of ISAC member participation

The quality of member participation also affects the ISAC's effectiveness.

Participation quality is largely a function of the training and experience of ISAC member analysts. Achieving and maintaining high quality is challenging because of relatively high turnover in ISAC member fraud analysts. Therefore, it is essential to have a cadre

[44] ISAC's strategic goals include: protecting the integrity of the tax ecosystem by preventing and deterring Identity Theft Tax Refund Fraud; collaborating with partners, endorsing organizations and stakeholders proactively to improve prevention and detection of IDTTRF; and, advancing data access, usability and analytics to inform decision-making and improve operational outcomes.

of experienced resources that can accelerate the development of new members and analysts.

National groups can supplement the ISAC's community of experienced resources in order to accelerate the development and capabilities of ISAC members and analysts.

Several key national groups are already endorsing organizations of the ISAC and Security Summit. At the state level, the key endorser of the Security Summit is the Federation of Tax Administrators (FTA),[45] which has had a steadily increasing role in coordinating between state revenue agencies and the ISAC.[46] At the industry level, there are several endorsing organizations of the Security Summit from various communities: tax software and preparation (CERCA, ACTR and Free File), tax professionals (National Society of Tax Professionals and National Society of Accountants), financial services (National Branded Prepaid Card Association) and payroll (American Payroll Association).

Endorsing organizations generally engage with the Security Summit through semi-annual Security Summit and ISAC roundtables. Despite restrictions on access to sensitive ISAC information, these endorsing organizations can still work together to increase the quality of their members' participation. In particular, the ISAC and its endorsing organizations should consider whether and how they can develop a communication and education plan to increase member engagement, especially because endorsing organizations have insights that can help the ISAC tailor its outreach and training to particular membership segments.

……

ISSUE: The Payroll Community possesses information that is an attractive target for IDTTRF cybercriminals, and also has insights that can help detect and prevent IDTTRF. The IRS can better protect payroll information and improve its ability to detect and prevent IDTTRF by more fully integrating the Payroll Community into the Security Summit and ISAC.

RECOMMENDATION #4: ***Integrate the Payroll Community more fully into the Security Summit***

The IRS should, in collaboration with Security Summit members, conduct a prompt review of the Payroll Community and develop a plan for the Community's full integration into the Security Summit and ISAC on an accelerated basis.

Support for Recommendation:

ETAAC reaffirms its 2018 payroll-related recommendations

[45] The FTA is an association of state and local tax and revenue agencies that provides training, information and opportunities for collaboration to its membership.

[46] The ISAC and FTA coordinate periodic calls to provide state fraud analysts with up-to-date information and opportunities to collaboratively examine evolving threats.

In its 2018 Report, ETAAC offered two recommendations relating to the Payroll Community: (i) integrate the Payroll Community more broadly into the Security Summit and the ISAC, and (ii) increase outreach to employers and businesses.[47] ETAAC also observed that the IRS's first step to determine the best way to integrate the payroll industry more broadly into the Security Summit is to "gain a clear understanding of the structure of the industry, the roles and functions performed by its different segments and the risk profiles of different business and operational models."[48]

ETAAC reaffirms these 2018 recommendations and observations, and believes the IRS should move quickly to better understand and more fully integrate the Payroll Community into the Security Summit.

The Payroll Community has multiple and complicated operating models

Generally, employers are handling two core functions in the payroll area: (i) paying employees, which includes making tax deposits and issuing Forms W-2, and (ii) filing periodic employment tax returns. About 30 million federal employment tax returns are filed annually.[49]

Employers arrange their payroll functions between in-house staff and contracted service providers, which can make it difficult to understand payroll functions, roles and operating models. Our inquiry suggests that the most commonly used arrangements are:

- In-house payroll and in-house employment tax compliance.[50]
- In-house payroll coupled with contracted employment tax compliance.
- Contracted payroll coupled with in-house employment tax compliance.
- Contracted payroll and contracted employment tax compliance.[51]

These arrangements typically involve at least five key stakeholders: the employee, the employer, software vendor(s), the payroll contractor and the employment tax compliance contractor.[52]

The multiplicity of possible operating models contributes to the use of confusing or vague Payroll Community terminology that can create uncertainty and misunderstanding. For example, employers that perform payroll functions in-house usually do not consider themselves to be payroll processors. As a result, employers may ignore IRS communications messaged to "payroll providers" even if those communications are relevant to the employer performing those services in-house. The same confusion exists for IRS communications messaged to "Reporting Agents," which

[47] ETAAC 2018 Report, Recs. #1 and #2.

[48] ETAAC 2018 Report, p. 15.

[49] "Employment returns" refers generally to Form 940 Employer's Annual Federal Unemployment (FUTA) Tax Return, Form 941 Employer's Quarterly Federal Tax Return and related returns..

[50] Employers performing these functions in-house typically use internally or third-party developed payroll/employment tax or ERP software, which may be hosted on remote servers.

[51] These two contractors may be the same company or different companies.

[52] There can be even more stakeholders if the employer arranges its functions differently.

appear to be directed to contractors when, in fact, they may be relevant to an employer's in-house tax compliance function.

Moreover, the Payroll Community seems more fragmented than the income tax software community. Although the Payroll Community may have some very large Reporting Agents (such as ADP, Paychex, Ceridian and Intuit), there are hundreds of thousands of independent payroll service providers and employers that must be engaged. The challenge in communicating to and educating the various stakeholders in the Payroll Community is akin to the challenge facing the IRS in terms of the hundreds of thousands of income tax professionals.

Payroll information is at risk…it is valuable to cybercriminals while, at the same time, is not subject to any legally required minimum security standard

One challenge in protecting payroll information is the potential for its wide distribution and broad access. The information may reside across multiple databases with employers, hosted software solutions, and payroll and employment return compliance contractors. Additionally, multiple stakeholders may have access to it. For example, hundreds or thousands of employees may have access to payroll self-service portals to access their payroll information on a contractor's system. These portals are at risk for account takeovers or breaches, and have been identified as a known risk.[53]

ETAAC believes that many Payroll Community stakeholders have robust cybersecurity programs based on established security protocols such as ISO 27000 series.[54] However, the implementation of effective information security programs is an ongoing challenge for any company, especially smaller ones that may lack significant internal cybersecurity expertise and resources. The cybersecurity challenge facing the Payroll Community is akin to that facing the hundreds of thousands of tax professionals.

Unfortunately, there is no basic security standard applicable to the business tax area to guide companies and employers. As previously explained, the FTC Safeguards Rule only applies to "tax preparers" in consumer settings. The Rule does not extend to employers or to businesses providing services to other businesses, including payroll.

The Security Summit's STAR Work Group, including its Payroll Subgroup, is developing best practices around security controls based on the *National Institute of Standards and Technology (*NIST) Cybersecurity Framework.[55] However, ETAAC believes this situation is insufficient. Instead, the IRS should have the independent legal authority to develop, implement and enforce appropriate information security standards and practices in the tax administration area, including the business tax and payroll areas. Recommendation #7 in this Report is intended to address this need.

---

[53] An FBI public service announcement reported complaints of cybercriminals "targeting the online payroll accounts of employees." (See https://www.ic3.gov/media/2018/180918.aspx).

[54] See https://www.iso.org/isoiec-27001-information-security.html. NIST actually maps the NIST controls found in NIST 800-53 to the relevant ISO 27001 controls in its Appendix I (See https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf).

[55] See https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. For specific security controls, see https://nvd.nist.gov/800-53.

The IRS currently engages with the Payroll Community in several ways

Outside the Security Summit. The IRS has numerous communication channels with different elements of the Payroll Community including:

- Periodic calls/meetings with the Payroll Community.
- IRS security awareness communications and campaigns.[56]
- IRS e-News & Alerts.[57]
- IRS Website content targeting the Payroll Community.[58]

Inside the Security Summit. The IRS issued formal membership criteria in 2018 for various tax industry companies including members of the Payroll Community, and has begun to accept applications.[59] Additionally, the STAR Work Group has formed a Payroll Subgroup, which is currently following the same approach that the STAR Tax Software Subgroup took to conduct a phased implementation of the NIST Cybersecurity Framework.

But there is more the IRS can do to enhance and increase the Payroll Community's role in the IDTTRF fight and improve its cybersecurity

Outside the Security Summit. IRS can communicate more effectively with the Payroll Community by, for example:

- Payroll Community Calls/Meetings: Leveraging its payroll-related events more systematically and deliberately to communicate with and get feedback from the Payroll Community.
- IRS Communications Campaigns, e-News & Alerts: Communicating more clearly and systematically with Payroll Community stakeholders on relevant topics and risks in these channels.[60] These communications should use payroll terminology that resonates with payroll stakeholders (including employers), and address the broader range of payroll-specific or unique risks such as self-serve portals.[61]

---

[56] See, for example: https://www.irs.gov/newsroom/national-tax-security-awareness-week-no-5-small-businesses-be-alert-to-identity-theft, and https://www.irs.gov/individuals/taxes-security-together, https://www.irs.gov/tax-professionals/protect-your-clients-protect-yourself.

[57] IRS has several email notices and alerts potentially relevant to the Payroll Community, e.g., e-News for Payroll Professionals; e-News for Tax Professionals; e-News for Small Businesses; and Quick Alerts.

[58] IRS reports that it has updated resources to assist businesses with identity theft including https://www.irs.gov/identity-theft-fraud-scams, https://www.irs.gov/individuals/form-w2-ssn-data-theft-information-for-businesses-and-payroll-service-providers and https://www.irs.gov/individuals/identity-theft-guide-for-business-partnerships-and-estate-and-trusts.

[59] See https://www.irs.gov/newsroom/security-summit. (Scroll down to heading at bottom of the page titled, "Apply to Become a Member of the Security Summit").

[60] ETAAC found one press release specifically addressing the targeting of payroll and HR departments with W-2 scams. See https://www.irs.gov/newsroom/irs-states-and-tax-industry-renew-alert-about-form-w-2-scam-targeting-payroll-human-resource-departments. However, on Security Summit topics, IRS's press releases are not typically targeted to the Payroll Community on issues specific to their risks.

