IRS

TAXES + SECURITY TOGETHER

Electronic Tax Administration Advisory Committee

ANNUAL REPORT TO CONGRESS

June 2018

Publication 3415 (Rev. 6-2018) Catalog Number 28110R Department of the Treasury **Internal Revenue Service** www.irs.gov

ELECTRONIC TAX ADMINISTRATION ADVISORY COMMITTEE

MEMBERS

John Ams

Robert Barr

Shannon Bond

John Breyault

Luanne Brown

Angela Camp

John Craig

Jenine Hallings

Michael Jackman

Courtney Kay-Decker

Suzanne Kruger

Kathy Pickering

Phillip Poirier, Jr.

John Sapp (Chair)

Joseph Sica

Mark Steber

Atilla Taluy

Doreen Warren (Vice Chair)

ETAAC's 2018 Report is dedicated to the memory of our dear friend and colleague Atilla Taluy who passed away this year

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 2018 Annual Report to Congress. Our primary focus in 2018 continues to be on protecting taxpayers by suggesting methods and processes to fight identity theft tax refund fraud (referred to as IDTTRF or fraud in this Report) and enhancements to the security of our electronic tax infrastructure. Our Report also provides recommendations for the Internal Revenue Service (IRS) to increase electronic filing and expand electronic services.

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

1. The Security Summit, under the IRS' leadership, continues to make progress in the fight against IDTTRF.
2. The IDTTRF threat will never end -- criminals are constantly adjusting their strategies and tactics to find new ways to steal individual and business identities and convert those stolen identities into tax refunds.
3. The IRS, States and Industry have made a strong commitment of resources to the Security Summit, but Congressional funding and support remains a key enabler.
4. The Security Summit must continue to expand its scope and the level of member participation.
5. Success in cybersecurity is a moving target – it requires continuous innovation and a forward thinking mindset.

The Report is organized to provide key insights at a glance or to dig into supporting details:

- For a high level overview, read the short Executive Summary following this Letter and the Summary List of ETAAC 2018 Recommendations.
- To understand the details underlying ETAAC's recommendations, review the Detailed Support for ETAAC 2018 Recommendations section – each area includes an Introduction followed by specific recommendations and support (page numbers for each area and recommendation are listed in the Table of Contents)

Finally, ETAAC appreciates the support and interest that Congress has expressed in our work – it makes the thousands of volunteer hours worthwhile. ETAAC would also like to recognize the IRS' employees and leadership for their continued responses to what sometimes can be an overwhelming list of questions and data requests from ETAAC, and also for their commitment to the Security Summit and the American taxpayer. We are grateful for their thoughtful and candid insights.

Sincerely,

John Sapp	Doreen Warren
ETAAC Chair	ETAAC Vice Chair

EXECUTIVE SUMMARY

Primary Focus of Report -- Cybersecurity and Identity Theft Tax Refund Fraud

Congress established ETAAC in 1998 principally to report on the IRS' progress in advancing electronic filing (e-file) and its electronic tax administration strategy.[1]

ETAAC's 2017 Report shifted its primary focus to two areas foundational to the success and integrity of our nation's electronic tax system – the implementation of strong cybersecurity protections and the detection and prevention of IDTTRF. The 2017 Report supplemented these areas with recommendations concerning the IRS' achievement of its 80% e-file goal and other electronic tax administration initiatives. All of these areas of electronic tax administration are interdependent. Our 2018 Report focuses on these same areas.

Cybersecurity and IDTTRF are ongoing threats, but the IRS Security Summit continues to make progress

Cybercriminals continue to threaten our nation – they are organized, smart, nimble and well-funded.

Americans continue to receive notices about data breaches, most of which occur outside of our tax system.[2] Criminals use this stolen personal information, coupled with other information readily available online and through social media, to fuel IDTTRF. Essentially, these criminals know so much about a given taxpayer that their fraudulent electronically filed returns can be largely indistinguishable from those of the legitimate taxpayer.

Our voluntary compliance electronic tax administration system relies on the trust and confidence of American taxpayers and policy makers, which requires that we remain ever vigilant in the fight against IDTTRF.

The IRS Security Summit continues to demonstrate the value and necessity of public/private collaborations in the fight against IDDTRF. The About the IRS Security Summit section of this Report reviews the key achievements of the IRS, States and Industry through the Security Summit.

Focus of 2018 Report Recommendations

ETAAC's principal recommendations in 2018 generally fall into four broad areas:

I. Expand and strengthen the Security Summit and the IDTTRF Information Sharing and Analysis Center (ISAC) by:

- *Integrating the payroll community more broadly into the Security Summit and the ISAC*
- *Increasing outreach to employers and businesses*

[1] The Internal Revenue Service Restructuring and Reform Act of 1998, Public Law 105-206 (105th Congress) enacted July 22, 1998.

[2] The Equifax breach is only one recent example. Past examples of data breaches include the Office of Personnel Management (government), Anthem (healthcare) and LinkedIn (social media).

- *Ensuring the effective operation of the Security Summit and the ISAC*
- *Enabling collaborative innovation*

II. Strengthen the cybersecurity of the tax ecosystem by:

- *Establishing a common security standard and IRS' authority to enforce it*
- *Increasing participation in Security Summit cybersecurity initiatives*
- *Communicating and building tax professional awareness*
- *Requiring security continuing education for tax professionals*
- *Building accountability…Engaging, enforcing and learning*
- *Establishing clear IRS internal responsibility for tax professional security*

III. Improve IDTTRF detection, analysis and reporting by:

- *Enacting an Internal Revenue Code (IRC) Section 6103 IDTTRF exception*
- *Improving detection with enhanced business tax schema data elements*
- *Enabling EFIN and PTIN validation*[3]

IV. Enable electronic tax services and electronic filing by:

- *Continuing to enhance identity proofing and authentication*
- *Enabling the development of online tools*
- *Increasing the electronic filing of employment tax returns*

Summary of Requested Congressional Support for the IRS and Security Summit

Congressional appropriations and legislative policy actions play a critical role in enabling enhanced cybersecurity and the IRS' fight against IDTTRF.

In its 2018 Report, ETAAC is asking Congress to take action in several areas.

First, ETAAC asks that Congress provide sufficient funding to the IRS so that it can adequately staff and fund priorities relating to the Security Summit and the ISAC. The IRS has made a significant commitment of staff and other resources to these initiatives, as have the States and Industry. However, in light of the resources that will be required for the IRS to implement the Tax Cuts and Jobs Act (TCJA), ETAAC is concerned that the funding requirements for the continued fight against IDTTRF and for enhanced cybersecurity could be overshadowed by the implementation of tax reform measures.

Second, as further described in this Report, ETAAC is recommending that Congress take legislative action in the following areas:

[3] EFIN refers to an Electronic Filing Identification Number. PTIN refers to a Preparer Tax Identification Number.

- Gramm Leach Bliley and the FTC Safeguards Rule. To better protect taxpayers, ETAAC is recommending that Congress (i) extend the applicability of the Federal Trade Commission's (FTC) Safeguards Rule solely from those serving individual return filers (consumers) to also include persons serving business, employment and information return filers, and (ii) grant the IRS the corresponding authority to apply and enforce the FTC Safeguards Rule in areas under its jurisdiction. (See Recommendation #5) [4]
- Internal Revenue Code Section 6103. To enable more effective cybersecurity and IDTTRF identification and prevention, ETAAC is recommending that Congress add an exception to IRC Section 6103 that permits the use and disclosure of federal tax information relating to cybersecurity and IDTTRF prevention activities in tax administration. (See Recommendation #11)

As a side note, some of these recommendations for Congressional action are driven by limits on the IRS' regulatory authority illustrated either by (i) the decision in *Loving v. IRS* [5] or (ii) potential gaps in current cybersecurity legislation and associated regulations.[6] A broader Congressional grant of authority for the IRS to regulate tax preparers would obviate the need for some of these types of one-off actions.

Closing Thoughts

The IRS Security Summit has made a significant contribution in protecting taxpayers in innovative and collaborative ways. ETAAC would like to recognize the IRS' leadership, and the many capable, thoughtful and committed IRS employees assigned to the IRS Security Summit and ISAC initiatives.

There is also no doubt that coordinating the efforts of such a diverse stakeholder group presents challenges. The IRS has done a remarkable job of managing the efforts of both State departments of revenue and a broad range of private sector stakeholders including tax preparation (both commercial and non-profit), financial services and payroll service providers.

IRS' continued leadership, coupled with its ability to develop and manage diverse public/public and public/private partnerships, will continue to be a critical competency for the success of the Security Summit and electronic tax administration.

[4] This recommendation is directional. The creation of a tax security standard enforceable by the IRS might be accomplished by expanding GLB and the FTC Safeguards Rule coverage and providing for IRS jurisdiction or, alternatively, through some other legislative approach. ETAAC is not a legislative expert, and defers to Congress on the most effective and appropriate legislative approach.

[5] *Loving v. IRS*, 742 F.3d 1013 (D.C. Cir. 2014). See https://www.irs.gov/newsroom/irs-statement-on-court-ruling-related-to-return-preparers

[6] See analysis for Recommendations #'s 5-9 in the Detailed Support for ETAAC 2018 Recommendations section of this Report for background on the Gramm Leach Bliley Act and the FTC Safeguards Rule.

TABLE OF CONTENTS

ABOUT THE IRS SECURITY SUMMIT

Security Summit: Formation and Structure

By 2015, the levels of identity theft tax refund fraud (IDTTRF) had reached alarming levels. To address these challenges, then IRS Commissioner John Koskinen convened an unprecedented Security Summit meeting in Washington, D.C. on March 19, 2015.

The Security Summit included senior IRS officials, State tax administrators, and the chief executive officers of the leading tax preparation firms, software developers, and tax financial product processors. The Security Summit participants immediately recognized that fighting IDTTRF required the adoption of a multi-layered and coordinated approach across the entire tax ecosystem on both the federal and the state levels. The meeting focused on discussing common challenges and ways to use the tax ecosystem's collective resources and efforts to fight IDTTRF.

The following three work groups were formed at the first Security Summit meeting and tasked to deliver detailed recommendations by June 2015 for implementation in time for the 2016 filing season:[7]

- Authentication Work Group: Tasked with identifying opportunities for strengthening authentication practices, including new ways to validate taxpayers and tax return information, and new techniques for detecting and preventing IDTTRF.
- Information Sharing Work Group: Tasked with identifying opportunities for sharing information to improve the collective capabilities for detecting and preventing IDTTRF.
- Strategic Threat Assessment and Response (STAR) Work Group: Tasked with taking a holistic look at the entire tax ecosystem, identifying points of vulnerability (threats/risks) related to the detection and prevention of IDTTRF, developing a strategy to mitigate or prevent these risks and threats, and reviewing best practices and frameworks used in other industries.

Subsequently, the Security Summit recognized the need to create additional teams to enhance and expand their collaborative efforts, which resulted in the formation of three additional work groups and one new subgroup:

- Financial Services Work Group: Tasked with examining and exploring additional ways to prevent and deter criminals from potentially accessing tax-related financial products, deposit accounts, and pre-paid debit cards.
- Communication and Taxpayer Awareness Work Group: Tasked with increasing awareness among individuals, businesses and tax professionals on the need to protect sensitive tax and financial information.
- Tax Professional Work Group: Tasked with examining how new requirements will affect tax preparers who use professional software, how the preparer

[7] The Summit's initiatives for the 2016 filing season were reported in the Security Summit 2015 Report. See https://www.irs.gov/pub/newsroom/2015%20Security%20Summit%20Report.pdf

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.

- IDTTRF Information Sharing and Analysis Center (ISAC): Started as a sub-group of the Information Sharing Work Group, and tasked with centralizing, standardizing, and enhancing data compilation and analysis to facilitate sharing actionable data and information. The ISAC started pilot operations in 2017, and continued as a pilot into 2018 with the participation of all States and a majority of Security Summit industry partners.[8]

Each Security Summit work group has a co-lead from each of the IRS, the states and industry. The ISAC is separately managed through its Senior Executive Board.

Security Summit: Evolution of the ISAC

The IRS launched the ISAC pilot for the 2017 filing season and, based on the outlook for its success, continued its pilot operations into the 2018 filing season.[9] The ISAC has two key components: (i) an online platform run by the IRS to communicate data on suspected IDTTRF, and (ii) an ISAC Partnership, a collaborative organization comprised of the IRS, states, and industry, which is the ISAC's governance structure.

The ISAC plays an essential role for collecting and quickly sharing meaningful IDTTRF schemes among the member organizations and reducing the risk to taxpayers. The ISAC has established a secure foundation for analysts to communicate emerging schemes and confirmed fraud quickly across the tax ecosystem. The IRS identified three initial goals for the ISAC: (1) launch the online platform, (2) establish the governance structure, and (3) recruit new members. The ISAC has made progress against each of these goals.[10] Furthermore, the Treasury Inspector General for Tax Administration (TIGTA) reported that the ISAC has successfully implemented the minimum security requirements for ISACs (sometimes called ISAOs) established by the Department of Homeland Security.[11]

Filing Season 2017 Results

The IRS reported several successes for the Security Summit in calendar year 2017:[12]

- The number of taxpayers reporting to the IRS that they are victims of identity theft continued its major decline. In 2017, the IRS received 242,000 reports from taxpayers compared to 401,000 in 2016 – a 40 percent decline. This was the second year in a row this number fell, dropping from the 677,000 victim reports in

[8] The ISAC now includes 64 member organizations (45 states, 18 Industry and the IRS). There is limited financial and payroll industry participation at this time, largely due to sharing restrictions.

[9] Over twenty ISACs exist in a variety of sectors. ISACs were first introduced in Presidential Decision Directive 63, dated May 22, 1998, which called for the establishment of infrastructure sector-specific organizations to share information about threats and vulnerabilities. See https://www.nationalisacs.org for more information on ISACs, including the Financial Services ISAC and Information Technology ISAC.

[10] For a recent GAO review of the ISAC, see https://www.gao.gov/assets/690/688612.pdf

[11] See https://www.treasury.gov/tigta/auditreports/2017reports/201720064fr.pdf

[12] See https://www.irs.gov/newsroom/key-irs-identity-theft-indicators-continue-dramatic-decline-in-2017-security-summit-marks-2017-progress-against-identity-theft

2015. Overall, the number of identity theft victims has fallen nearly 65 percent between 2015 and 2017.

- The number of tax returns with confirmed identity theft declined to 597,000 in 2017, compared to 883,000 in 2016 – a 32 percent decline. The amount of refunds protected from those fraudulent returns was $6 billion in 2017, compared to $6.4 billion in 2016. In 2015, there were 1.4 million confirmed identity theft returns totaling $8.7 billion in refunds protected. Overall during the 2015-2017 period, the number of confirmed identity theft tax returns fell by 57 percent with more than $20 billion in taxpayer refunds being protected.
- The financial industry continued to be a key partner in fighting identity theft and helping the IRS recover fraudulent refunds that may have been issued. In 2017, banks recovered 144,000 refunds compared to 124,000 in 2016 – a 16 percent increase. The amount of refunds recovered was $204 million in 2017, compared to $281 million in 2016. In 2015, the financial industry recovered 249,000 refunds totaling $852 million.
- The IRS continues to reduce the year-over-year inventory backlog of taxpayers who file identity theft reports. For fiscal year 2017, the beginning inventory of identity theft reports submitted by taxpayers was approximately 34,000, under 10 percent of the fiscal year 2013 beginning inventory of 372,000 taxpayer identity theft cases.

Filing Season 2018 Focus

For the 2018 filing season, the Security Summit's emphasis remained on awareness, authentication, information sharing and analysis, prevention and cybersecurity. Some specific IRS and Security Summit accomplishments and initiatives include:

Increase awareness and action

- Conducted National Tax Security Awareness Week
    - Developed and issued a series of 10 news releases and tax tips to guide individual and business taxpayers on steps to protect their tax data and identities in advance of the 2018 filing season.
    - Worked with state and private-sector Security Summit partners, local consumer groups, law-enforcement agencies and other government groups to conduct 32 different events across the country, with more than 50 local television stories and coast-to-coast media attention. 24 state revenue departments participated in the effort.
- Drove increased publicity and awareness by issuing more than 30 different IRS news releases and tax tips highlighting various security and Security Summit messages since October 2017.
    - Continued taxpayer-focused awareness campaigns related to "Taxes.Security.Together."
    - Expanded tax professional-focused security awareness campaigns: "Protect Your Clients, Protect Yourself" to raise awareness among tax

professionals about their legal obligation to protect taxpayer data and to highlight the security risks posed by identity thieves. Provided four data security messages, reaching over 700,000 return preparers with PTIN accounts.

- Conducted an extensive communication campaign to inform tax professionals and continuing education provider communities of the availability of continuing education credit for programs covering data security topics.

Enhance detection, prevention and analysis in tax and financial sectors

- Continued ISAC pilot with more robust capabilities including sharing of near real-time tax ecosystem alerts, and analysis of leads generated by the tax software and tax preparation industry and other member data.
- Completed data elements (tax return attributes) analysis and individually shared with industry partners to discuss data quality, completeness and effectiveness in assisting with identity theft detection.
- Completed leads analysis and shared comprehensive and customized analysis with each partner regarding their unique reporting of leads.
- Expanded authentication of individual tax returns.
- Launched a pre-validation pilot with financial institutions to address suspicious refunds -- the pilot is available to all states.
- Expanded outreach with financial institutions to assist in recovering fraudulent refunds and continued work with the Bureau of Fiscal Service to improve accuracy and efficiency of detecting fraud and identity theft.
- Updated and formalized Security Summit membership criteria and standards of conduct

Strengthen authentication and protection of taxpayer information

- Continued work on strategy to ensure that updates to the Trusted Customer Requirements align with the National Institute of Standards and Technology (NIST) standards to improve the safeguarding of Taxpayer Information and reduce the instances of IDTTRF.
- Expanded business identity theft protections to more business taxpayers

The impact of Security Summit actions in 2018 will be assessed in the coming months.

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.

Looking Ahead – Sustaining the Momentum

At the time of its initial creation, the Security Summit was facing a clear challenge from IDTTRF. There were equally clear opportunities in some key areas (e.g., authentication, information sharing, and cybersecurity standards) that the IRS, States and Industry pursued quickly with good progress. As the Security Summit matures, it must continue to sustain its progress and momentum by assessing and prioritizing its biggest opportunities and challenges.

PROGRESS TOWARD 80% E-FILE GOAL

ETAAC's charter provides that it will research, analyze, consider and make recommendations on the IRS' progress toward achieving its 80% e-file goal for major returns. Consistent with prior years reporting, ETAAC has calculated an updated electronic filing rate to benchmark overall e-filing performance. ETAAC focuses on the major series of individual and business returns as outlined in Appendix C, coupled with ETAAC's review of published IRS data and its own calculation methodology.

IRS should hit the 80% target for all major returns in 2018

In last year's Report, ETAAC projected for the first time that in 2017 the IRS should achieve its 80% e-filing goal for major return types with a total of 80.1%. IRS' most current filing estimate of 79.9% for 2017 reflects that it may have fallen just short of that projection but that it should exceed the 80% target in 2018 (See Table 1).

This is a momentous achievement for the IRS, and ultimately for the American taxpayer. It reflects years of hard work by a public/private partnership between the IRS, state tax administrators and the private sector to increase electronic filing.

Table 1: 2015-2018 Electronic Filing Rate for Major Returns

	2015 (IRS Actual)	**2016 (IRS Actual)**	**2017 (IRS estimated)[13]**	**2018 (IRS projected)**
Electronic Filing Rate	77.8%	79.3%	79.9%	81.2%

Source: IRS Publication 6186 (as updated annual from 2015-2017)

E-file growth continues, but employment return e-file remains a key opportunity

As of April 20, 2018, the e-file rate for individual returns during the initial part of Filing Season 2018 increased by 1.9% compared to the prior year comparable period.[14] This is encouraging because the e-file rate for individual returns through a comparable period last year had decreased by 0.3%, although the rate did catch up by the end of the full filing season.[15] The shift in filing volume to later in the season was identified as an issue by ETAAC last year, but 2018 appears to reflect a return of normality and predictability to the timing of e-file receipts.

As shown in Table 2 below, individual returns have the highest e-file rate and represent almost 77% of major returns filed. While the growth rate of individual e-file is relatively low, it reflects the maturity of e-file and is still consistently increasing. It is safe to say that e-file has become the norm for filing tax returns.

E-file rates continue to increase for all other major return types. However, employment tax returns continue to be the next obvious target for the IRS' efforts to increase e-file,

[13] See IRS Publication 6186 2017 Update (revised 11-2017) p. (1) for explanation of IRS' estimate and projection methodologies.

[14] See https://www.irs.gov/newsroom/filing-season-statistics-for-week-ending-april-20-2018

[15] See https://www.irs.gov/newsroom/filing-season-statistics-for-week-ending-april-21-2017

which currently have the lowest e-file rate of all major return types. (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.)

Table 2: 2018 Projected Electronic Filing Rates

	2017 IRS Estimated			2018 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)	151,568,500	132,973,800	87.7%	153,329,500	136,082,600	88.8%	1.0%
Employment (Form 94X Series)	30,744,400	12,719,700	41.4%	30,897,400	13,471,700	43.6%	2.2%
Corp Income Tax (1120,1120-A,1120-S), etc.	7,081,600	5,521,600	78.0%	7,184,900	5,703,400	79.4%	1.4%
Partnership (Forms 1065/1065-B)	4,083,500	3,476,700	85.1%	4,179,400	3,611,900	86.4%	1.3%
Fiduciary (Form 1041)	3,200,400	2,650,800	82.8%	3,213,200	2,716,400	84.5%	1.7%
Exempt Orgs (Forms 990, 990-EZ, etc.)	1,572,600	1,013,100	64.4%	1,607,600	1,053,500	65.5%	1.1%
Totals	198,251,000	158,355,700	79.9%	200,412,000	162,639,500	81.2%	1.3%

Source: See Table 2, IRS Publication 6186 2017 Update (revised 11-2017)

The individual return electronic filing rate in 2018 should hit approximately 88%

The latest update to IRS Publication 6186, which is based on information available as of August 2017, projects that individual tax returns will be e-filed at a rate of 88.8%.

As in past reports, ETAAC has developed its own methodology to estimate the current year individual return e-file rate based on season-to-date filing information as of April adjusted for changes in historical e-file patterns between May and October. ETAAC’s methodology is described in Appendix C.

This year, ETAAC estimates that individual returns should achieve an e-file rate of almost 88% in 2018, which is consistent with IRS’ projection in Publication 6186.

PROGRESS ON ETAAC 2017 RECOMMENDATIONS

ETAAC made twenty-two recommendations in its 2017 Report. Generally, the IRS agreed with ETAAC's 2017 recommendations and indicated an intention to implement or evaluate them, as appropriate.

Of course, the IRS has no shortage of priorities -- from enacting major tax legislation to meeting other challenges.[16] Funding is always a constraint. For example, it would appear that funding is a key barrier to implementing the ability to electronically file Form 1040X, Amended U.S Individual Income Tax Return, through the IRS Modernized e-file (MeF) System. As a result, it is up to the IRS to determine the extent or manner in which it will implement any ETAAC recommendations, and the associated prioritization and allocation of resources.