[61] IRS may repurpose communications originally used for tax professionals or send out a combination communications intended to speak to both income tax and payroll professionals. These communications may not resonate with payroll professionals. For example, ETAAC found one e-News for Payroll

- IRS Website: Improving Payroll Community content on irs.gov, and centralizing payroll-relevant IDTTRF and security information to make it easier to find. Only a small amount of irs.gov content specifically targets the Payroll Community about cybersecurity practices, identifying and dealing with unique risks or reporting IDTTRF schemes (beyond stolen W-2s).[62]

Inside the Security Summit. The IRS has opportunities to integrate the Payroll Community including:

- STAR Payroll Subgroup. Based on ETAAC's inquiries, the IRS should reassess the direction and focus of the STAR Payroll Subgroup. Payroll Subgroup participants do not seem to be aligned on the current focus of the Payroll Subgroup on implementing the NIST Cybersecurity Framework.[63] This situation could be suppressing active participation and engagement by the Payroll Community. Additionally, many smaller payroll providers are overwhelmed by the discussions since they lack internal cybersecurity and technical sophistication. Finally, there is little cohesion in the Payroll Subgroup. Unlike the income tax area, there has not yet been a face-to-face meeting of the Payroll Subgroup, which is critical to building trust.
- Other Work Groups & ISAC. The Payroll Community can also contribute to the efforts of other Summit Work Groups, including leads and scheme reporting that have crossover benefits to prevent IDTTRF in the income tax area.

The IRS needs a focused, short term effort to understand, prioritize and integrate the Payroll Community

The integration of the Payroll Community must be defined and scoped in a way that delivers a clear return on the IRS's investment of resources, money and time. This effort requires careful consideration but should be done quickly. Although there may be different approaches, ETAAC has some suggestions to accelerate the effort.

First, develop a better understanding of the Payroll Community, including its stakeholders, their roles, their risks and vulnerabilities and what they can bring to the IDTTRF prevention effort. Additionally, any team looking at this opportunity should identify or even create incentives for Payroll Community participation in and support for the Security Summit.

Second, build working relationships among Payroll Community participants and obtain Payroll Community senior executive support for the Security Summit. A face-to-face meeting of Payroll Community participants should occur to build trust and relationships. There has also never been a meeting of senior executives from the Payroll Community

---

Professionals that focused on reporting data thefts at payroll professionals' offices. However, the link to "report data theft" took the reader to a page captioned "data theft reporting process for tax professionals," which could confuse many employers and payroll professionals. (See https://content.govdelivery.com/accounts/USIRS/bulletins/20eb8dc#Sixth).

[62] For example, see https://www.irs.gov/individuals/how-do-you-report-suspected-tax-fraud-activity where the focus is on reporting traditional substantive tax or tax professional fraud, not on IDTTRF.

[63] The focus of the STAR Payroll Subgroup has been to follow the example of the STAR Tax Software Subgroup, which implemented selected NIST security controls over a three year period.

with IRS senior leadership to discuss the Security Summit, which was essential to the IRS gaining support from the income tax industry at the launch of the Security Summit. Now that the IRS is accepting applications from the Payroll Community for the Security Summit, ETAAC recommends that the IRS build these bridges and engage with executive leadership from the Payroll Community to build support. This is not intended to create a parallel Security Summit for the Payroll Community but, instead, get initial alignment and support for Payroll Community participation within the existing Security Summit.

Third, develop a basic plan by:

- Being clear on the most important outcomes for any integration.
- Creating a basic strategy with a limited number of elements, such as:
    - Executing an outreach campaign for the Payroll Community to increase its awareness of payroll-related IDTTRF schemes and how to prevent them.
    - Working with the Payroll Community to develop and implement a cybersecurity approach that responds to that industry's primary threats, potentially broken down by segment.
    - Developing a process to report payroll-related IDTTRF data breaches and schemes (not just W-2 phishing).
- Prioritizing the most important actions under each strategy element, including implementation timing.
    - Outreach could include developing messaging, web content and off-the-shelf tools, e.g., presentations for employees about spear phishing schemes and tip sheets for payroll employees about payroll-related IDTTRF indicators.
    - Cybersecurity could include applying the NIST Cybersecurity Framework to larger enterprises but shifting to outreach and education on the FTC Safeguards Rule for mid-sized and smaller enterprises.
    - Breach & scheme reporting could include creating an electronic mechanism to report data breaches or IDTTRF schemes to the IRS.

Fourth, move fast.

- One way for IRS to do this would be to create a temporary project team from Security Summit members to develop the above deliverables and an implementation plan/timetable. To support this, the IRS could:
    - Identify key groups that should be represented from among the IRS, states & industry.[64]

[64] Industry representativeness should include an employer payroll department, payroll processor and reporting agent (which should also reflect large and small organizations). It may be helpful to have some income tax companies with Security Summit and ISAC experience on the team to provide insights.

- Identify a limited number of knowledgeable, committed individuals who can and will make the time for this effort.
- Set a short time frame for the deliverable (e.g., 60 – 90 days) to avoid dragging out this effort. This deadline-driven approach is modeled after the IRS's approach when it kicked off the Security Summit in 2015 with a two-month to three-month deadline for initial deliverables.

Finally, in the Security Summit, the Payroll Community is currently concentrated in a subgroup of the STAR Work Group focused on cybersecurity. The Security Summit should consider whether the Payroll Community would be more rapidly integrated if it created a dedicated Payroll Work Group. The Security Summit took this approach previously by forming dedicated work groups for the Financial Services and Tax Professional communities.

Unless the IRS moves aggressively, the Security Summit will lose another year of effective Payroll Community engagement.

ETAAC has a final observation in this area. Currently, multiple IRS functions manage different aspects of the Payroll Community. The integration of the Payroll Community efficiently and effectively across the spectrum of IDTTRF and security issues will require close management and coordination. One IRS function should be responsible for coordinating and monitoring this effort across the IRS.

……

ISSUE: Financial Services Companies (FSCs) play a key role in the delivery of tax refunds, which provides them with unique insights into potential IDTTRF activities. These insights include timely threat intelligence, which IRS could use to enhance and adjust its IDTTRF screening filters, detect IDTTRF more effectively and reduce the current high rate of "false positives."[65] To the extent permitted by existing law, the IRS can enhance its information sharing and analysis by creating a "collaboration space"[66] where FSCs can share information that is not currently being shared across the ISAC membership.

RECOMMENDATION #5: ***Pilot a Financial Services Company (FSC) Collaboration Space in the ISAC***

The IRS should pilot a dedicated Financial Services Company (FSC) Collaboration Space in the ISAC to facilitate FSC information sharing in order to leverage their unique insights in identifying and preventing IDTTRF.

[65] "False positives" are legitimate taxpayers whose returns have been identified as suspicious and, for example, selected for further review under the IRS Taxpayer Protection Program (for elaboration, see supporting analysis for Recommendation #10 in this Report).

[66] A collaboration space would be a secure electronic area in the ISAC platform where FSCs can share IDTTRF-related information.

Support for Recommendation:

FSCs play a key role in tax administration

Almost three-quarters of the 154 million individual tax returns filed in 2018 resulted in a tax refund (approximately 112 million refunds worth $325 billion annually).[67] About 80% of refunds are direct deposited with the rest being delivered by mailed checks (which must eventually be cashed or deposited). Some of these refunds reflect the delivery of funds under important federal programs like the Earned Income Tax Credit and Additional Child Tax Credit.

FSCs facilitate the receipt, deposit and cashing of nearly all of these refunds. They also facilitate the opening of deposit and savings accounts, provide bank products and enable the receipt of refunds into those accounts and the disbursement of funds onto pre-paid cards or check issuance.

Simply put, FSCs provide the primary refund settlement vehicles for millions of taxpayers receiving refunds and play a key role in tax administration.

FSCs have a legal and business responsibility to monitor and report criminal and fraudulent activity, which aligns with IRS's interest in stopping IDTTRF

FSCs have both an obligation and an incentive to maintain robust fraud deterrent and identification programs.

First, federal laws set high standards of accountability for financial services companies, including a requirement for fraud deterrent and identification programs. The 2010 Dodd-Frank Act creates a framework of transparency and accountability. The 1970 Bank Secrecy Act (BSA) requires that national banks, federal savings associations, federal branches, and agencies of foreign banks have the necessary controls in place and provide the requisite notices to law enforcement to deter and detect money laundering, terrorist financing and other criminal acts and the misuse of our nation's financial institutions. The anti-money laundering clause of the 2001 USA PATRIOT Act holds banks accountable for opening accounts or lending money to terrorists.

Second, FSCs have a business obligation and incentive to protect the assets of their customers and shareholders. If it lacks a robust fraud detection and identification program, an FSC would be recklessly risking the assets of its customers and create a safety and soundness issue that would put it at risk of sanction or closure by regulatory authorities.

FSCs have long supported the IRS anti-fraud activities

FSCs are the last stop before fraudsters abscond with stolen refunds that have cleared the IRS's extensive fraud screening processes. The IRS data reflects that in the three most recently completed filing years, FSCs have helped the IRS recover over $1.3 billion in fraudulent refunds that may have otherwise been issued.[68]

---

[67] See Filing Season Statistics for Week Ending November 23, 2018 (https://www.irs.gov/newsroom/filing-season-statistics-for-week-ending-november-23-2018).

[68] See IRS IR-2018-21, released Feb. 8, 2018 (https://www.irs.gov/newsroom/key-irs-identity-theft-indicators-continue-dramatic-decline-in-2017-security-summit-marks-2017-progress-against-identity-

Before the Security Summit was even created, FSCs began engaging with the IRS to respond to potential fraudulent or criminal activity when they began detecting suspicious activity in connection with refund deposits. These early engagements resulted in hundreds of millions of dollars of suspicious refunds being returned to the IRS annually and enabled the IRS to conduct further taxpayer verification. These early collaborative efforts served as the foundation for the current IRS "External Leads Program" and as a demonstration of the benefits of public/private collaboration. Over time, with the external leads program in place, the IRS has expanded its reach by engaging more banks and states to participate in the effort.