Looking back, the IRS made excellent progress on several of ETAAC's 2017 recommendations, including IRS':

- Analysis of the effectiveness of specific data elements used to authenticate returns
- Documentation of the Security Summit's information sharing process
- Continuation of the ISAC pilot for the 2018 filing season
- Continued implementation of the *National Institute of Standards and Technology* (NIST) Cybersecurity Framework and NIST 800-63-3
- Engagement with vulnerable financial institutions to gain their participation in the External Leads/Rejects programs
- Continued outreach and communication through the "Taxes. Security. Together." awareness campaign

There are, however, three 2017 recommendations where ETAAC encourages more or continued IRS attention.

ETAAC 2017 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.*

IRS Response: The IRS stated that it would conduct research into the effectiveness of the PY AGI/SS PIN taxpayer signature methods, and subsequently partner with the Security Summit to determine the feasibility of replacing these signature methods. Currently, the IRS is in the preliminary stages of research and no decisions have been made regarding the PIN's effectiveness.

ETAAC Thoughts: ETAAC's estimate that the e-file reject rate for primary taxpayer AGI/PIN errors would increase to almost 6 million e-file rejects in 2017 came true.

[16] See TIGTA's Management and Performance Challenges Facing the Internal Revenue Service for Fiscal Year 2018. https://www.treasury.gov/tigta/management/management_fy2018.pdf

The AGI/PIN reject rate is far and away the largest cause of e-file rejects and must be remedied. Security Summit stakeholders continue to support a replacement for the current model. Hopefully, the IRS' success in enhancing return authentication will help to find a replacement in the near future. ETAAC encourages the IRS to complete this evaluation quickly so that action can be taken in time for the 2019 filing season, or as soon as possible thereafter.

ETAAC 2017 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.*[17]

IRS Response: The IRS agreed with this recommendation, and advised ETAAC about a red team exercise conducted with the ISAC. The IRS also noted its continued collaboration with stakeholders to anticipate future trends in identity theft, but stated it was not currently planning a red team exercise with Security Summit participants (as distinguished from the ISAC). The IRS further noted its ongoing work group meetings to address impending threats and look for opportunities to further expand identity theft protections, as well as its ongoing brainstorming activities that, although not specifically red team exercise, served to facilitate collaboration and the generation of new ideas.

ETAAC Thoughts: ETAAC supports the IRS' ongoing practice of brainstorming threats and identifying courses of action. The knowledge and insights of IRS employees involved with the Security Summit universally reflect the value of this practice. ETAAC is also aware that IRS conducted a red team-type exercise with ISAC analysts and leadership. However, State and Industry members of the Security Summit have expressed to ETAAC a belief that a comparable event would be helpful to Security Summit members as well. For that reason, ETAAC encourages the IRS to consider a red team exercise for the Security Summit. By their very nature, red team exercises are designed to create insights that are often not identified through normal business operations, "lessons learned" sessions and post-season reviews.

ETAAC 2017 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 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*

[17] See https://en.wikipedia.org/wiki/Red_team for an overview of red team exercises.

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.

IRS Response: The IRS agreed with this recommendation, and noted its review and updating practices regarding its publications. It also noted that these publications are made up from information provided and owned by many parts of the IRS organization. The IRS also reports that it has not made material changes to Publications 1345, 3112 and 4557 since its initial response to ETAAC because IRS Electronic Products and Services Support *(*EPSS*)* has not received additional guidance or changes for security-related participation rules and requirements.

ETAAC Thoughts: 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 articulates our concerns and suggested actions.

SUMMARY LIST OF ETAAC 2018 RECOMMENDATIONS

Below are ETAAC's 2018 recommendations organized into four specific areas. Our underlying analysis and support for each recommendation is found in the following "Detailed Support for ETAAC 2018 Recommendations" section of this Report. These recommendations are not listed in priority order. Ultimately, the IRS must decide whether and how to implement these recommendations based on its assessment of benefit/cost of any given action.

I. EXPAND AND STRENGTHEN THE SECURITY SUMMIT AND ISAC

RECOMMENDATION #1: *Integrate the payroll community more broadly into the Security Summit and the ISAC*

The IRS should engage and integrate the Payroll Community more broadly into the Security Summit with an initial focus on expanding its participation into reporting key data elements in e-file schemas, leads reporting and the ISAC operations.

RECOMMENDATION #2: *Increase outreach to employers and businesses*

The IRS should collaborate with the Security Summit to identify ways to increase its outreach to and support of employers and businesses to help them (i) identify potential indicators of fraudulent activities affecting their returns and accounts, and (ii) report quickly and easily to the IRS concerning fraudulent activity on their accounts.

RECOMMENDATION #3: *Ensure the effective operation of the Security Summit and ISAC*

The IRS should create consolidated reference materials that explain the purpose, responsibilities and goals for both the Security Summit and ISAC, and for each of their respective work groups and committees.

RECOMMENDATION #4: *Enable collaborative innovation*

The IRS should use the authorities granted under Title II of the 1998 IRS Restructuring and Reform Act to create collaborative partnerships and programs, including the re-implementation of its Requests for Agreement Program, to facilitate private sector innovation in pursuit of the IRS' electronic tax administration and IDTTRF goals and objectives.

II. STRENGTHEN THE CYBERSECURITY OF THE TAX ECOSYSTEM

RECOMMENDATION #5: *Establish a common security standard and the IRS' enforcement authority*

Congress should (i) extend the applicability of the FTC Safeguards Rule to all persons providing preparation or filing services for tax returns under the Internal Revenue Code, and (ii) grant the IRS the explicit authority to implement and enforce the FTC Safeguards Rule as so extended.

RECOMMENDATION #6: ***Increase participation in Security Summit cybersecurity initiatives***

The IRS should work with Security Summit members to achieve 100% participation in the current STAR Work Group controls implementation and self-assessment initiatives, including engaging with non-participants to identify and remove barriers, considering ways to increase transparency and providing incentives to increase active participation.

RECOMMENDATION #7: ***Communicate and build tax professional awareness***

The IRS should communicate security requirements to tax professionals through all appropriate channels (including their employers) with a clearer, stronger message about their existing legal requirements under the Safeguards Rule, and leverage other regular interactions to reinforce that message, validate awareness and discuss compliance.

RECOMMENDATION #8: ***Require security continuing education***

The IRS should require that all tax professionals successfully complete two hours of continuing education in data security annually, potentially as a condition of obtaining or renewing their PTIN or applying for and maintaining their status as an Authorized IRS e-file Provider. Additionally, the IRS should supplement existing security education programs targeted to tax professionals by partnering with the Security Summit to select an experienced private sector expert (whether academic, nonprofit or commercial) to assist in the development of a comprehensive security program of instruction.

RECOMMENDATION #9: ***Build Accountability…Engage, Enforce and Learn***

The IRS should leverage its existing channels and processes to obtain periodic: (i) acknowledgments from tax professionals that they are aware of their security requirements under the FTC Safeguards Rule and IRS publications, and (ii) attestations that they are in compliance with those requirements.

RECOMMENDATION #10: ***Establish clear IRS internal responsibility***

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 of such requirements across IRS stakeholders.

III. IMPROVE IDTTRF DETECTION, ANALYSIS AND REPORTING

RECOMMENDATION #11: ***Enact an IRC Section 6103 IDTTRF exception***

Congress and the Department of the Treasury should make targeted legislative and regulatory changes, respectively, to permit appropriate use and disclosures under Internal Revenue Code Section 6103 to enable appropriate tax administration cybersecurity and IDTTRF prevention activities.

RECOMMENDATION #12: ***Improve detection with enhanced business tax schema data elements***

The IRS should work with Security Summit partners to evaluate the need to require the reporting of certain data elements in business income tax schemas, and to establish a business return leads reporting process to enable analysis by the Security Summit and ISAC.

RECOMMENDATIONS #13: ***Enable third party EFIN and PTIN validation***

Recommendation #13: *The IRS should collaboratively develop and implement a plan to enable real-time electronic EFIN and PTIN validation by authorized third parties.*

IV. ENABLE ELECTRONIC TAX SERVICES AND ELECTRONIC FILING

RECOMMENDATIONS #14 – 15: ***Continue to enhance identity proofing and authentication***

Recommendation #*14*: *The IRS should 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.*

Recommendation #*15*: *The IRS should extend eligibility to obtain an Identity Protection Personal Identification Number (IP PIN) to all individual taxpayers.*

RECOMMENDATIONS #16 – 18: ***Enable the development of online tools***

Recommendation #16: *The IRS should increase and deepen its collaborative engagement with stakeholders concerning the features, design and implementation of the IRS' digital services, including being more transparent about and publicly reporting on goals for both customer service metrics, stakeholder feedback and other key elements that inform its digital strategy.*

Recommendation #17***:*** *The IRS should prioritize the development of an electronic means to submit and accept powers of attorney.*

Recommendation #18***:*** *The IRS should continue its investigation and development of a lock/unlock feature for individual and business taxpayer accounts.*

RECOMMENDATION #19: ***Increase the electronic filing of employment returns***

Recommendation #19***:*** *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 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.*

DETAILED SUPPORT FOR ETAAC 2018 RECOMMENDATIONS

I. EXPAND AND STRENGTHEN THE SECURITY SUMMIT AND ISAC

- Integrate the payroll community more broadly into the Security Summit and ISAC (Recommendation #1)
- Increase outreach to employers and businesses (Recommendation #2)
- Ensure the effective operation of the Security Summit and ISAC (Recommendation #3)
- Enable collaborative innovation (Recommendation #4)

INTRODUCTION

Business tax return IDTTRF is increasing

Last year, the IRS identified increasing business tax return IDTTRF as a disturbing new trend[18] at the same time that individual IDTTRF appeared to be declining.[19] The majority of IDTTRF business return activity appears to be associated with Forms 1041, 1120S and 1120. Although the overall number of IDTTRF-related business returns is lower than fraudulent individual returns, the refund amounts being claimed are significantly higher on a per return basis. For reference, in Processing Year 2017, the IRS identified 20,764 fraudulent returns for a total of $2 billion in refunds. The average refund amount claimed on confirmed identity theft Form 1120 returns was $1.3 million.

Business IDTTRF schemes often involve filing a fraudulent business return in the name of a legitimate business to generate refunds that can be subsequently recovered by filing a fraudulent individual tax return using a stolen identity. However, other business IDTTRF schemes seek either to claim refundable business tax credits or to obtain a refund of allegedly overpaid payroll tax deposits previously made by legitimate filers. The IRS and the Security Summit have been working to implement stronger controls to better authenticate business returns.

A large volume of IDTTRF-related business returns also involve the misuse of federal employer identification numbers (EINs) either obtained using stolen SSNs or misappropriated from dormant companies. TIGTA has recommended changes to increase screening filters and make other business improvements in the EIN application process, which ETAAC supports.[20]

Employers and payroll and HR professionals are at increasing risk

Employers and payroll and HR professionals are at increased risk. Criminals have engaged in phishing email schemes that purport to be from company executives and

[18] See https://www.usatoday.com/story/money/2017/07/25/irs-identity-thieves-now-targeting-businesses-partnerships/508348001/. Common business tax forms are: 1120 (Corporation), 1120S (S Corporation), 1041 (Trust), 1065 (Partnership) and 940 and 941 (Employment).

[19] See https://www.irs.gov/newsroom/key-irs-identity-theft-indicators-continue-dramatic-decline-in-2017-security-summit-marks-2017-progress-against-identity-theft

[20] See https://www.treasury.gov/tigta/auditreports/2018reports/201840013fr.pdf

request personal information on employees.[21] Payroll service providers that provide web access to payroll information for their clients and/or their clients' employees have also been compromised.[22]

The IRS has taken some initial steps to integrate the payroll and employment return community more broadly into the Security Summit. More needs to be done.