This public/private collaboration has also identified other opportunities to fight IDTTRF. One opportunity involved situations where FSCs received direct deposits from the IRS or a state department of revenue that it could not accept.[69] Previously, the FSC would reject the deposit and transmit a NACHA[70] reject code back to the appropriate federal or state agency. Prior to the Security Summit, the IRS treated this type of rejection as a banking system error and, subsequently, mailed a paper check to the taxpayer. However, in connection with the Security Summit, a Financial Services Working Group (FSWG) was formed and determined that these rejects were potential indicators of IDTTRF. Further work by the FSWG resulted in the creation and standardization of the NACHA "R17" deposit reject code, which now represents a yellow flag for the IRS and states to take a second look at a specific taxpayer account before re-issuing any refund.

In another opportunity, the IRS has worked with an FSC to create a pre-refund verification process that enables IRS or state revenue agencies to check with the appropriate FSC electronically before the refund issues to determine if the FSC will accept the deposit. A successful pilot was conducted, and the IRS is currently considering how to expand this opportunity in connection with operation of the ISAC.

Unfortunately, legislative barriers block full FSC participation in the ISAC

Information sharing is a critical enabler in the fight against IDTTRF.[71]

Currently, individual FSCs share fraud-related information directly with the IRS outside of the Security Summit and ISAC. Then, under IRC Section 6103(k)(6), the IRS is permitted to share limited information back to the individual FSC relating to the suspicious activity that the FSC reported.

However, current laws restrict other important types of sharing among FSCs, the IRS and ISAC members (including the states). IRC Section 6103 restricts the IRS from

---

theft). The declining volume of recovered refunds is believed attributable to improved IRS IDTTRF screening processes that have resulted in fewer fraudulent refunds being issued over time.

[69] Examples: Name/SSN on the ACH might not match the name/SSN on the deposit account; the bank may already have the account flagged internally for reported fraud; or the account may be already closed.

[70] The National Automated Clearing House Association (NACHA) manages the development, administration, and governance of the ACH Network - the backbone for the electronic movement of money and data in the US.

[71] ETAAC has commented in this area before. In 2017, ETAAC recommended that the IRS identify and, where possible, mitigate the barriers affecting the IRS's ability to share vital IDTTRF information with the ISAC. In 2018, ETAAC highlighted the barriers presented by IRC Section 6103 and recommended that Congress amend the section to create a narrow IDTTRF disclosure exception.

sharing IDTTRF-related information received from an industry member beyond the party that provided the information in the first instance. IRC Section 7216 restricts ISAC tax industry members from sharing IDTTRF-related information with FSCs.

An FSC Collaboration Space could facilitate additional FSC information sharing in compliance with existing laws

There may be an opportunity to facilitate information sharing by FSCs "into" the ISAC and between FSCs within the ISAC without violating current restrictions on IRS and tax company sharing of information "out to" FSCs. The opportunity involves the creation of an FSC Collaboration Space as outlined below.

First, the IRS may be able to rely on existing requirements for FSCs to detect criminal or fraudulent activities. USA PATRIOT Act Section 314(b) permits financial institutions, upon providing notice to the Department of the Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity.[72] For example, physical account activity occurring in multiple locations over a very short period of time can indicate fraud and typically triggers further investigation by the FSC. Similar information, coupled with other FSC insights, could aid in spotting or verifying already suspect criminal activity.

Second, the existing ISAC platform could be used to create an FSC Collaboration Space to facilitate permitted FSC information sharing.[73] Then, within legally permitted authorities, the FSC-reported information could be used by the IRS, states and the ISAC Trusted Third Party to share FSC information out to the other ISAC participants, the Analysts Community of Practice and other key stakeholders.

Third, FSCs would not receive any information restricted from disclosure under IRC Sections 6103 or 7216.

Finally, Treasury Department regulations permit, but do not compel, FSCs to share suspicious customer activity under certain conditions. ETAAC believes that the collaborative engagement between FSCs within the FSC Collaboration Space would provide valuable insights to individual FSCs to help them improve their own internal controls. This benefit would be an incentive for new FSCs to participate in the FSC Collaboration Space and ISAC.

ETAAC believes the concept of an FSC Collaboration Space has merit. If successful, the pilot effort could be broadened to include additional FSCs.

II. IMPROVE SECURITY IN KEY AREAS OF OUR TAX SYSTEM

INTRODUCTION

The recommendations in Part II improve the security of our tax system.

[72] See https://www.fincen.gov/section-314b.

[73] For illustration, the collaboration space could be a secure FSC folder within the existing ISAC Participant's Space accessible to other FSCs participating in the ISAC, as well as to the Trusted Third Party, the IRS and participating states.

Recommendation #6 calls for assessments of the tax professional community to understand the state of information security practices and vulnerabilities. This assessment is foundational to the IRS's future efforts to improve security in this area, whether or not Congress grants the IRS authority to implement security standards.

Recommendation #7 reinforces ETAAC's 2018 recommendation that the IRS should have the authority to establish, implement and enforce minimum security standards in the tax area.

ISSUES & RECOMMENDATIONS

……

ISSUE: Hundreds of thousands of tax professionals are a growing target for cybercriminals seeking high-quality taxpayer information, but there is an incomplete understanding of their current security posture and risks. At the same time, it appears that the IRS lacks the clear authority to establish and enforce information security standards in the areas of its jurisdiction. The IRS must research the security posture and risks of the tax professional community to enable it to guide and prioritize its efforts to improve the information security of tax professionals and reduce their information security vulnerabilities. Additionally, Congressional action is necessary to protect taxpayers from identity theft by granting the IRS the authority to establish and enforce security standards, as well as providing adequate funding for this responsibility.

RECOMMENDATION #6: *Assess the state of information security practices in the tax professional community*

In collaboration with the Security Summit, the IRS should develop and execute a plan for ongoing research on the state of information security practices and vulnerabilities in the tax professional community.

RECOMMENDATION #7: *Grant the IRS the authority to establish and enforce security standards*

Congress should grant IRS clear legal authority to develop, implement and enforce appropriate information security standards and practices in the area of tax administration, which would include establishing administrative, technical, and physical safeguards, implementing required education and training, and providing ongoing guidance.[74]

[74] The language in this recommendation parallels the provisions of GLB Section 501(b), which provides, in part, that the responsible agencies shall "establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." GLB Section 501(b) is the legislative authority for the FTC Safeguards Rule.

Support for Recommendations:

ETAAC has made past recommendations to improve tax professional security

Cybercriminals are smart, persistent and constantly probing for the weakest link. They have been increasingly targeting tax professionals who hold valuable taxpayer information. Most recently, the IRS reported a 29 percent annual increase in the number of data thefts reported by tax professionals through November 5, 2018.[75]

ETAAC has been aware of this growing threat and made recommendations to improve tax professional security in both its 2017 and 2018 reports.

Our 2017 recommendations focused on increasing tax professional awareness of the threat and improving IRS guidance on the implementation of security programs, e.g., clarifying key security publications, providing clearer and more actionable guidance, increasing tax preparer awareness of continuing education credits for security programs, and amending Circular No. 230 concerning taxpayer information security.[76] The IRS has made progress in improving certain publications and implementing a communications program to raise tax professional awareness.

Our 2018 recommendations extended our focus beyond building awareness and looked for approaches that might lead to action by tax professionals, e.g., establishing a common security standard and the IRS's enforcement authority, requiring security continuing education, building tax professional accountability and engagement, and establishing clear IRS internal responsibility for tax professional security.[77]

There has been limited progress on our 2018 recommendations in this area. We believe there are several reasons for this situation, including the implementation of a major tax law change, a government shutdown, competing priorities and IRS resource limitations. However, we also believe the most important reason is a concern that the IRS lacks the clear legal authority to set requirements in this area even with respect to something as basic as requiring security education.

The end result is to leave taxpayer information more exposed to cybercriminals than it should or needs to be.

IRS's current limitations foster cybersecurity risks in the tax area

Given questions about its legal authority, the IRS has had to rely principally on more traditional "one-way" outreach and education approaches to influence tax professionals to implement information security programs. The three primary approaches have been: (i) press campaigns with news releases such as the IRS's "Don't Take the Bait" and "Protect Your Clients, Protect Yourself" campaigns, (ii) communications through established email distribution channels for e-file providers and tax professionals, and (iii) security programs offered at annual IRS Tax Forums. The primary objective of these initiatives has been to increase awareness and provide guidance on information security

[75] See https://www.irs.gov/newsroom/irs-security-summit-partners-warn-tax-professionals-of-high-risk-of-data-theft-attacks.

[76] ETAAC 2017 Report, Recs. #17 - #19, pps. 41–44.

[77] ETAAC 2018 Report, Recs. #5 - #10, pps. 19–31.

practices with the ultimate goal of causing tax professionals to implement effective security programs.

ETAAC has supported these efforts and even offered recommendations to improve them. Now, however, ETAAC realizes the current approach is inadequate. While IRS outreach and education programs are vital, ETAAC believes that the IRS cannot "communicate" its way to a more secure tax professional community.

Program evaluation and measurement must be part of key IRS security initiatives

It is important to determine the effectiveness of IRS security initiatives whether they involve outreach, education, guidance, tools or implementation. Critical IRS security initiatives should be designed with program evaluation in mind. The IRS cannot afford to be spending valuable resources on major efforts that are not producing results.

There are well-known models for designing public service campaigns with this in mind. One illustration is the Ad Council.[78] In its Overview of Ad Council Research & Evaluation Procedures, the Ad Council references its conduct of "qualitative and quantitative research to guide the strategic and creative development of our campaigns" and notes that program evaluation is a critical component of every campaign.[79]

Another element of program evaluation is identifying key process and output metrics for the effort. One conceptual approach in this area is the "Theory of Change," which is a description of how and why a desired change is expected to happen. The Center for the Theory of Change refers to this as "filling in the middle."[80]

Specifically, any program should be designed so that one can measure specific indicators of action taken (process metrics) and the achievement of the desired end result (outcome metrics). These indicators demonstrate both progress towards the goal, as well as its achievement. The table below provides some illustrations of possible process or output metrics.

Desired Action or Result	**Process or Output Metric**
Increase awareness of cybersecurity threat	# people watching IRS YouTube programs # people attending IRS-approved security training # social media posts/news stories on topics generated by IRS
Communicate requirement for having security program	# of people receiving IRS email # of people opening/reading IRS email

[78] See https://www.adcouncil.org/Impact/Research/Overview-of-Ad-Council-Research-Evaluation-Procedures (Overview of Ad Council).

[79] "In order to assess a campaign's impact, we conduct research that encompasses a dashboard of indicators, including media exposure, consumer response, website analytics, and national pre- and post-tracking surveys that measure awareness, attitudinal and behavioral shifts among the target audience." See Overview of Ad Council.

[80] See https://www.theoryofchange.org/what-is-theory-of-change/

Communicate security program design and implementation guidance	# of people downloading initial or detailed guidance
Tax professional implementation of security programs	# people attending IRS-approved security training # reports of system breaches reported to IRS # tax professionals implementing security program # tax professionals obtaining cybersecurity insurance

Program evaluation is not easy to perform and requires resources. Not every security initiative has a sufficient impact to warrant this investment of effort, but some do. Otherwise, the IRS is just putting resources into an effort that may sound good but, in reality, has little or no impact. IRS should work with Security Summit members to develop pilots to identify promising practices and enable the IRS to build its know-how in this area.

The IRS must assess and understand the current state of tax professional security

Currently, there is no clear understanding of the state of affairs in tax professional security. This gap in understanding lends itself to "one size fits all" solutions that will fail to achieve the desired outcome of improving tax professional security.

To target and design effective programs, the IRS must understand the structure of the tax professional community, the nature of its tax practices, the current state of any security practices and primary vulnerabilities. Hypothetically, there may be different segments in the tax professional community that warrant higher levels of attention and different approaches. For example, large national and regional accounting firms likely have more sophisticated information security programs. Similarly, local offices of large national tax preparation firms (whether company-owned or franchisees) are likely subject to more sophisticated centrally managed information security programs. On the other hand, smaller tax practices may be in a different situation, and lack both the resources and technical sophistication to implement effective security programs.

Based on its research, the IRS might also decide to develop guidance or requirements based on the role that tax professionals or their firms play in electronic filing rather than their tax preparation role. For example, certain requirements might apply to Electronic Return Originators,[81] but not to individual preparers.

The IRS needs to close the gap by executing a research effort to guide its future decisions. The effort will require the engagement of experienced research professionals, and may require OMB clearance for any necessary surveys.

[81] For the definition and role of an ERO, see IRS Pub. 3112 (See https://www.irs.gov/pub/irs-pdf/p3112.pdf).

The IRS needs the authority to establish security standards in the tax area

ETAAC has previously reported two important limitations in existing security standards as applied to the tax area. First, the FTC Safeguards Rule does not apply to the business tax area given the limited focus of the Gramm-Leach-Bliley Act (GLB). Second, the IRS has no enforcement authority under the FTC Safeguards Rule.

ETAAC believes that the tax professional community needs a basic security standard that covers both the individual and business tax filing areas and is enforceable by the IRS.

In 2018, we recommended investigating the application of the FTC Safeguards Rule across both the individual and business tax professional communities, and granting IRS enforcement authority of that Rule. Our 2018 Report focused on the potential of leveraging the Safeguards Rule for three primary reasons: (i) it was developed through a rigorous regulatory process; (ii) it already applies to tax professionals serving individual consumers; and, (iii) it is sufficiently flexible to be adapted across a broad spectrum of tax professionals – from sole practitioners to regional tax firms to national tax firms.

Although we still believe that a security standard comparable to the FTC Safeguards Rule is a good first step, ETAAC suspects it may not be feasible or preferable to try to dovetail IRS into a regulatory framework currently managed and enforced by another agency, i.e., the FTC.

Given that, ETAAC now recommends that Congress grant to the IRS the independent legal authority to develop, implement and enforce appropriate information security standards and practices in the tax administration area.

Recent legislative proposals responding to calls for the IRS to have oversight authority for preparers may not adequately address this topic. For example, a recent Senate bill provided the IRS with the authority to set minimum competency standards, but did not appear to extend to the IRS the authority to develop, implement and enforce security standards.[82]

As a side note, the IRS must determine the best way to organize around this challenge. As noted in our 2018 Report, ETAAC believes that the IRS needs a "single owner" and that tax professional information security should not be based on whether someone is a CPA, EA, Attorney or unenrolled preparer.[83] They are all tax professionals holding taxpayer information that is at risk. We have concerns about the efficiency of the IRS managing tax professional security by distributing this responsibility within its existing organizational structure that manage the various categories of tax professionals, e.g., preparers, practitioners, VITA volunteers and EROs.

ETAAC's characterization of a "single owner" refers to the designation of a specific IRS organization (existing or new) which would be responsible for working with current IRS

[82] Section 2 "Regulation of Tax Return Preparers," Senate Bill S. 1192 – Taxpayer Protection and Preparer Proficiency Act of 2019 introduced into the 116th Congress (2019-2020). (See https://www.congress.gov/bill/116th-congress/senate-bill/1192/text)

[83] See ETAAC 2018 Report, Recommendation # 10, p. 31.

functions responsible for the tax professional community to facilitate the development and execution of a cohesive, coordinated tax professional security strategy. (Note: ETAAC is aware of the just-issued GAO Report entitled "Taxpayer Information: IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices" (GAO-19-340; May, 2019), which was unable to be reviewed and discussed by the collective ETAAC membership before the deadline to finalize its 2019 Annual Report to Congress.)

Finally, any Security Summit initiative(s) to improve tax professional security should involve and be coordinated across relevant work groups, e.g., STAR, Communications and Tax Professionals Work Group.

III. PROTECT & ENABLE TAXPAYERS

INTRODUCTION

The recommendations in Part III protect and enable taxpayers.

Recommendations #8 and #9 improve the accessibility and operation of the IRS's identity proofing and authentication platforms by expanding the availability of non-digital alternatives and collaboratively identifying, testing and piloting evolving approaches to identity proofing and authentication.

Recommendation #10 calls for the IRS to collaborate with its Security Summit partners to identify improvements to the Taxpayer Protection Program taxpayer experience.

ISSUES & RECOMMENDATIONS

……

ISSUE: Taxpayers must be able to prove their identity before gaining initial access to IRS services containing sensitive taxpayer information. At the same time, digital identity proofing and authentication is a rapidly evolving and challenging area. To respond to the challenges and barriers associated with digital identity proofing, the IRS needs to expand the availability of identity proofing to alternative non-digital channels and should regularly engage with state and industry experts to gain ongoing insights.

RECOMMENDATION #8: ***Develop and expand channels for identity proofing***

The IRS should (i) continue its current efforts to implement digital identity proofing protocols compliant with NIST Special Publication 800-63-3 Digital Identity Guidelines, and (ii) identify and develop opportunities to expand the availability of identity proofing mechanisms in other channels including the implementation of an IRS trusted third-party identity verification program.

RECOMMENDATION #9: ***Collaborate with Security Summit members to identify and pilot emerging approaches for identity verification***

The IRS should engage regularly with subject matter experts from Security Summit members to identify and potentially pilot emerging technologies or approaches to verify identities across all channels.

Support for Recommendations:

Effective and accessible identity proofing is a condition for secure IRS electronic services

The IRS must continue to supplement its existing service channels with secure IRS digital and mobile services to meet taxpayer needs and expectations. The critical first step for users of these services is successful identity proofing.

As described in our 2018 Report, identity proofing is the process by which the IRS collects, validates and verifies information about a person to ensure the applicant is who they claim to be to a stated level of confidence.[84] Historically, identity proofing was accomplished telephonically or in-person, because most services were delivered in these channels. The advent of electronic services introduced a third method of identity proofing, typically referred to as "digital" identity proofing.

By contrast, authentication is the process of determining the validity of one or more authenticators used to claim a digital identity previously issued based on successful identity proofing. Successful authentication provides reasonable risk-based assurances that the person accessing the service today is the same person who accessed the service previously. (For ease of understanding, ETAAC may occasionally use the term "identity verification" to refer to identity proofing and/or authentication.)

The IRS's current digital identity proofing platform is Secure Access, which requires a series of steps to successfully complete the identity proofing process as a condition to accessing the desired service or application.[85] The IRS's Secure Access protocol is relatively standard and appears to meet or exceed the practices of state departments of revenue.[86] Taxpayers engaging with financial institutions, and increasingly with other types of online services (e.g., email accounts), are presented with multi-factor identity

[84] See ETAAC 2018 Report, pps. 39-40. See also the NIST SP 800-63 *Digital Identity Guidelines* at https://pages.nist.gov/800-63-3/.

[85] Generally, the user provides personal information, validates his/her email address, confirms personal financial information and verifies his/her cell phone. See https://www.irs.gov/individuals/secure-access-how-to-register-for-certain-online-self-help-tools.

[86] ETAAC engaged with several state revenue agencies to determine their current practices. The federal government is also attempting to develop a government identity proofing platform called Login.gov. At this stage, Login.gov is relatively new and still being proven out (see https://login.gov/). See also articles from Federal News Network on January 9, 2017 (https://federalnewsnetwork.com/reporters-notebook-jason-miller/2017/01/ups-downs-continue-gsa-18fs-identity-management-effort/), DigitalGov on August 28, 2017 (https://digital.gov/2017/08/28/government-launches-login-gov-to-simplify-access-to-public-services/) and Nextgov on December 26, 2017 (https://www.nextgov.com/cybersecurity/2017/12/gsa-needs-verify-whos-logging-logingov/144823/).

proofing models that operate based on some combination of personal information, shared secrets, publicly available information and confirming communications.

Digital identity proofing presents significant challenges

Digital identity proofing requires a deep understanding of the taxpayer and presents its own set of challenges in the current cybersecurity environment, as described in recent IRS testimony before House Ways and Means.[87]

First, taxpayers may not have public financial information or cell phone accounts in their names (or, in some cases, at all) as sources of validating information. For these and other reasons, the IRS advised ETAAC that only about 40% of taxpayers successfully complete Secure Access.[88] Tax professionals have a slightly higher success rate in using Secure Access to identity proof themselves -- approximately 65%. This higher success rate may be because tax professionals are more likely to have the validating sources of information, or are more comfortable completing the identity proofing process. In any case, the numbers show that not everyone can digitally identity proof.