Security Summit and ISAC expansion make this a good time to ensure alignment

The expansion of Security Summit and ISAC membership presents a good time to review and document the collaborative efforts of these two structures. Given a full year of joint operations, operational lessons learned should be captured and applied to enhance how these two structures operate separately and together. A clear understanding of the respective responsibilities of the Security Summit and ISAC is a critical first step to ensure their alignment and efficient operations, especially as new members and industries join the Security Summit.

The Security Summit and electronic tax administration benefit from innovation

Innovation is required to address the opportunities and challenges facing electronic tax administration, including IDTTRF. Effective innovation requires an efficient process that generates multiple ideas to solve a defined opportunity or challenge, and the rapid and efficient identification of the most promising solutions to test and, ultimately, implement.

The IRS has some statutory authorities that it might leverage to foster innovation in its fight against IDTTRF. Specifically, Title II of the IRS Restructuring and Reform Act of 1998 (RRA 1998) established certain objectives, mandates and authorities for the IRS to accelerate the electronic filing of federal returns and achieve a minimum 80% electronic filing rate.[23] To accomplish this objective, RRA 1998 granted the IRS authorities (among others) to (i) encourage the use of electronic tax administration programs through mass communication and other means, including the payment of incentives for electronically filed returns, and (ii) develop procedures for the acceptance of signatures in digital or other electronic form, including waiving the requirement for a signature for or providing for alternative methods of signing or subscribing particular types or classes of returns or other documents required or permitted under relevant laws and regulations.

The IRS employed these statutory authorities immediately following RRA 1998's passage by creating a vehicle commonly referred to as the "Request for Agreements" (RFA). RFA was a non-monetary program where, without any expenditure of procurement funds, the IRS sought and received pilot proposals to increase electronic filing. If accepted, the IRS would cooperate to enable the submitting organization to implement its pilot, which could include the IRS' granting of incentives. RFAs presented limited risk and cost to the IRS and taxpayers. If the proposal worked, the IRS made

[21] See https://www.irs.gov/newsroom/irs-alerts-payroll-and-hr-professionals-to-phishing-scheme-involving-w2s

[22] See https://krebsonsecurity.com/2016/05/fraudsters-steal-tax-salary-data-from-adp/

[23] Public Law 105-206 (105th Congress) July 22, 1998.

the opportunity more broadly available; if the proposal failed, then the IRS dropped it.

Several examples persist even today that were originally awarded under the RFA program, including access to free tax preparation software and electronic filing and the ability and option to pay one's federal taxes with a credit card. These authorities were also used to define and implement the Authorized IRS e-file Provider Program.

RECOMMENDATIONS

RECOMMENDATION #1: *Integrate the payroll community more broadly into the Security Summit and the ISAC*

> *The IRS should engage and integrate the Payroll Community more broadly into the Security Summit with an initial focus on expanding its participation into reporting key data elements in e-file schemas, leads reporting and ISAC operations.*

Support for Recommendation:

Criminals have increasingly targeted tax preparers and businesses engaged in payroll processing and employment tax return filing – ETAAC sometimes refers to these stakeholders as the "payroll industry." Generally, organizations in this industry fall into three broad groups -- Reporting Agents, tax and payroll professional service providers and individual filers/employers.

Recognizing the risks to the payroll industry, the STAR Work Group created a Payroll Subgroup in 2017. That subgroup is currently focused on implementing NIST controls, in the same way that the Tax Subgroup has been doing over the past few years.

There is an opportunity to integrate the payroll industry beyond the STAR Work Group and into other Security Summit activities. Several areas seem to offer promise – the Authentication Work Group (schema data elements), the Information Sharing Work Group (leads reporting) and the ISAC (IDTTRF reporting and analytics). For example, the payroll industry has existing fraud prevention groups that should be evaluated for potential integration into ISAC reporting and analytical processes. Additionally, at some point, the payroll community should be considered for integration into digital identity management (identity proofing and authentication) given the online solutions they offer to their customers.

However, the IRS' first step to determine how to integrate the payroll industry more broadly into the Security Summit must be 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. The payroll industry has some of the attributes of the tax industry, but it also appears to have some important differences. These differences must be carefully reviewed and understood at the outset.

RECOMMENDATION #2: *Increase outreach to employers and businesses*

> *The IRS should collaborate with the Security Summit to identify ways to increase its outreach to and support of employers and businesses to help them (i) identify potential indicators of fraudulent activities affecting their returns and accounts, and (ii) report quickly and easily to the IRS concerning fraudulent activity on their accounts.*

Support for Recommendation:

Because of the significant risks presented, the Security Summit has focused primarily on taxpayers and the tax preparation community filing individual tax returns.

However, mindful of the evolving threat landscape, IRS has also increased its engagement with small businesses and business return filers. For example, IRS has introduced new data elements for business return schemas to help it distinguish fraudulent and legitimate returns. IRS has also increased its outreach to small businesses in connection with its other Security Summit communications campaigns.[24]

ETAAC supports these efforts and, because of the increasing risk associated with business return IDTTRF, encourages the IRS to find ways to expand the scope and quality of its business outreach with a focus on:

- Continuing to educate businesses and employers on IDTTRF and cybersecurity risks, including existing indicators to help them spot potentially fraudulent activity involving their tax returns or accounts[25]
- Providing clear and simple procedures and mechanisms for businesses and employers to report IDTTRF and remediate their accounts[26]
- Investigating the creation of new indicators or mechanisms to more quickly alert business filers about potential fraudulent activity[27]

Outreach efforts should also include engaging with tax professionals about their role in validating the officers and principals of entities as well as the legitimacy of any associated entities. For example, a tax professional should be suspicious if a million dollar revenue company cannot provide a filing history or prior year return information.

RECOMMENDATION #3: *Ensure the effective operation of the Security Summit and ISAC*

> *The IRS should create consolidated reference materials that explain the purpose, responsibilities and goals for both the Security Summit and ISAC, and for each of their respective work groups and committees.*

Support for Recommendation:

Consolidated documentation is needed for the Security Summit and the ISAC

The Security Summit work groups and the ISAC have been successful in part due to stable team leadership and membership. As time has passed, more turnover among

---

[24] For a few examples, see: https://www.irs.gov/newsroom/national-tax-security-awareness-week-no-5-small-businesses-be-alert-to-identity-theft, https://www.irs.gov/newsroom/dont-take-the-bait-step-3-security-summit-safeguards-help-protect-individuals, and https://www.irs.gov/newsroom/irs-urges-small-businesses-protect-it-systems-from-identity-theft.

[25] IRS has identified a few of these types of indicators in past communications. See https://www.irs.gov/individuals/identity-theft-guide-for-business-partnerships-and-estate-and-trusts

[26] Current IRS guidance on "reporting fraud" seems focused on individuals and preparers, not employers. See https://www.irs.gov/individuals/how-do-you-report-suspected-tax-fraud-activity

[27] Illustration of a mechanism: Many companies (banks, social media, and email providers) provide proactive notifications that inform you of any account profile changes, account accesses, etc.

Security Summit and ISAC participants is occurring as people change jobs or new members join. The loss of this expertise and knowledge, and the time it takes to get new participants up to speed, can adversely affect the Security Summit and ISAC.

One way to minimize the impact of turnover is to have consolidated off-the-shelf reference materials concerning the purposes, responsibilities and goals of the Security Summit and ISAC, and their work groups. These materials would help to ensure a consistent understanding of and alignment between the two structures. For new members, they could be part of an onboarding packet, and supplemented by introductory calls/meetings and other training and education experiences.

Other important points that could be documented at a high level concerning the Security Summit and ISAC (and their committees and work groups) are:

- Structure, governance and operating mechanisms
- Desired qualifications, background and expertise for members of any work groups or committees.
- Workflows and interdependencies (One interdependent workflow is the development and adjustment of Industry Leads schemas.[28])

As it consolidates this documentation, the IRS could also consider the adequacy of ongoing operating mechanisms used by the Security Summit and ISAC to communicate and coordinate their activities.[29] Operating mechanisms can also help manage the direction and progress of initiatives whether through regular reporting or reviews, as well as one off events focused on specific challenges or opportunities.

RECOMMENDATION #4: *Enable collaborative innovation*

> *The IRS should use the authorities granted under Title II of the 1998 IRS Restructuring and Reform Act to create collaborative partnerships and programs, including the re-implementation of its Requests for Agreement Program, to facilitate private sector innovation in pursuit of the IRS' electronic tax administration and IDTTRF goals and objectives.*

Support for Recommendation:

IRS has several areas where public/private collaborative innovation could generate

[28] Illustration: (i) Summit Work Groups create Industry Leads schemas; (ii) ISAC receives Industry Leads files containing schema data, and conducts analytics on the data – ISAC analysis necessarily provides insights into the effectiveness of certain lead categories or reported data elements; (iii) ISAC shares its results with relevant Summit Work Groups; and (iv) Security Summit Work Groups apply lessons learned from the ISAC to the Summit's next iteration of the Industry Leads Schemas.

[29] Past examples of Security Summit and ISAC coordination include: defining membership criteria, reviewing the impact of the Equifax breach, and training state and industry fraud analysts. Specific future opportunities could include: Communicating ISAC activities and findings to help educate tax administrators and industry analysts and to identify opportunities to improve tax administrators' fraud detection during earlier stages of return processing; Communicating ISAC's insight to Security Summit work groups to improve leads reporting (Information Sharing) or return header information (Authentication); Creating a dialog to improve the alerts and Rapid Response program; and, Exchanging information between Security Summit Work Group co-leads and the ISAC Senior Executive Board regarding priorities and progress.

ideas to solve challenges, such as: increasing the electronic filing of employment tax returns (Form 94X); creating more taxpayer-friendly electronic filing instructions; evolving security education requirements for tax professionals; and, leveraging partners to conduct in-person identity proofing.

There are a variety of ways to facilitate collaborative innovation – two come to mind that the IRS has used in the past or is currently using.

First, the IRS could relaunch the RFA program (described in the Introduction above) to solicit and pilot new ideas in a risk-managed setting.[30] RFA's might avoid the burden of permanently changing policy unless and until the IRS determines that a proposed idea is effective. A pre-condition to using RFA's might be the need for the IRS to create expedited processes to develop temporary or trial policies to pilot ideas.

Second, the IRS should continue to look for partnership opportunities given its past history of leveraging partnerships to better serve taxpayers. Two past examples of public/private partnerships in tax preparation are VITA/TCE[31] and Free File.[32] A recent example of a government/government partnership is the integration of the IRS' Identity Theft Affidavit submission process into the FTC's identity theft reporting platform.[33] Collaborative engagement can also be more informal, such as standalone events focused on generating ideas to address specific problems or opportunities.

ETAAC supports the IRS' continued pursuit of these types of collaborative engagements.

II. STRENGTHEN THE CYBERSECURITY OF THE TAX ECOSYSTEM

- Establish a common security standard and the IRS' enforcement authority (Recommendation #5)
- Increase participation in Security Summit cybersecurity initiatives (Recommendation #6)
- Strengthen tax professional security through communications, guidance and required education (Recommendations #7 - #10)

INTRODUCTION

Cybersecurity plays a key role in defending our electronic tax system.

To be effective, cybersecurity requires engagement across the entire spectrum of participants in the tax ecosystem. In addition to tens or hundreds of electronic tax companies (software developers, transmitters, etc.), there are hundreds of thousands of

[30] ETAAC has made similar recommendations in the past to leverage the RFA process. For example, see ETAAC 2011 Report, pps. 32-33, regarding the use of the RFA process as a collaboration model to increase Form 94X e-file.

[31] See https://www.irs.gov/individuals/free-tax-return-preparation-for-you-by-volunteers.

[32] See https://www.irs.gov/filing/free-file-do-your-federal-taxes-for-free.