Second, as previously noted, criminals have compromised a significant amount of personal information from both government and private data sources.[89] They have the answers to the "private" questions posed to taxpayers.

Third, identity proofing technologies are rapidly evolving as the criminals improve their tactics. For example, several companies offer identity verification platforms that leverage biometric features such as fingerprints, faces, iris and palm recognition.[90] It is a challenge for government agencies to stay current with, and for consumers to comprehend, rapidly evolving identity proofing technologies presented to them.

Finally, as criminals get better, the bar for government agencies goes higher. The recently issued NIST Special Publication (SP) 800-63-3 Digital Identity Guidelines have increased the requirements for identity proofing. For example, the IRS may need to implement new types of digital identity proofing that require biometric features or other "liveness checks."

Implementing the NIST SP 800-63-3 requirements is a major undertaking

We should not underestimate the challenge of implementing NIST SP 800-63-3 guidelines.

These new guidelines allow more taxpayers the opportunity to prove who they say they are through digital transactions and allow for increased reliability in the identity established for returning users through continuous authentication processes. However, the new requirements are also more rigorous and require additional identity verification and authentication steps.

---

[87] For video of this Hearing, see https://www.congress.gov/committees/video/house-ways-and-means/hswm00/_1SQHj7iOyE.

[88] In her 2017 Annual Report to Congress, the Taxpayer Advocate reported Secure Access verification rates of 30% in calendar year 2017. See Most Serious Problem #3, page 42.

[89] See the Current Environment for IDTTRF and Cybersecurity section of this Report.

[90] See for example MorphoTrust (http://www.morphotrust.com/identix.aspx), and ID.me (https://www.id.me/business/digital-identity).

As a result, the new NIST SP 800-63-3 guidelines will be more expensive to implement and maintain. Associated costs will include the transition to the new guidelines, the increasing adoption of taxpayers over time (as well as the associated transaction costs for identity assurance, authentication assurance and federation), and the ongoing maintenance of IRS systems to counter the ever-increasing sophistication of cybercriminals.

A principal challenge presented by NIST SP 800-63-3 is the tension between improving cybersecurity while, concurrently, improving the customer experience.

The IRS is taking a deliberate approach to comply with new NIST guidelines

The IRS has made effective digital identity proofing a priority. It is part of the IRS Strategic Plan (FY2018 – 2022), which calls for the IRS to drive increased agility, efficiency, effectiveness and security in its operations.[91] One element of this effort is the safeguarding of taxpayer data, including the continued development of authentication, authorization and access abilities as a foundation for its move to digital services. The IRS also has an Identity Assurance (IA) Strategy and Roadmap, which includes a focus on digital identity proofing.[92]

The IRS has taken a proactive, deliberate and collaborative approach to implement the NIST SP 800-63-3 guidelines.

The IRS has actively contributed to the NIST SP 800-63-3 guidelines and the forthcoming OMB Directive that will supersede OMB Memorandum 04-04. It has also been involved in the iterative development and application of the NIST requirements and provided comments to OMB.

The IRS has developed a systematic and comprehensive approach to implement the new NIST SP 800-63-3 guidelines. It is carefully reviewing the requirements specific to each section of the guidelines, breaking down each of the requirements, and conducting a digital identity risk assessment process to enable the consistent selection of appropriate identity and authentication assurance levels across IRS applications and transactions.

The IRS has also taken a collaborative approach to this effort. It has proactively engaged with NIST throughout the process to validate its understanding and interpretation of the guidance and requirements, and has retained NIST SP 800-63-3 authors to serve in an advisory role to IRS staff. It has also engaged with numerous federal agencies including the Treasury Department, Social Security Administration (SSA), U.S. Postal Service (USPS), Department of Agriculture (USDA), Digital Service, General Services Administration and the Centers for Medicare & Medicaid Services (CMS). These engagements have included monthly meetings with SSA, USPS and USDA, as well as hosted face-to-face working sessions with SSA, USPS and CMS. The IRS has also engaged with state revenue agencies and the tax software industry through the Security Summit on the topic of identity assurance.

[91] See https://www.irs.gov/pub/irs-pdf/p3744.pdf

[92] See GAO Authentication Report, pps. 52-53.

However, the IRS cannot overly rely on digital identity proofing, and must expand its identity proofing alternatives

The IRS is working hard to develop enhanced, compliant identity proofing platforms. But, given the challenges of digital identity proofing (especially after new requirements are added to comply with current federal requirements), many taxpayers will still have difficulties or not be able to complete the digital identity proofing process successfully. As a result, many taxpayers will need an alternative channel to be identity proofed.

The IRS recognizes the diverse needs of its taxpayers, and has advised ETAAC that it is looking closely at alternative options for identity proofing and authentication. It is also looking at several alternatives with which to implement cross-channel identity proofing, e.g., a taxpayer identity proofs in-person in order to be granted access to online services accessible through irs.gov.

For example, the IRS is evaluating the use of its 300+ Taxpayer Assistance Centers (TACs) to conduct in-person identity proofing. However, the IRS would need to improve TAC availability, e.g., create special service lines and expand operating hours to accommodate working taxpayers. Another challenge is the fact that TACs generally work by appointment, which might take weeks – or even months -- to obtain.[93] IRS might also consider leveraging other agencies with large physical footprints, such as the SSA and USPS.

ETAAC reaffirms its recommendation for the IRS to consider creating third-party in-person identity proofing services

In its 2018 Report, ETAAC recommended that the IRS evaluate a trusted third-party identity proofing program to expand its physical footprint and increase taxpayer convenience. We mentioned the precedent of the Certifying Acceptance Agent (CAA) Program for the issuance of ITINs.[94]

Participation in an identity proofing agent program could follow the model currently used by the CAA program with any necessary modifications.[95] Generally, the agent enrollment process would include:

- An Application to Participate in the IRS Acceptance Agent Program, including a fingerprint card.
- Completion of mandatory training and the issuance of an applicable certification.
- The passage of background checks and tax compliance checks.

Existing CAAs might have an expedited process to become identity agents. As with the current CAA program, participation would not be limited to paid practitioners but could

[93] See National Taxpayer Advocate 2018 Annual Report to Congress (Taxpayer Advocate 2018 Report), Vol. One, pps. 87-88, discussing taxpayer challenges getting timely TAC appointments.

[94] State notary programs provide another illustration of third-party identity proofing services. Notary programs generally have age limits and residency requirements, and may require a specified course of study, written examination and background checks.

[95] See https://www.irs.gov/individuals/new-itin-acceptance-agent-program-changes.

include financial institutions, state agencies, and volunteers with the IRS Volunteer Income Tax Assistance (VITA) and IRS Low Income Taxpayer Clinic (LITC) programs.

Of course, the IRS would need to develop a method of connecting the in-person identity proofing process to its online services. There are a variety of possibilities. Rather than develop and implement this type of program in one fell swoop, we would support any IRS decision to start with a small pilot with trusted third-party participants to determine the integrity and effectiveness of such an approach.

Importantly, the IRS would need additional funds to increase any staffing of the IRS department handling any new responsibilities in this area.

The IRS should also leverage Security Summit membership to brainstorm and pilot other ideas for identity proofing and authentication

There is also an opportunity to collaborate with the Security Summit state and industry experts to brainstorm other ID proofing opportunities – whether digital, telephonic or in-person. In particular, some states and industry have actively worked to develop and pilot identity proofing models and developed insights that would benefit the IRS.[96]

A recurring engagement would be consistent with those elements of the IRS's Identity Assurance Roadmap[97] calling for repeatable environmental scans and collaboration in this area, and be responsive to GAO's call for a "comprehensive, repeatable process to identify and evaluate potential new authentication technologies and approaches."[98] Another potential benefit of this type of collaboration would be the creation of more consistent identity proofing protocols at the federal and state level, which would be less burdensome on taxpayers and other stakeholders.

Additionally, the IRS has indicated that conducting proofs-of-concepts and pilots of potential solutions is an important step in the development process. ETAAC agrees with this approach.

Finally, the launch of any new IRS identity proofing solution should be considered the equivalent of a product launch and accompanied by a robust IRS communications and education "launch plan" beyond just the issuance of press releases. For example, subject to security considerations, the IRS could provide YouTube videos to set taxpayer expectations and ensure they understand the kind of information they may need. Security Summit members can also help communicate any new services.

[96] Alabama is one state that has done extensive work in this area (See https://www.alabamaeid.com/).

[97] See GAO Authentication Report, Appendix II.

[98] See GAO Authentication Report, p. 33.

……

ISSUE: The Taxpayer Protection Program (TPP) plays a key role in mitigating the impact of IDTTRF on legitimate taxpayers. There are opportunities to find ways to increase the number of taxpayers responding timely to IRS communications in this area.

RECOMMENDATION #10: ***Engage with the Security Summit to improve the Taxpayer Protection Program's taxpayer experience***

The IRS should collaborate with Security Summit and ISAC members to identify actions to increase the number of legitimate taxpayers timely responding to Taxpayer Protection Program communications.