[33] See https://www.ftc.gov/news-events/press-releases/2018/04/ftc-irs-initiative-aims-make-it-easier-consumers-report-tax and https://www.identitytheft.gov/.

individual preparers, electronic return originators and reporting agents. We need to have active participation across this spectrum of participants, and provide them with more guidance, education and support.

The FTC Safeguards Rule currently establishes a security standard…partially

Effective cybersecurity also requires a clear standard.

The Gramm-Leach-Bliley Act (GLB)[34] was enacted in 1999 and, among other things, mandates privacy and security requirements for businesses providing financial products and services to individuals for personal, family, or household use. Section 501(b) of GLB requires that these financial institutions "protect the security and confidentiality" of nonpublic personal information and directs specified federal agencies to "establish appropriate standards…relating to administrative, technical, and physical safeguards."

Pursuant to GLB, the Federal Trade Commission (FTC) issued the FTC Safeguards Rule (16 CFR 314), which sets a standard for financial institutions to have written security plans, designate information security employees, and conduct safeguard assessments, implementation and monitoring.[35] The FTC has issued implementation guidance, including materials targeted for small businesses.[36]

The FTC has defined "financial institutions" to include tax preparation firms,[37] and brought an enforcement action against a consumer tax software company for its failure to have a security plan and an associated data breach.[38] The FTC has also issued tips for tax preparation firms relating to this action.[39]

However, the FTC's authority does not appear to extend to tax preparers serving businesses only. GLB and the regulations thereunder generally provide that the FTC Safeguards Rule applies to financial institutions (including tax return preparers) serving customers. The term "customer" is defined as a "consumer" who is "an individual who obtains or has obtained a financial product or service (emphasis added)."[40]

The IRS references the requirements of the Safeguards Rule in its e-file guidance

---

[34] Aka the Financial Services Modernization Act of 1999, Public Law 106-102 enacted November 12, 1999.

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

[36] See Start with Security: A Guide for Business (https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf); Data Breach Response: A Guide for Business (https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf)

[37] 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.

[38] See https://www.ftc.gov/news-events/press-releases/2017/08/operator-online-tax-preparation-service-agrees-settle-ftc-charges

[39] See https://www.ftc.gov/news-events/blogs/business-blog/2017/08/4-gramm-leach-bliley-tips-take-ftcs-taxslayer-case

[40] See 16 CFR 313.3(e)(1) and 16 CFR 313.3(h). 16 CFR 314 incorporates these provisions by reference.

IRS Revenue Procedure 2007-40 governs the Authorized IRS e-file Program for both individual (Form 1040 series) and business and employment returns (including Forms 940, 941, 1041, 1065, 1120 and 1120S).[41] Section 5.03 of Rev. Proc. 2007-40 refers to the applicability of the FTC Safeguards Rule and states, in part:

> "The security of taxpayer accounts and personal information is a top priority for the Service. It is the responsibility of each Authorized IRS e-file Provider (Provider) to have security systems in place to prevent unauthorized access to taxpayer accounts and personal information by third parties. The Gramm-Leach-Bliley Act, codified at 15 U.S.C. §§ 6801–6827, includes rules applicable to Authorized IRS e-file Providers that are designed to ensure the security and privacy of taxpayer information. Violation of the provisions of the Gramm-Leach-Bliley Act and the implementing rules and regulations promulgated by the Federal Trade Commission…are considered violations of this revenue procedure and may subject an Authorized IRS e-file Provider to penalties…or sanctions."[42]

There appear to be open questions about the application of the FTC Safeguards Rule to IRS Authorized e-file Providers

There seem to be two ways to interpret Rev. Proc. 2007-40's reference to the FTC Safeguards Rule. Both leave open questions about the IRS' enforcement authority and whether it can extend the provisions of the FTC Safeguards Rule to Authorized IRS e-file Providers serving only businesses (not individual consumers).

Narrow interpretation of Rev. Proc. 2007-40 and related questions

The narrow interpretation of Section 5.03 of Rev. Proc. 2007-40 is that the IRS is merely recognizing only that GLB and the FTC Safeguards Rule apply to those Authorized IRS e-file Providers serving individual taxpayers.[43]

At least one key question remains under the narrow interpretation -- does the IRS have the authority to enforce the FTC Safeguards Rule against these Providers or, alternatively, must the FTC bring any enforcement action?

Support for the IRS' authority to enforce the FTC Safeguards Rule is unclear. With respect to the security regulations issued under Subtitle A, Section 505 of GLB gives the FTC enforcement authority over financial institutions (as defined in GLB) not otherwise subject to functional regulators such as the banking regulators and the SEC. ETAAC could not find any grant of enforcement authority under GLB to the IRS or other agencies generally. In the absence of that authority, the IRS would appear to need to refer enforcement actions under the FTC Safeguards Rule to the FTC.

Of course, Rev. Proc. 2007-40 Section 5.03 may not be suggesting that the IRS believes it can enforce the FTC Safeguards Rule against any Providers. Instead, it may

---

[41] See https://www.irs.gov/irb/2007-26_IRB#RP-2007-40

[42] ETAAC is not aware of any instances where IRS has applied the Safeguards Rule to any Authorized IRS e-file Provider to suspend them from the IRS e-file program.

[43] There are several classifications of Providers under the IRS e-file Program including Electronic Return Originators (EROs), Software Developers, Transmitters and Reporting Agents.

only reflect the IRS' belief that it can suspend any Provider from the IRS e-file Program for failing to comply with the FTC Safeguards Rule.

Broader interpretation of Rev. Proc. 2007-40 and related questions

The broader interpretation of Section 5.03 of Rev. Proc. 2007-40 is that the IRS is extending the FTC Safeguards Rule to Providers serving business and employment taxpayers, presumably under some independent IRS authority.[44] Under this broader interpretation, there are at least two key questions.

The first question is the same one as under the narrow interpretation. That is, does the IRS have the authority to enforce the FTC Safeguards Rule against any Providers or, alternatively, must the FTC bring any enforcement action?

The second question is whether the IRS has the authority to extend the application of the FTC Safeguards Rule to business preparers. Assuming GLB does not grant that authority to the IRS, then the IRS would need to have some independent authority to create security standards. ETAAC has not confirmed the existence (or lack) of this authority.

It is possible that an affected party might claim that the IRS has overstepped its authority and invoke the decision in *Loving v. IRS* which found limitations on the IRS' authority to regulate federal tax preparers. In response, the IRS might assert that it is not "regulating tax preparation" but, instead, regulating the security of electronic tax administration. The IRS has distinguished between return preparation and e-file in the past. IRS Publication 3112 states that Authorized e-file Providers "may also be tax return preparers, but the activities and responsibilities for IRS e-file and return preparation are distinct and different from each other."[45]

In any case, the situation regarding the applicability of the FTC Safeguards Rule and IRS' authority is unclear.

Why this is important…

Criminals are attacking the full spectrum of our tax system – individual, business, employment and information returns.

In the face of this threat, it appears that key segments of the tax and payroll industry may have no legal requirement to have a security plan or program. And, even for those preparers of individual returns who are subject to the FTC Safeguards Rule, there are potential limits on the IRS' ability to implement and enforce security requirements under the FTC Safeguards Rule without involving the FTC. That seems unnecessarily burdensome and complicated. The IRS' authority and responsibility to protect taxpayer information should be crystal clear.

---

[44] Note that Section 5.04 of Rev. Proc. 2007-40 indicates that IRS may define "additional responsibilities" for Authorized IRS *e-file* Providers beyond those set forth in Section 5.03 pursuant to statutes and regulations, revenue procedures, publications, postings to the IRS web site and guidance in the Internal Revenue Bulletin and the Federal Register.

[45] Publication 3112, p. 4. See https://www.irs.gov/pub/irs-pdf/p3112.pdf

RECOMMENDATIONS

RECOMMENDATION #5: ***Establish a common security standard and the IRS' enforcement authority***

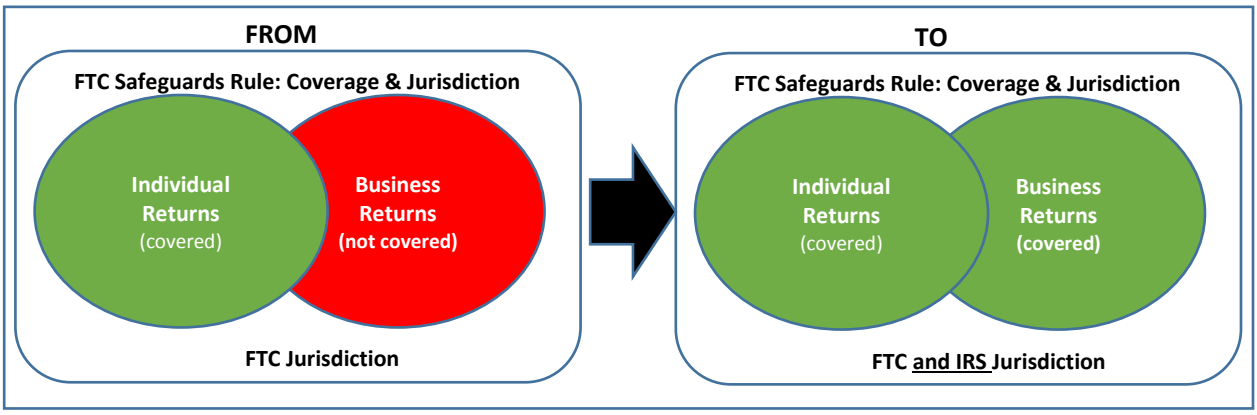
> *Congress should (i) extend the applicability of the FTC Safeguards Rule to all persons providing preparation or filing services for tax returns under the Internal Revenue Code, and (ii) grant the IRS the explicit authority to implement and enforce the FTC Safeguards Rule as so extended.*[46]

Support for Recommendation:

The creation of a more secure electronic tax environment has at least two prerequisites:

- A meaningful common security standard must exist
- The IRS must have the legal authority and responsibility to implement and enforce that security standard across the entire tax ecosystem

As illustrated below, ETAAC has two recommendations: (i) in effect, extend the application of the substantive elements of the FTC Safeguards Rule as a security standard for all persons providing preparation or filing services for tax returns under the Internal Revenue Code (i.e., individual, business, employment, etc.), and (ii) grant the IRS the authority and responsibility to implement and enforce those standards.



The Safeguards Rule is a good starting point for a common security standard

The FTC Safeguards Rule has been an established security standard for over fifteen years. Rather than start from scratch, ETAAC is recommending that the substantive elements of the FTC Safeguards Rule be leveraged and expanded to cover all persons providing preparation or filing services for tax returns under the Internal Revenue Code.

[46] As noted previously, this recommendation is directional. The creation of a tax security standard enforceable by the IRS might be accomplished by expanding GLB and the FTC Safeguards Rule coverage and providing for IRS jurisdiction or, alternatively, through some other legislative approach. ETAAC defers to Congress on the most effective and appropriate legislative approach.

The IRS must have the authority and responsibility to secure our electronic tax system

Additionally, the IRS should have the authority and responsibility to implement and enforce security standards for our tax system – it is much closer to the issues and operations of that system than the FTC.

The IRS' efforts in this area should include helping the tax and payroll community become more secure. There should be a strong focus on collaboratively educating and guiding industry, just as the IRS has done in the Security Summit. One illustration of the IRS' creativity and initiative in the Security Summit is its development of standard policy templates for use by participants in the STAR Work Group. IRS and the STAR Work Group are also developing tools to help companies conduct self-assessments. These types of tools and templates can help accelerate the implementation of the FTC Safeguards Rule.

The requirements of the FTC Safeguards Rule presents other opportunities for common tools and templates. For example, the Rule requires that covered parties "identify and assess the risks to customer information in each relevant area of the company's operation."[47] There's a high likelihood that many tax professional practices operate in similar ways that present common risks. Rather than have individual tax professionals duplicate effort (and cost) by conducting risk assessments from scratch, the IRS could jumpstart the effort by developing baseline risk assessments templates to use as a starting point.

This outreach and guidance effort should not be stymied by concerns that proactive IRS engagement might create risks for the agency. At this stage, inaction by the IRS creates its own set of risks.

RECOMMENDATION #6: ***Increase participation in Security Summit cybersecurity initiatives***

> *The IRS should work with Security Summit members to achieve 100% participation in the current STAR Work Group controls implementation and self-assessment initiatives, including engaging with non-participants to identify and remove barriers, considering ways to increase transparency and providing incentives to increase active participation.*

Support for Recommendation:

STAR Work Group – current focus and progress

In its 2017 Report, ETAAC noted the tremendous progress of the STAR Work Group and reinforced the key elements enabling its success.[48] ETAAC also noted the importance of increasing the participation of Security Summit MOU signatories,

---

[47] See https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

[48] These included: IRS' leadership; Collaborative engagement; A focus on NIST as a single recognized security framework; and, IRS' development of tools to enable industry to implement the NIST controls.

expanding the implementation of enhanced security controls beyond current Summit participants and increasing engagement with the tax preparer community.

Coming into Filing Season 2018, STAR Work Group's two subgroups continued to focus on implementing the NIST security controls. The Tax Subgroup focused on implementing the third, and final, phase of the NIST controls, including the submission of self-assessments for Year 2 controls implementation. The more recently formed Payroll Subgroup focused on implementing the first year NIST controls.

In preparing this Report, ETAAC reengaged with Security Summit leaders from the IRS, States and each of the Tax and Payroll Subgroups to understand the current direction and progress of the STAR Work Group. Most encouraging was the positive response -- key stakeholders strongly value the work and approach of the STAR Work Group and support the Security Summit initiative. Below are a few themes from those discussions.

STAR Tax Subgroup self-assessment participation rate is approximately 70%

About 70% of the tax industry MOU signatories in the Security Summit are submitting annual self-assessments regarding the implementation of the NIST Cybersecurity Framework.[49] These self-assessments play a critical role in this initiative by:

- Measuring industry progress in implementing the specified NIST controls during the three year phase-in period;
- Identifying and overcoming the challenges of applying the NIST government security framework to much smaller private sector organizations;
- Identifying necessary self-help tools to help the private sector more effectively and efficiently implement the NIST controls; and,
- Building State confidence that the Security Summit is the platform for enabling industry to protect taxpayer information and that separate state legislation or regulation is not necessary.

ETAAC would like to see 100% MOU signatory participation in self-assessments. The IRS should work within the Security Summit to identify barriers to and incentives for participation, and evaluate how to provide increased transparency about companies that are conducting self-assessments.[50]

The IRS should anticipate the need to consider other emerging policy issues

State and Industry representatives believe the STAR Work Group should anticipate the need to consider the below emerging policy issues in early 2019.[51]

- <u>Controls Implementation: Required vs. Voluntary</u>: The Security Summit should consider whether, based on the security threats, it is acceptable for any company

[49] As a reference point, state departments of revenue receiving federal tax information from IRS must conduct annual self-assessments pursuant to IRS Publication 1075.

[50] Be aware that many companies active in the Security Summit go well beyond these self-assessments and have periodic security assessments or audits conducted by independent third party security experts.

[51] 2019 will be the third and final year of the Tax Subgroup's implementation of the NIST control framework and associated self-assessments.

not to be in the process of implementing the NIST Cybersecurity Framework, starting with companies that are Security Summit MOU Signatories.

- Assessment Model: Self or/and Independent Assessments: The Security Summit should consider the need for periodic independent assessments to supplement self-assessments.[52] There are various possible models for conducting and funding independent assessments. One example would be having individual companies fund periodic independent assessments using third parties that meet IRS-established qualifications. Another example would be the IRS conducting or funding random spot checks by independent parties to validate the effectiveness of company self-assessments.
- Compliance Model: Validation and Enforcement. Most States are confirming a company's compliance with the Security Summit's controls by requiring attestations in company applications to participate in that state's electronic filing program. These applications are often referred to as a "letter of intent." On a case-by-case basis, individual States decide the consequences of any non-compliance. Ultimately, the IRS may be faced with the same question – will it implement some validation and enforcement model in connection with a company's compliance with the FTC Safeguards Rule or the implementation of NIST Cybersecurity Framework? (If the IRS does not create a single national approach, individual states may go their separate ways which could create a significant increase in compliance burden.)

Generally, these policy issues reflect a need to balance the protection of taxpayer information with the countervailing implementation costs.

RECOMMENDATIONS #7 to #10: *Strengthen tax professional security through communications, guidance and required education*

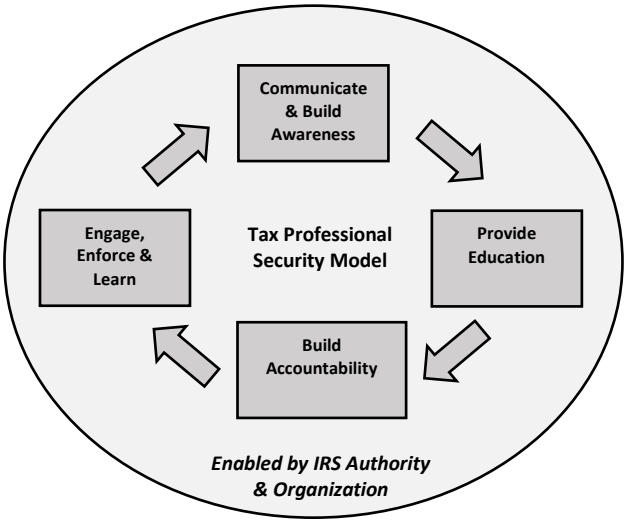
Tax professionals play a key role in tax administration and are at increasing risk

About 700,000 tax professionals prepare just over half of the approximate 150,000,000 individual tax returns filed every year. Additionally, approximately 300,000 Electronic Return Originators (EROs) actively participate in the IRS e-file Program.

Tax professionals and EROs are attractive target for criminals.[53] Every tax professional needs an effective security program, and ETAAC has recommendations to strengthen tax professional security framed around the below Tax Professional Security Model:

[52] In 2011, ETAAC recommended conducting annual self-assessments supplemented by independent assessments every three years, which is consistent with IRS Publication 1075. The final 2011 ETAAC Security Subcommittee Report is publicly available online in the GSA FACA database. See http://www.facadatabase.gov/committee/historymeetingdocuments.aspx?flr=91433&cid=1648&fy=2011

[53] The IRS receives reports every week from tax professionals who have experienced a data theft or loss. See https://www.irs.gov/newsroom/prepared-remarks-of-john-a-koskinen-commmissioner-internal-revenue-service-before-the-irs-nationwide-tax-forum-las-vegas-nevada-august-29-2017. See https://www.irs.gov/identity-theft-fraud-scams/identity-theft-information-for-tax-professionals



RECOMMENDATION #7: ***Communicate and build tax professional awareness***

The IRS should communicate security requirements to tax professionals through all appropriate channels (including their employers) with a clearer, stronger message about their existing legal requirements under the FTC Safeguards Rule, and leverage other regular interactions to reinforce that message, validate awareness and discuss compliance.

Support for Recommendation:

The IRS has taken several steps to inform tax professionals about security

First, the IRS provides general security guidance in several publications. Publication 3112 (IRS e-file Application and Participation) references the applicability of GLB and Rev. Proc. 2007-40 and generally discusses safeguarding taxpayer information with a reference to IRS Publication 4557 (Safeguarding Taxpayer Data).[54] IRS Publication 1345 (Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns) makes a passing reference to GLB and familiarizing oneself with Rev. Proc. 2007-40, but does not outline the FTC Safeguards Rule's requirements.[55] Finally, IRS Publication 4557 contains several security checklists, including ones for Information Systems Security and Computer Systems Security[56] and references elements of the FTC Safeguards Rule and Rev. Proc. 2007-40.

On a related note, ETAAC has previously recommended more frequent or timely updating of security content in IRS publications. It appears that the IRS is now updating online versions of its e-file publications in advance of its issuance of full .pdf print editions. We support this approach. Additionally, whenever the IRS updates its e-file-related publications, including any other relevant requirements or guidance (such as changes to Publication 4557), the IRS should not only display the date of the "Update"

[54] Publication 3112, pps. 19-21. See https://www.irs.gov/pub/irs-pdf/p3112.pdf

[55] See https://www.irs.gov/pub/irs-pdf/p1345.pdf

[56] See https://www.irs.gov/pub/irs-pdf/p4557.pdf

in the online table of contents[57] but also issue a QuickAlert or other communications with a clear notification and explanation of the publication changes.[58]

Second, the IRS has content on its website about identity theft and data security. One section focused on tax professionals provides links to IRS and NIST security publications.[59]

Third, the IRS is executing "Don't take the Bait" and "Protect Your Clients, Protect Yourself" communications campaigns to raise awareness of the need for tax professionals to increase security. These communications alert professionals, sometimes in useful bite-size pieces, about schemes and preventative action. The IRS also communicates security and IDTTRF prevention information through its national tax forums and social media.[60]

Fourth, the IRS has extended continuing education credit for qualified data security courses[61] to Enrolled Agents and to Annual Filing Season Program participants. However, although IRS recognizes security education, its online listing of IRS-approved continuing education providers does not clearly identify those providing security training.[62]

BUT the current approach is not working -- too many are unaware or unprepared

Based on their personal experience and other anecdotal information, ETAAC members believe far fewer than half of tax professionals are aware of their responsibilities under the FTC Safeguards Rule and that even fewer professionals understand their responsibilities and have implemented required security practices. Rev. Proc. 2007-40 states that the security of taxpayer accounts and personal information is a top priority. If so, the IRS needs to take additional steps to protect taxpayers by increasing the security awareness and understanding of tax professionals and helping professionals implement necessary security practices.

---

[57] IRS displays the date of an "updated" section in the publication's online Table of Contents (See https://www.irs.gov/e-file-providers/publication-1345-handbook-for-authorized-irs-e-file-providers-of-individual-income-tax-returns). However, the practice seems inconsistent. For example, Publication 3112 was reissued April 2017. One would assume that the online version of Publication 3112 would be the April 2017 release, but numerous items in the online Table of Contents have dates preceding April 2017 (https://www.irs.gov/e-file-providers/publication-3112-applying-and-participating-in-irs-e-file). These may just be administrative oversights, but can confuse affected stakeholders.

[58] ETAAC could not find any QuickAlerts relating to publication changes in the QuickAlert Library. See https://www.irs.gov/e-file-providers/quickalerts-library.

[59] See https://www.irs.gov/identity-theft-fraud-scams/identity-theft-information-for-tax-professionals

[60] See https://www.youtube.com/watch?v=IEZrN2ThoB4

[61] See https://www.irs.gov/tax-professionals/continuing-education-credit-for-qualified-data-security-courses

[62] See https://www.ceprovider.us/public/default/listing. The "program categories" columns include: federal tax law update, federal tax, ethics, annual federal tax refresher and qualified plan retirement matters. Data security is not separately identified.

The IRS needs to send a clear message about tax professionals' existing security obligations

From ETAAC's perspective, the IRS needs to reinforce that tax professionals have an existing legal requirement to implement a security plan under the FTC Safeguards Rule and emphasize its five key elements.[63]

Current guidance falls short. Publications 3112 and 1345 only generally reference GLB and the FTC Safeguards Rule without any explanation of its specific requirements. Publication 4557 provides more details in its to-do checklists, but these are more an un-prioritized list of actions than a holistic breakdown of the elements of a security plan.[64] All actions are not equal, and the IRS should provide guidance on which of them are most impactful.