Support for Recommendation:

The Taxpayer Protection Program benefits most taxpayers, but has its challenges

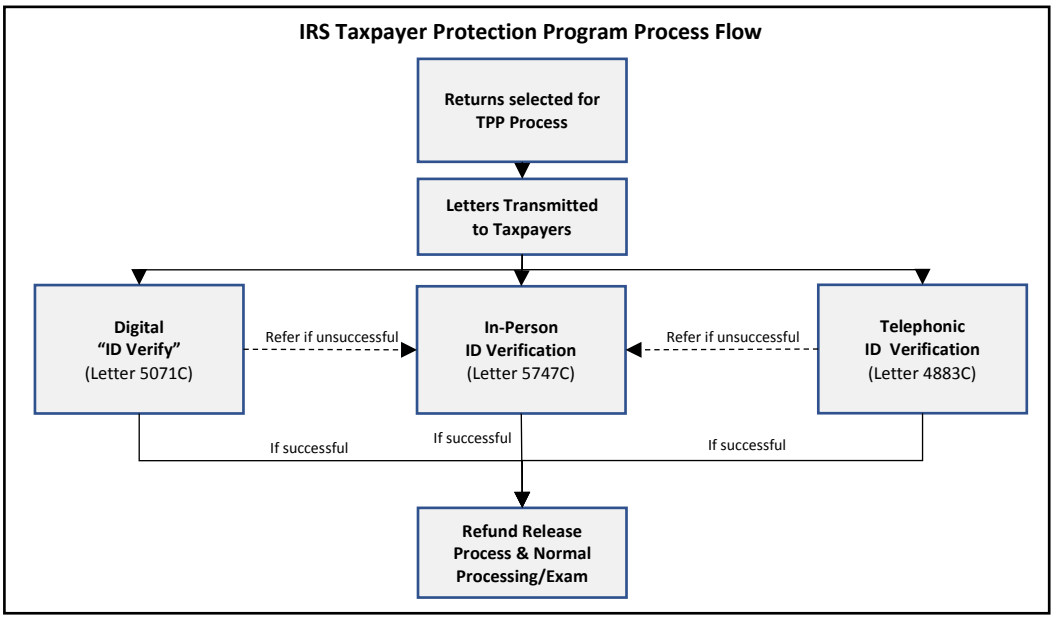
The wholesale theft of huge volumes of detailed personal information has fueled IDTTRF and makes it difficult for the IRS to distinguish fraudulent from legitimate returns.

In response, the IRS has taken numerous actions, including investing in IDTTRF strategies and tactics focused on identifying potential IDDTRF before returns are processed and refunds issued. One such IRS initiative is the Taxpayer Protection Program. The premise of the Taxpayer Protection Program is to screen returns for IDTTRF indicators early in the IRS's return submissions process and engage with taxpayers then, instead of processing suspicious returns and relegating victimized taxpayers to the more burdensome ID Theft Affidavit process.[99]

The Taxpayer Protection Program generally involves four functional steps (see below graphic):

1. Identifying, removing and holding suspicious returns from the normal processing flow,
2. Notifying the affected taxpayers by mail that they must take further action to authenticate themselves and clear their return,
3. Providing multiple mechanisms (digital, telephonic or in-person) for legitimate taxpayers to authenticate themselves and their returns, and
4. Completing the processing and refund issuance for taxpayers who have successfully authenticated their returns.

[99] In connection with our review, ETAAC reached out to several states to better understand their equivalent processes. There were some differences but, generally, the IRS's Taxpayer Protection Program approach and taxpayer experience are consistent with state practices.



As reported by TIGTA, about 2 million returns are selected for the Taxpayer Protection Program, which is just over 1% of all individual returns.[100] Unfortunately, the Taxpayer Protection Program is not without its challenges.

One of the biggest challenges for the Taxpayer Protection Program is the relatively high "false positive" rate. Currently, approximately 65% of the returns selected for the Taxpayer Protection Program are later determined to be legitimate taxpayers.[101] Although this number seems (and is) high, some industry participants in the Security Summit thought this rate was not surprising given the nature and volume of IDTTRF in the income tax space. Again, the criminals have very precise and accurate taxpayer information so it is no surprise that legitimate taxpayer returns are being selected.

The IRS could reduce this false positive rate by increasing the score used to select returns into the Taxpayer Protection Program. However, that decision could trigger two adverse consequences: (i) increase the number and amount of fraudulent refunds, and (ii) increase the number of taxpayers having a fraudulent return processed in their name, which would subsequently subject them to the more onerous and time-consuming ID Theft Affidavit process after they file their legitimate return.

Another challenge for the Taxpayer Protection Program is the relatively high rate of "non-responders," which is on the order of 30% of all returns selected for the program.[102] It is difficult to understand why a legitimate taxpayer with a refund due them would not promptly contact the IRS upon receipt of a TPP letter. For that reason, the IRS categorizes a non-responder as confirmed IDTTRF. However, ETAAC has anecdotally identified use cases where non-responders may be legitimate taxpayers,

[100] See TIGTA Report: The Taxpayer Protection Program Includes Processes and Procedures That Are Generally Effective in Reducing Taxpayer Burden (October 17, 2018) (TIGTA Taxpayer Protection Program Report)

[101] See TIGTA Taxpayer Protection Program Report. The Taxpayer Advocate 2018 Report puts this figure at 63% (see p. 79).

[102] One state reported that its non-responder rate was comparable.

e.g., military members who frequently move and never received the IRS's letter, and non-English speakers who may not understand the IRS letters.

The Taxpayer Protection Program has the potential for an improved taxpayer experience

At the IRS's request, ETAAC has reviewed the Taxpayer Protection Program to identify possible improvements to the taxpayer experience under the Program.

Despite its challenges, ETAAC still considers the Taxpayer Protection Program to be a reasonable approach given the alternatives. However, there may be opportunities to increase the response rate of legitimate taxpayers and, thereby, improve their experience with the Program.

Response rates by legitimate taxpayers seem to rest on four steps for the taxpayer: (i) receipt of the IRS communication; (ii) opening and reading the communication; (iii) understanding the situation and options; and, (iv) successful authentication.

Although there is no silver bullet, each of these steps may have opportunities that, collectively, would have a material impact on response rates (examples below).

- Send second letters to taxpayer groups that frequently move and may have missed Taxpayer Protection Program communications, e.g., active military.
- Find ways to provide back-up communications through other platforms, e.g., MeF, Where's my Refund and the IRS.
- Evaluate IRS envelopes to reduce taxpayer anxiety or confusion. In some cases, taxpayers are frightened by IRS communications, which may cause them to be ignored. In other cases, government communications may be discarded because they look like junk mail given the number of mailings that try to resemble "official" government communications.
- Review communications for potential clarifications. In particular, taxpayers with English as a second language may not understand the TPP guidance.[103]
- Review alternatives to digital identity proofing, which is currently required to access the TPP "ID Verify" platform.[104]

[103] IRS has organized several working groups to gather feedback on Taxpayer Protection Program communications since 2014, including an engagement with the Taxpayer Advocacy Panel in 2017 to conduct a thorough review of the language in the Taxpayer Protection Program letters.

[104] The supporting analysis for Recommendations #8 and #9 in this Report describe some of the challenges that taxpayers face in successfully completing IRS's Secure Access identity proofing platform, which is the front-end to the TPP's ID Verify system.

Security Summit members have insights into potential improvements in the Taxpayer Protection Program

There are opportunities to collaborate within the Security Summit to leverage state and industry insights and resources to support or enhance the TPP. In addition to the items outlined above, state or industry members may have valuable insights around:[105]

- Backing up primary Taxpayer Protection Program communications by leveraging tax professionals or tax software. For example, in the "Confirmed IDT Fraud" files[106] provided to industry members, the IRS could identify those returns for which the taxpayer was a "non-responder." This information could be used by the industry member to determine whether the non-responder is, in fact, a legitimate taxpayer and reach out to assist them.
- Helping IRS identify techniques to distinguish legitimate Taxpayer Protection Program non-responders in high-risk categories such as the military, e.g., flagging returns associated with active duty Forms W-2 from Defense Finance and Accounting Services (DFAS) or using physical or IP addresses located on military bases.
- Creating direct mail communications that drive higher open and response rates.
- Developing common definitions and metrics for Taxpayer Protection Program-related processes to create a common understanding across the Security Summit, e.g., confirmed IDTTRF, non-responders, etc.

Several of the above ideas align with the recommendations in the Taxpayer Advocate's 2018 Report relating to (i) developing common metrics and setting appropriate targets, (ii) studying why it takes some taxpayers longer to authenticate their identities and what barriers they may encounter when attempting to do so, and (iii) requesting insights from outside parties on ways to reduce false positives and non-responders.[107]

In conclusion, the Taxpayer Protection Program is a reasonable approach to a difficult challenge. However, given the relatively large number of legitimate taxpayers adversely affected by the current process, the IRS should work with the Security Summit to identify improvements to increase the likelihood that legitimate taxpayers will respond to Taxpayer Protection Program communications.

---

[105] ETAAC appreciates that IRS must also consider the feasibility of back-up communications and balance the risk that any additional or ancillary communications might be going to the criminal who originated the return and not to the legitimate taxpayer.

[106] The Confirmed IDT Fraud file provided by IRS contains those returns filed through that industry partner that IRS believes are IDTTRF returns. Currently, that file would include non-responders as "confirmed" IDTTRF. However, we know that a sizeable number of non-responders are legitimate taxpayers.

[107] See Taxpayer Advocate 2018 Report, Volume One, Most Serious Problem #5, pps. 79-90.

Appendix A

About ETAAC

The Electronic Tax Administration Advisory Committee (ETAAC) was formed and authorized under the Internal Revenue Service Restructuring and Reform Act of 1998 (RRA 98). The historical charter of ETAAC was to provide input to the Internal Revenue Service on electronic tax administration.

ETAAC's responsibilities involve researching, analyzing, and making recommendations on a wide range of electronic tax administration issues. Additionally, pursuant to RRA 98, ETAAC reports annually to Congress concerning:

- The IRS's progress on reaching its goal to electronically receive 80% of tax and information returns;
- Legislative changes assisting the IRS in meeting the 80% goal;
- Status of the IRS strategic plan for electronic tax administration; and
- Effects of e-filing tax and information returns on small businesses and the self-employed.

In March of 2015, the IRS assembled a coalition of IRS, tax industry and state revenue agency leaders to undertake a major initiative to combat IDTTRF by creating what has become the IRS Security Summit.

The ETAAC charter was amended in 2016 to expand ETAAC's focus to address the serious problem of IDTTRF, which was threatening to erode the integrity of the tax system. In this and future reports, ETAAC will continue to reflect this expansion of focus to provide strategic and tactical recommendations on combating IDTTRF and improving information security.

ETAAC expanded its authorized size to eighteen members to broaden the experience of its members and add new stakeholder perspectives from the government, commercial, non-profit and consumer sectors. ETAAC members come from state departments of revenue, large tax preparation companies, low-income and consumer advocacy groups, solo tax practitioners, tax software companies and the financial services industry. (See Appendix B for ETAAC member biographies.)