The IRS should evaluate additional communications channels and mechanisms

Although it should continue to use its existing channels, the IRS should also examine additional scalable channels to reach specific audiences with targeted messages.[65] For example, the IRS should consider how tax software companies might leverage their products and other customer communications with tax professionals to communicate key security messages and educational opportunities. The IRS could also leverage its "preparer channel" if it started capturing the tax professional's employment relationships in the PTIN system. For example, any company employing or engaging more than a specified number of tax professionals could serve as a direct communications channel to those tax professionals. This approach might enable the IRS to focus its ongoing communications on preparers that are not part of a larger organization and may need more support.

RECOMMENDATION #8: *Require security continuing education*

> *The IRS should require that all tax professionals successfully complete two hours of continuing education in data security annually, potentially as a condition of obtaining or renewing their PTIN or applying for and maintaining their status as an Authorized IRS e-file Provider. Additionally, the IRS should supplement existing security education programs targeted to tax professionals by partnering with the Security Summit to select an experienced private sector expert (whether academic, nonprofit or commercial) to assist in the development of a comprehensive security program of instruction.*

Support for Recommendation:

The IRS' communication campaigns about tax professional security requirements are important, but insufficient. They need to be supplemented with guidance and required education.

---

[63] The five key elements are identified in 16 CFR Section 314.4.

[64] ETAAC's 2017 Report Recommendation #17 (that IRS review and update Publications 1345, 3112 and 4557 to make them more clear and useful) remains relevant.

[65] There are different "preparer" audiences. Typically, the firm is primarily responsible for the overall security environment (IT systems, etc.), while the individual preparer is responsible for handling individual client/taxpayer data within that overall environment.

First, tax professionals need relevant guidance to help them develop and implement appropriate security plans. Current guidance regarding security responsibilities do not sufficiently account for the limitations and challenges of the tax professional audience. For example, tax return preparers and EROs may have very different roles and responsibilities in an overall security plan. Additionally, the quality and actionability of the guidance is mixed. Some IRS security guidance is widely distributed across multiple publications and may be overly technical. The situation leaves tax professionals overwhelmed and unable to prioritize their focus.

Second, tax professionals need access to high quality security education. The private sector today provides many continuing education options for tax professionals including courses focused on data security. However, IRS does not have a comprehensive security course as a standard. To supplement any other independently developed data security courses, IRS should partner with the Security Summit to select an experienced private sector expert (whether academic, nonprofit or commercial) to assist in the development of a comprehensive security program of instruction. Education materials should cover cybersecurity threats, risk assessment and management, cybersecurity best practices, and strategies to detect, prevent and respond to breaches. Then, IRS can use its existing procedures to approve qualifying continuing education courses and providers.[66]

Finally, tax professionals should have a 1-2 hour annual requirement for security continuing education. Targeted education requirements are an established IRS practice. For example, the IRS requires Enrolled Agents and Annual Filing Season Program participants to have a specified number of hours of ethics and professional conduct training each enrollment period.[67] Security should be on the list.

Fortunately, security training lends itself to scalable delivery models, whether in-person workshops or presentations at IRS Tax Forums or online multi-media training targeted to specific audiences (e.g., preparers, administrative staff, EROs, Transmitters, Online Service Providers, etc.).[68]

RECOMMENDATION #9: *Build Accountability…Engage, Enforce and Learn*

> *The IRS should leverage its existing channels and processes to obtain periodic: (i) acknowledgments from tax professionals that they are aware of their security requirements under the FTC Safeguards Rule and IRS publications, and (ii) attestations that they are in compliance with those requirements.*

Support for Recommendation:

Communications, guidance and education are important, but the IRS needs to go further to build a culture of accountability.

Short of requiring security audits, one way to build accountability is to require annual security acknowledgments and attestations from preparers and EROs.

---

[66] See https://www.irs.gov/tax-professionals/irs-continuing-education-providers

[67] See Circular 230, Section 10.6. https://www.irs.gov/pub/irs-pdf/pcir230.pdf

[68] VITA volunteer online tax training is just one illustration of an online delivery model used by IRS.

An annual acknowledgement would be an affirmative statement of awareness and understanding, such as "We are aware of, have reviewed, and understand our security requirements under the FTC Safeguards Rule and applicable IRS publications."

On the other hand, an annual attestation would be an affirmative statement of compliance, such as "We have reviewed the FTC Safeguards Rule and applicable IRS security requirements and, after a review of our operations, attest that our security program is in compliance with those requirements and operating effectively to protect taxpayer information."[69]

For ease and scale, the IRS could obtain acknowledgements or attestations annually in connection with regular administrative interactions with tax professionals. They could be part of the application or renewal process for PTINs, EFINs or the Annual Filing Season Program. The IRS could also leverage other periodic engagements with tax professionals, such as office visits, to educate and evaluate compliance with the FTC Safeguards Rule and capture potential improvements in the program.

RECOMMENDATION #10: *Establish clear IRS internal responsibility*

> *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 of such requirements across IRS stakeholders.*

Support for Recommendation:

ETAAC perceives a multiplicity of owners inside of the IRS relating to the security obligations for tax professionals. For example, if the issue deals with "practitioners," possibly the Office of Professional Responsibility (OPR) is the owner. If it deals with "preparers," possibly the Return Preparer Office (RPO) is the owner. If it deals with "EROs," possibly IRS Electronic Products and Services Support (*EPSS*) is the owner. If it deals with cybersecurity standards, possibly IRS Cybersecurity is the owner.

One illustration of this diffusion of accountability is the IRS' current security guidance for Authorized IRS e-file Providers, which is a patchwork of regulations, revenue procedures and publications.[70] As a result, there is not clear, consistent and coherent security guidance for tax professionals.

Security needs clarity, consistency and coherency. Security policy should not be pieced together by multiple organizations depending on what "hat" a tax professional may be wearing at any given point in time, e.g., preparer, enrolled agent, ERO, etc.

The IRS should have a clear internal "owner" for setting security policy and determining security requirements for all tax professionals. Once set, those policy and requirements can be communicated and implemented consistently across the various internal IRS organizations -- OPR, RPO, EPSS, etc.

---

[69] By comparison, the attestation required in the FTC enforcement action against a tax software company stated that the "security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected."

[70] See Recommendation #17 in ETAAC's 2017 Report.

III. IMPROVE IDTTRF DETECTION, ANALYSIS AND REPORTING

- Enact an IRC Section 6103 IDTTRF exception (Recommendation #11)
- Improve detection with enhanced business tax schema data elements (Recommendation #12)
- Enable third party EFIN and PTIN validation (Recommendation #13)

INTRODUCTION

The ISAC plays a key role in identifying and helping stop fraudulent schemes

The ISAC plays a key role in detecting fraudulent schemes because of its visibility across the tax ecosystem and its analytical capabilities. Traditionally, IDTTRF prevention has been measured using key outcome metrics such as the number of fraudulent returns identified and the dollar amount of fraudulent refunds stopped. As the ISAC evolves, additional metrics must be developed that take into account its focus on inputs to those outcome metrics, such as the number of schemes identified or disrupted.

IRC Section 6103 is designed to protect taxpayers, but also impacts IDTTRF

Sharing information is a critical enabler in the fight against IDTTRF. In 2017, ETAAC recommended that the IRS identify and, where possible, mitigate the barriers affecting the IRS' ability to share vital IDTTRF information with the ISAC.

A primary barrier to IRS information sharing is IRC Section 6103.[71] IRC Section 6103 protects taxpayers by restricting the use and disclosure of tax returns or tax return information[72] by the IRS unless a specified exception applies.[73] These exceptions are carefully crafted to protect taxpayers while enabling certain activities that are vital to the proper operation and integrity of our tax system. IRC Section 6103 also provides for severe penalties if either tax returns or return information is disclosed inappropriately, including felony charges, fines, and termination of employment.

The IRS correctly scrutinizes any proposed data uses or disclosures to ensure they fall within the permitted scope of IRC Section 6103. However, as explained below, IRC Section 6103 may be creating unintended barriers in the effort to improve cybersecurity and prevent IDTTRF. ETAAC believes that an appropriate balance can be struck that both protects taxpayers from improper use and disclosure of their tax information, while enabling the IRS to prevent IDTTRF (which also causes serious injury to taxpayers).

[71] IRC Section 6103 is codified at 26 U.S.C. Section 6103.

[72] See IRC Section 6103(b)(1) and (2) generally.

[73] See https://www.irs.gov/government-entities/federal-state-local-governments/disclosure-laws

Enhanced data element reporting in business tax return schemas would enable the IDTTRF fight

Incidents of confirmed identity theft in individual tax returns continue to decline.[74] ETAAC believes one of the factors contributing to this decline is the transmittal to the IRS of additional critical data elements to authenticate individual returns.

Likewise, the addition of new data elements to (or the required reporting of currently optional data elements in) the Business Master File (BMF) schemas could enable more effective authentication and help to prevent business return IDTTRF.

EFINs and PTINs are important in identifying and validating EROs and preparers

An Electronic Filing Identification Number (EFIN) is issued by the IRS in connection with its electronic filing program. Any tax return preparer expecting to file eleven or more Form 1040/1041 returns must e-file them. In order to e-file returns, the returns must be transmitted through an Authorized IRS e-file Provider (Provider), which is a business or organization (firm) accepted by the IRS to participate in IRS e-file Program. The responsible official of the firm must submit an e-file application, meet certain eligibility criteria and pass a suitability check before the IRS will assign an EFIN. EFINs must be included with all electronic return data transmitted to the IRS.

In contrast, a Preparer Tax Identification Numbers (PTIN) is a number issued by the IRS to paid tax return preparers. It is used as the tax return preparer's identification number and, when applicable, must be placed in the Paid Preparer section of a tax return. Obtaining a PTIN requires that the preparer verify his or her identity with the IRS.

EFINs and PTINs play a role in the fight against fraudulent and improper activity

Unfortunately, EFINs can be subject to improper use. In more benign settings, preparers not formally affiliated with an EFIN might use or "share" an EFIN to transmit legitimate returns, i.e., this is an unauthorized use of the EFIN. On the other hand, EFINs can be compromised, and then used to file fraudulent tax returns.

Within the IRS, a compromised EFIN could be identified in various ways, such as through a criminal investigation, a preparer audit, or IDTTRF analytical processes. Outside of the IRS, a transmitter or ERO could identify a misuse by comparing the number of returns reported on its e-services account with the number of returns it knows has been filed from its offices (an indication that someone else has been filing returns under their EFIN).

Once an EFIN anomaly has been identified, it must be researched, confirmed and addressed. If an EFIN is determined to be compromised, IRS Electronic Products and Services Support (EPSS) will attempt to contact the firm, inactivate the EFIN, issue a new EFIN and notify the firm. EPSS will also review the situation to determine if further action is necessary, such as a fraud referral.

Before they ever file a fraudulent return, criminals possessing a compromised EFIN may try to license professional tax software.[75] To stop this type of scheme, tax software

[74] See About the IRS Security Summit section of this Report.

[75] Professional tax software is designed to prepare, queue and e-file large volumes of returns.

companies currently conduct a manual process to collect information and documentation from potential customers and validate they have legitimate EFINs. Due diligence could include reviewing a printout of EFIN information from an IRS e-services account or identification documents. But this process has gaps -- it does not enable the software company to validate the information directly with the IRS.

Similarly, in an IDTTRF setting, PTINs can be appropriated and misused by persons preparing returns. Because of the sensitive information handled by tax preparers, firms that hire preparers want to ensure their potential employees have valid PTINs. It is one more step an employer can take to ensure the integrity of their firm because of the IRS' due diligence before issuing a PTIN.

ETAAC believes there are opportunities to enhance IDTTRF prevention by enabling more proactive approaches to deal with EFIN and PTIN validity issues.