In conducting its assessments and formulating its recommendations, ETAAC relies on a variety of information sources. Most importantly, ETAAC participates in numerous discussions with IRS representatives and Security Summit participants. Many of the ideas that ETAAC has incorporated into its recommendations arose in these discussions and are already being considered or acted upon by the Security Summit Work Groups.

ETAAC also reviews reports from a variety of sources, including other advisory boards, the National Taxpayer Advocate, the Government Accountability Office (GAO), and the Treasury Inspector General for Tax Administration (TIGTA). The Committee is most grateful for their observations. On occasion, ETAAC may also seek background insights from policy leaders, industry and state revenue agencies as well as other experts.

Then, ETAAC members use this information and these insights to develop the ETAAC's annual report in a highly collaborative and rigorous deliberation and drafting process. Any recommendations and opinions expressed in this report are solely those of ETAAC.

ETAAC recognizes IRS employees and leadership for their continued efforts to administer an increasingly complex tax system, meet taxpayer service expectations, improve cybersecurity, fight IDTTRF and successfully process billions of transactions and hundreds of millions of tax returns. The United States tax system could not operate without their dedication, commitment, and talent. IRS employees and managers have made themselves available during the filing season and on other occasions to brief ETAAC on a variety of issues. We are most grateful for their thoughtful and candid insights essential to the preparation of this report.

Public comments on this report may be sent to publicliaison@irs.gov.

Appendix B

ETAAC Member Biographies

John Ams - Mr. Ams has over 40 years of experience in the federal tax arena with expertise providing legislative and regulatory representation in accounting and federal tax matters to a variety of constituencies including individuals, non-profit organizations, and corporations. He served as the Executive Vice President and Chief Operating Officer of the National Society of Accountants in Alexandria, VA from 2001 to 2018. At NSA, a professional society whose members practice in the areas of accounting and taxation, he was responsible for all operations and provides information, education and guidance to his membership regarding tax legislation, tax and accounting regulations, and administrative concerns. He has presented testimony to IRS and Congress on numerous occasions and served as a member of the IRS Advisory Council from 2012-14, where he was the 2014 chair of the Professional Responsibility Subgroup. Mr. Ams is a Certified Association Executive, a member of the D.C Bar Association, and a member of Phi Beta Kappa. He holds a J.D. from the Georgetown University Law Center and a BA, magna cum laude, from Michigan State University, East Lansing, MI.

Shannon Bond - Ms. Bond's association with the tax industry started in 2001 with an entrepreneurial franchise company in Jacksonville, Florida. Over the course of the past 15 years, she has engaged with hundreds of tax professionals, assisted new preparers in setting up their first tax office, worked with growing firms to establish best practices around compliance and workflow, and convened customer advisory boards to understand how their software can assist them in serving their clients. She has had the opportunity to work with professionals across the industry ranging from individual owners, multi-office operators, VITA locations, franchise systems and larger CPA firms to understand the needs of their business and the client's they support. She is a board member of CERCA, past secretary of ACTR and co-lead of the Tax Professional Work Group for the Security Summit.

John Breyault - Mr. Breyault joined the National Consumers League in September 2008. Breyault's focus at NCL is on advocating for stronger consumer protections before Congress and federal agencies on issues related to telecommunications, fraud, technology, and other consumer concerns. In addition, Breyault manages NCL's Fraud Center and coordinates the Alliance Against Fraud coalition. He is also Research Director for the Telecommunications Research and Action Center (TRAC), a project of NCL. In his role with TRAC, Breyault advocates on behalf of residential consumers of wireline, wireless, VoIP, and other IP-enabled communications services. Prior to coming to NCL, Breyault spent five years as director of research at Amplify Public Affairs, where he helped launch the firm's Web 2.0-based public affairs practice and focused on producing actionable public policy research. Breyault was a member of the FCC's Consumer Advisory Committee from 2005 to 2007 and served on the Board of the Arlington-Alexandria Coalition for the Homeless. He is a graduate of George Mason University, where he received a bachelor's degree in International Relations.

Luanne Brown - Ms. Brown has served as the Director of Payroll Services for Grand Valley State University for the last 13 years. For more than 20 years she has worked in varied industries including sports management, advertising, manufacturing, and higher

education. In her current role at the University there has been a major emphasis on data security. She has participated on a Senior Management Cyber Security Team and helped develop new security procedures and policies in the Payroll/Finance area along with communicating to employees on how to protect their personal data from identity theft and steps to take if their information has been compromised. Brown currently serves as a Director on the American Payroll Association Board of Directors. Brown holds a master's degree in Public Administration with an emphasis on Public Management from Grand Valley State University.

Angela Camp - Ms. Camp has over 20 years of experience in the tax industry. Camp was a member of the Intuit Corporate Affairs and Government Relations team for seven years with a focus on driving tax administration and policy from the point of view of a software provider. During that time, Camp was a key point of contact for Intuit for tax reform implementation, IRS Security Summit, Free File and a number of tax policy and related initiatives. Camp also worked for IRS, where she spent time managing relationships and working issues for individual and small business taxpayers, as well as payroll providers. She worked with the electronic tax administration, where she was responsible for managing IRS relationships with software industry partners, States, and the Federation of Tax Administrators and ETAAC to advance electronic filing for businesses and individuals, Free File, and Federal/State electronic initiatives.

John Craig - Mr. Craig is a non-profit consultant specializing in strategy and technical support for Volunteer Income Tax Assistance (VITA) programs. He has more than 15 years of experience in managing and advising on VITA programs across the nation, with diverse expertise in service delivery, consumer advocacy, and use of tax credits to build financial stability among low-income taxpayers. He has worked extensively with the IRS, corporations, and non-profits on electronic filing implementation and improvement. In 2014, he led the Corporation for Enterprise Development's successful launch of the Taxpayer Opportunity Network, a more than 800-member coalition that promotes delivery of free high-quality tax services, protects rights, and promotes financial empowerment of low-income taxpayers. Mr. Craig was also instrumental to the creation of TON's predecessor, the National Community Tax Coalition and served on its steering committee from 2001-2006. He has managed high-volume VITA tax service programs at the Chicago-based Center for Economic Progress and at Community Tax Aid in the Washington D.C. area, generating more than 100,000 tax returns during his tenure. Mr. Craig holds a B.A. from Earlham College and an M.A. from the Earlham School of Religion, graduating with honors.

Jenine Hallings- Ms. Hallings is a Compliance Risk Manager for Paychex. Her team is responsible for research, analysis and communication of legislative and regulatory changes impacting the company and its clients and partners, and manages Paychex' relationships with various federal and state tax agencies on behalf of clients. Hallings represents Paychex in key industry consortiums to ensure the company is abreast of regulatory trends and developments. Hallings has been at Paychex for over 20 years, and has extensive experience on a broad range of payroll tax matters. Hallings holds an MBA from the Rochester Institute of Technology.

Michael Jackman- Mr. Jackman has extensive experience in taxation, tax administration and related information systems. He currently operates a small tax

practice and serves as the coordinator for two Volunteer Income Tax Assistance (VITA) sites. Over a 22-year tenure as an IRS employee he held several compliance and information technology positions, culminating in serving in the IRS National Office as the Chief of Systems Development for the original Electronic Filing System. As a consultant, he provided expertise to the IRS in the development of numerous IRS information systems including Modernized E-File, and the Customer Account Data Engine (CADE). In addition, he owned and operated several Jackson Hewitt Tax Service franchises in Maryland, after which he founded Patriot's Choice Tax Service in Gettysburg. Jackman is an Enrolled Agent and holds an MS in Taxation from the Deming School of Business at William Howard Taft University.

Courtney Kay-Decker- Ms. Kay-Decker served as the Director of the Iowa Department of Revenue from 2011 through January of 2019. While at the Department, Decker focused on improving administrative rules, guidance and processes to simplify and reduce compliance burdens for Iowa taxpayers. Decker has served on various boards and committees related to tax administration, and is active in various endeavors to prevent identity theft and tax refund fraud. Decker received her B.A. in Economics from Northwestern University in Evanston, Ill. She holds a Doctorate of Jurisprudence with distinction from the University of Iowa College of Law. Prior to joining the Department, Decker was a partner at Lane & Waterman LLP in Davenport, Iowa. She served as a member of the Iowa State Board of Tax Review from 2000-2007 and was Chair of the Board from 2003-2007.

Suzanne Kruger- Ms. Kruger currently serves as the Security Specialist for the Montana Department of Revenue and is responsible for the operational security posture for all department information systems. She has served on several committees for the Montana Information Security Advisory Council (MT-ISAC) since its inception in May 2015. MT-ISAC's mission is to recommend an integrated interagency information security strategy to enhance the state information security posture. Kruger had more than 12 years of experience working with businesses, non-profits and individuals in the accounting, tax preparation and banking fields prior to obtaining a degree in Network Security along with one in Network Administration in 2007. She obtained her Certified Information Systems Security Professional (CISSP) credential in 2014.

Kathy Pickering, EA - Ms. Pickering is the executive director of The Tax Institute (TTI) and vice president of regulatory affairs for H&R Block. With over 20 years of experience in tax administration, Kathy is responsible for the strategic direction and management of a team of the nation's top tax experts. As head of The Tax Institute, Ms. Pickering oversees a group of 23 credentialed tax experts, with deep knowledge of the industry and regular, direct interaction with tax professionals and taxpayers. This team provides four key functions: 1) providing expert research and analysis to frontline tax professionals and taxpayers, 2) tax law and policy analysis, 3) leading the identification, communication, and integration of tax changes across H&R Block's operations, and 4) coordination and communication among the IRS, state and local agencies on issues affecting the tax industry. In her role as H&R Block's vice president of regulatory affairs, she leads the relationship-management strategy with the IRS and state taxing agencies. Ms. Pickering is currently focusing on the IRS Security Summit, which brings together

representatives from the IRS, state tax agencies, and private industry to work on collaborative solutions to combat stolen identity refund fraud schemes.

Phillip L. Poirier, Jr. – Mr. Poirier is a volunteer tax preparer in the IRS Volunteer Income Tax Assistance (VITA) program and is active in the Taxpayer Opportunity Network, which is managed by Prosperity Now and supports VITA programs at the national level. He is also a Senior Fellow with the Center for Social Development at Washington University in St. Louis. His consulting work with academia, non-profits and foundations focuses on investigating ways to better leverage the U.S. tax system to improve individual and family financial well-being in personal finance, credit, asset building and savings, as well on improving information security. His previous employment included working as an in-house lawyer and executive in the tax software industry with Intuit Inc. and practicing law in a private firm. Mr. Poirier served in the U.S. Navy and Naval Reserve for nearly three decades, retiring as a Captain. He holds a J.D. from the University of San Diego School of Law, and a bachelor's degree in international affairs from the United States Naval Academy.

Lynnette T. Riley- Ms. Riley was appointed the Georgia State Revenue Commissioner in January 2015. Riley comes to the Department of Revenue most recently from the Georgia General Assembly, where she served four years in office as the House District 50 (Johns Creek) Representative. While in the General Assembly, she was a member of the Ways and Means, Natural Resources and Environment, Retirement and the Metropolitan Atlanta Rapid Transit Oversight committees, was the Fulton County House Delegation Chair and an administration Floor Leader. Commissioner Riley currently serves on the Board of Trustees of the Federation of Tax Administrators, the Southeast Association of Tax Administrators, and Senior Executive Board of the Identity Theft Tax Refund Fraud Information Sharing & Analysis Center.

Gene Salo- Mr. Salo has over 25 years of experience in the tax industry, initially in tax preparation and later in tax software development. Recently, Salo has turned his focus to identity theft and tax refund fraud. He is active with the IRS, state tax agencies and tax industry members in the Security Summit, where he is a co-lead for the Tax Professional Working Group. Salo also serves as the Vice Chairman of the Board of Directors of CERCA, an association of tax industry firms that supports electronic filing. Salo earned his MBA from the University of Michigan and has a dual BA in Accounting and Finance from Oakland University. He is a veteran of the US Air Force.

John Sapp – Mr. Sapp has served a key role at Drake Software for over 20 years, with roles ranging from Chief Financial Officer to Vice President of Drake's Sales and Marketing divisions. Today he serves as the Vice President of Strategic Development, where his role is to help shape the future and growth of one of the largest professional tax software companies in the nation. As a CPA, he has considerable experience working in public accounting in technological and private industries. He holds a bachelor's degree in Accounting from Oral Roberts University.

Joseph Sica - Mr. Sica, Chief Public Policy Officer for Green Dot/Tax Products Group, has been affiliated with tax time financial products and combating fraud in the tax system for the last 28 years. In the earliest days of e-filing, Mr. Sica worked with the IRS to develop and pilot refund loans as an incentive for people to file electronically. Prior to

IRS having increased fraud detection capabilities, he started the Fraud Service Bureau in 1994 in which banks in the tax loan industry electronically exchanged data to identify fraud and shared results with the IRS. Years ago, Mr. Sica changed his primary focus in the tax industry from technology to related policy affairs and assisted in coordination of dialog between the industry and the IRS. As such, he is a co-founding board member and past chair of the Council for Electronic Revenue Communications Advancement (CERCA). Mr. Sica is also a co-founder member and past vice-chair of the American Coalition for Taxpayer Rights (ACTR), a tax industry policy group seeking to preserve taxpayer choices. Recently, he has worked with industry, state revenue departments and the IRS in connection with establishing the IRS Security Summit taking co-lead roles in the Information Sharing and the Financial Services work groups. Mr. Sica completed Executive Development work at The Wharton School in 1996.

Mark Steber - Mr. Steber, Chief Tax Officer with Jackson Hewitt Tax Service, is responsible for several key initiatives to support overall tax service delivery and quality assurance. Mr. Steber serves as a Jackson Hewitt liaison with the Internal Revenue Service, States, other government authorities, Walmart, other retail entities, and banking partners. With over 30 years of tax experience, Mr. Steber is widely referenced as an expert on consumer income tax issues and especially electronic tax and data protection issues. Mr. Steber has been an active participant in the IRS Security Summit Initiative since the founding of the effort in early 2015. He has been involved with all the work groups including the Information Sharing Group, Authentication Work Group and Strategic Threat Assessment and Response (STARS) group and subsequent new groups including the Tax Pro Subgroup of the Security Summit. Mr. Steber is active with various industry groups, including ACTR and CERCA, and has worked directly with leadership members in many instances. In prior years, he served on the IRS Electronic Tax Administration Advisory Committee and was Chairman in 2012. Prior to joining Jackson Hewitt, he was a tax partner with Ernst and Young LLP.

Doreen Warren - Ms. Warren has over 28 years' experience in state tax administration with the Idaho State Tax Commission. She served as the Administrator for the tax return processing division where preventing tax refund fraud became a critical issue, and then as the Public Information Director in charge of education and outreach for taxpayers, tax professionals, legislators and community groups. She has more than 20 years' experience with facilitating collaborative efforts with states, IRS and various industry partners. In the fall of 2014, through the coordination of the Federation of Tax Administrators and the National Association of Computerized Tax Processors (NACTP), she facilitated the beginning efforts of a collaborative approach to detecting and preventing fraud in the tax ecosystem. As the Security Summit formed in the spring of 2015, she was designated the chief state co-lead to represent state interests and ensure state participation in this monumental effort. In addition to her leadership role at the Tax Commission, she played an active role in the Authentication, Information Sharing and Tax Professional working groups until the fall of 2018. She is currently the chair of the IRS Electronic Tax Administration Advisory Committee (ETAAC). Ms. Warren's education includes an associate degree in computer science, a bachelor's degree in business, and a master's degree in business administration.

Appendix C

ETAAC E-File Analytical Methodology

This Appendix explains ETAAC's methodology for analyzing and projecting electronic filling rates for all major returns and for individual tax returns. ETAAC standardized its methodology for e-file estimates and projections to provide a consistent measure of IRS e-file performance, standardize cross-year comparisons and facilitate analysis.

E-file Rates for Major Returns

To determine the e-file rate for all major returns, ETAAC takes two steps.

First, ETAAC identifies the "major" returns, which it considers to be the following return headings found in Table 2 of IRS Publication 6186:

Individual Income Tax (Form 1040 series)	Employment (Form 94X series)
Corporation Income Tax (Form 1120 series)	Fiduciary (Form 1041)
Exempt Organizations (Form 990 series)	Partnership (Form 1065 series)

Second, using the IRS' most up-to-date published information from Publication 6186, ETAAC computes an electronic filing rate for each specified return family as well as an overall electronic filing rate for all major return families. These estimates and projections are reflected in Table 2 in the Progress Toward 80% E-file Goal section of this Report.

ETAAC-projection for Current Year E-file Rate for Individual Returns

Form 1040 series returns are the bellwether for IRS e-file given they account for the lion's share (over 75%) of all major return types.

In its projection for the current year, IRS Publication 6186 must necessarily rely on historical information as the foundation for its estimates and projections. We, in turn, have used IRS estimates and projections from IRS Publication 6186 as a baseline for ETAAC's projection.

To supplement insights from IRS Publication 6186, ETAAC has developed a methodology to project the current-year e-file rate for individual returns based on partial filing season data and historical trends. Specifically, the methodology extrapolates and adjusts current filing season year-to-date information into full-year estimates based on historical e-file trends in the May-October period.

Using this methodology, ETAAC estimates that the e-file rate for individual returns will be approximately 89% for the entire 2019 filing season.

Below is an explanation of ETAAC's three-step process to project the full-year electronic filing rate for individual returns for 2019.

Step 1: Estimate actual current year-to-date e-file rate.

Determine the current year-to-date e-file rate for individual returns based on actual return filing information through April 19, 2019, which ETAAC calculates to be 92.01%.

Table 3: Tax Year 2018 Individual Income Tax Returns Actual through April 19, 2019

Cumulative statistics comparing 4/20/18 and 4/19/19			
	04/20/2018	04/19/2019	**YOY % Change**
Total Receipts	136,919,000	137,233,000	0.23%
E-file Receipts	124,515,000	126,264,000	1.40%
E-file Rate	90.94%	92.01%	1.07%

Source: From "Filing Season Statistics for Week ending April 19, 2019" published by IRS at https://www.irs.gov/newsroom/filing-season-statistics-for-week-ending-april-19-2019.

Step 2: Estimate historical e-file degradation rate through remaining filing season

This is accomplished by comparing the e-file rate for the first four months of the year through late April (primary filing season) with the actual e-file rate for the full-calendar-year filing season for each of the two preceding years -- 2017 and 2018. Then, ETAAC uses the average degradation rate experienced over the comparable period for each of the previous two years to forecast degradation for the current year. Using this approach, the e-file degradation rate for the 2019 filing year is forecast to be 3.05%. (ETAAC will continue to monitor the degradation rate to note whether it has any significant year-to-year changes.)

Table 4: Historical Partial-Season Data vs. Full-Season Data

	04/21/17	**11/24/2017**	**Change**	**04/20/2018**	**11/23/2018**	**Change**	**Two Yr. Avg.**
Total Receipts	135,638,000	151,825,000		136,919,000	154,444,000		
E-file Receipts	122,164,000	132,319,000		124,515,000	135,459,000		
E-file Rate	90.1%	87.2%	-2.9%	90.9%	87.7%	-3.2%	**-3.05%**

Source: Various Filing Season Statistics found on www.irs.gov

Step 3: Project the full-year e-file rate for individual returns.

Subtract the e-file degradation rate from the actual current year-to-date e-file rate.

Using IRS' April 19, 2019 data, ETAAC's projected 2019 full-year e-file rate for the individual tax return family is 88.96%. This ETAAC projection is consistent with the IRS's 2019 projection of 89.1% in IRS Publication 6186.

Table 5: 2019 Individual Returns Electronic Filing Projection

	Current @ 4/19/19	**Avg. Degradation Rate**	**ETAAC 2019 Projection**
Total Receipts	137,233,000		
E-file Receipts	126,264,000		
E-file Rate	92.01%	**-3.05%**	88.96%

General Note: Select numeric percentages and results may have slight rounding adjustments.

This page left intentionally blank