RECOMMENDATIONS

RECOMMENDATION #11: *Enact an IRC Section 6103 IDTTRF exception*

Congress and the Department of the Treasury should make targeted legislative and regulatory changes, respectively, to permit appropriate use and disclosures under Internal Revenue Code Section 6103 to enable appropriate tax administration cybersecurity and IDTTRF prevention activities.

Support for Recommendation:

IRC Section 6103 presents barriers to IDTTRF detection and prevention

IDTTRF causes serious injury to large numbers of taxpayers. The legitimate taxpayer must complete a time-consuming and document-intensive process to prove his or her identity to the IRS if an IDTTRF return is filed in their name. Additionally, refund delivery may be delayed by months, which is a serious financial burden on lower and moderate income families living paycheck-to-paycheck and relying on tax refunds (including refundable tax credits) to make ends meet.[76]

The Security Summit has demonstrated that the IRS, States and Industry can detect and prevent IDTTRF at higher rates by working collaboratively. Sharing targeted data elements about compromised returns can help stakeholders identify IDTTRF schemes and patterns and distinguish them from legitimate returns, which reduces the false positives that adversely impact legitimate taxpayers.[77]

IRC Section 6103 affects the IDTTRF collaboration of the IRS, States and Industry.[78] Currently, the IRS is unable to share return-level information involving suspected or confirmed IDTTRF with the ISAC or elsewhere in the Security Summit. Instead, the IRS may only share relevant details regarding confirmed IDTTRF with states and the vendor

[76] Examples: Earned Income Tax Credit, Child Tax Credit and American Opportunity Tax Credit.

[77] Even legitimate tax filings can trigger IRS flags for potential fraud and create "false positives" despite IRS and State efforts to avoid them. Additional data sharing can help reduce false positives and the harm they cause to legitimate taxpayers.

[78] IRS Office of General Counsel Memorandum Number AM2017-004, Released 8/25/2017 is an example of some of the current complexities of the application of current IRC Section 6103. See https://www.irs.gov/pub/lanoa/am-2017-004.pdf

whose software was used to file the fraudulent returns. This prevents the sharing of key IDTTRF information with other tax software developers and electronic filing transmitters who might also be receiving fraudulent returns with similar characteristics. In the case of financial institutions, the IRS cannot share any information, which is a barrier to financial institutions effectively identifying accounts linked to fraudulent returns. All of these situations make it more difficult for Security Summit participants and the ISAC to see the broader picture, and identity IDTTRF patterns and schemes.

The ISAC's pilot operations have reinforced how IRC Section 6103 has prevented ISAC participants from having a holistic, high-level view of the IDTTRF being attempted across the tax ecosystem. Ironically, because of the limitations on sharing, the ISAC has not been able to fully assess the extent to which IDTTRF schemes have been undetected because of insufficient IRS-provided data within the ISAC.

A carefully crafted IRC Section 6103 exception could also enable the sharing of information useful in enhancing cybersecurity.

Data sharing within the ISAC process makes a difference in the IDTTRF fight

The work of some State and industry ISAC members anecdotally illustrates the opportunity presented by expanded information sharing.

After the 2017 filing season, a state and industry work group of ISAC members studied a sample of returns identified as fraudulent by one of the states to determine if schemes or IDTTRF networks could be detected. The goal of the work group was to identify what additional data elements would help identify fraudulent returns earlier in the season. Using the state-provided data,[79] the work group was able to link the fraudulent return information to specific bank accounts, software vendors and other state returns.

As expected, the most useful data elements included: name, address, social security number, PTIN, and bank account number. None of these data points can currently be shared by the IRS into the ISAC.[80] The work group suspects, based upon the information available to them, that most of the returns were likely filed with the IRS as well. But, again, the work group was not able to confirm that fact because of information sharing limitations.

ETAAC believes appropriate and principled changes can be made to IRC Section 6103

A carefully crafted exception could be added to Section 6103 to provide the IRS with the authority to make appropriate uses and disclosures of tax and return information to enhance cybersecurity and detect and prevent IDTTRF.

The implementation of any IRC Section 6103 IDTTRF exception should follow some guiding principles to ensure continued taxpayer protection, whether implemented by regulation, IRS guidance (e.g., publication, revenue procedure, etc.) or written agreement:

[79] The state-provided data was not subject to Section 6103, and was disclosable under state law.

[80] Some states may also be limited in their ability to share return-level data based on their state laws.

- Any IRS disclosures and recipient uses of information should be carefully defined, e.g., limited to a clear, stated IDTTRF-prevention purpose.
- Any recipients of the information should have a need to know and meet requirements set by appropriate means, e.g., regulation, IRS publication, written agreement, etc.
- Any analytics performed on the information should be conducted in accordance with standards approved by the IRS.
- The amount of information disclosed should be the minimum reasonably necessary to enable the recipient to take appropriate action to detect or prevent IDTTRF. For example, instead of entire tax returns, disclosures should be limited to the minimum number of data elements reasonably necessary to detect schemes, unless another exception applied.
- Any changes to IRC Section 6103 and associated regulations should allow some flexibility for the IRS to establish and adjust practices in response to a constantly shifting IDTTRF environment.
- Recipient security and privacy (use and disclosure) practices should meet minimum standards established by law, regulation or otherwise by the IRS to ensure the protection and appropriate use of taxpayer and return information. These practices should be subject to review or audit by qualified parties.
- Information disclosed by the IRS to approved recipients should not be further disclosed to any third party not approved by the IRS or subject to an existing exception.

ETAAC is aware that the House of Representatives is considering legislation in this area, and supports that effort.

RECOMMENDATION #12: ***Improve detection with enhanced business tax schema data elements***

> *The IRS should work with Security Summit partners to evaluate the need to require the reporting of certain data elements in business income tax schemas, and to establish a business return leads reporting process to enable analysis by the Security Summit and ISAC.*

Support for Recommendation:

The Authentication Work Group's Business Subgroup has identified 22 additional optional data elements that might be sent to the IRS and States – some could be automated while others would require manual entry by the preparer.

Requiring the transmittal of additional data elements has an impact across the entire tax ecosystem. Any user-based field adds a new burden on the taxpayer and/or the tax preparer, and can increase the time necessary to complete a return. Additionally, there are programming complexities associated with any automated technical implementations for both the IRS and software companies.

However, if optional reporting participation is low, the IRS may not be able to analyze the relevance and impact of these incremental data elements in preventing IDTTRF.

For that reason, the IRS should continue to work within the Security Summit framework to determine whether some or all of the proposed business-related data elements should be mandatory to report.

Given the increase in business IDTTRF, the IRS should also evaluate the benefits of establishing a business return leads reporting process comparable to the existing individual return leads reporting process.

RECOMMENDATION #13: ***Enable third party EFIN and PTIN validation***

> Recommendation #13: *The IRS should collaboratively develop and implement a plan to enable real-time electronic EFIN and PTIN validation by authorized third parties.*

Support for Recommendations:

EFIN Validation

Protecting the integrity of EFINs is important to IDTTRF prevention. The IRS recognizes this necessity by requiring Providers to conduct due diligence that they are engaging with other authorized Providers, e.g., "Transmitters must ensure they are transmitting only for Providers."[81]

However, even the IRS acknowledges the imperfections in its current model for verifying EFINs. IRS Publication 3112 notes that "Providers can also confirm EROs using the Authorized IRS e-file Provider Locator at IRS.gov" but then notes the potential gaps in the Locator's data[82] and apparent limitations on the IRS' ability to confirm a Provider's legitimacy.[83]

Authorized software developers face a significant challenge to validate tens of thousands of EFINs when persons or firms attempt to license their professional tax software.[84] These companies must conduct time consuming and potentially imperfect manual processes to attempt to validate the EFIN of each licensee. Additionally, a second EFIN validation may be required if an EFIN is compromised during the filing season and the legitimate firm is reissued a new EFIN.

Building on the recent enhancements to this process, the integrity and speed of the EFIN validation process would be significantly enhanced by the creation of a database that could be "pinged" by authorized companies to validate EFIN holders at the time of EFIN setup.

ETAAC has concerns that a lack of IRS funding or development resources could be an insurmountable barrier to this initiative. As an alternative to an IRS-developed database/system, the IRS should evaluate other opportunities to create such a

---

[81] See IRS Publication 3112, p. 13.

[82] "If an ERO cannot be found it may still be an Authorized IRS e-file Provider as EROs may elect not to be included on the Authorized IRS e-file Provider Locator." IRS Publication 3112, p. 13.

[83] "The IRS can advise if the firm is an Authorized IRS e-file Provider only if it is on the Authorized IRS e-file Provider Locator." IRS Publication 3112, p. 13.

[84] EFIN validation also typically occurs when tax professionals attempt to sign up with an e-file transmitter separate from their software provider or with a financial institution to participate in a tax-related financial product program.

database[85] for use by tax software providers and financial institutions to screen potential customers. Regardless of how this solution is implemented, if the EFIN could not be validated using this database, then the stakeholder would know that additional due diligence is required before initiating a business relationship.

As a side note, the Security Summit Authentication Work Group has been developing solutions to assist in the authentication of EFINs on e-filed returns by validating a vendor control number appended to the e-filed return. This process is well underway and should continue to be developed. The results of these efforts will be monitored in subsequent tax seasons.

PTIN Validation

Currently, a firm hiring a preparer uses manual processes to confirm that a potential new hire has a valid PTIN. As a result, the same benefits noted above concerning real-time validation of EFINs applies to the validation of PTINs. An automated PTIN validation system would enable all those who employ preparers to conduct their due diligence much more quickly and accurately, whether they are large CPA firms, small tax businesses or national or regional branded retail preparers.[86]

Reporting and Response

Because a compromised EFIN or PTIN can be an IDTTRF indicator, information about compromised EFINs and PTINs must be communicated quickly across the tax ecosystem. Currently, separate processes exist for notifying a legitimate EFIN holder and state departments of revenue of a compromise. The timing of these notification processes can vary significantly.

The ISAC is in the early stages of issuing alerts about compromised EFINs and PTINs. This type of alert is relatively new, and requires further assessment to determine its value in the fight against IDTTRF. Hypothetically, reporting information on compromised EFINs and PTINs could provide early warning of issues, and improve the speed of reporting and the ability of impacted stakeholders to act more quickly.

The Security Summit and ISAC should continue to evaluate the effectiveness of these alerts, and consider how to integrate them into existing reporting processes.

[85] If within the scope of appropriate activities, it may be feasible for the ISAC to host a copy of IRS' EFIN database, and create an API or similar capability to provide a solution for the validation of EFINs and confirmation of related information.

[86] The process for real time validation of EFINs and real time validation of PTINs appear to be very similar. As such, there may be an opportunity to build one solution that would support both purposes, thereby optimizing costs and resources.

IV. ENABLE ELECTRONIC TAX SERVICES AND ELECTRONIC FILING

- Continue to enhance identity proofing and authentication (Recommendations #14 - #15)
- Enable the development of online tools (Recommendation #16 - #18)
- Increase the electronic filing of employment returns (Recommendation #19)

INTRODUCTION

Future State and IRS online services

The IRS Future State initiative envisions the IRS' customer service concept of operations for delivering services for all taxpayers whether in-person or online.[87]

Under Future State, the IRS continues to enhance its online services for individual taxpayers, including online access to account information and online payments. For the 2017 fiscal year, the IRS indicated that 79% of taxpayers "self-assisted" (including automated calls). The IRS also reported there were 331 million online "electronic transactions," of which 279 million were for the Where's my Refund? look-up feature (i.e., 84% of all online electronic transactions).[88] Despite their volume, "Where's my Refund?" and similar self-assistance are likely not fully replacing the need for taxpayer communication with a person at the IRS. Given that, the IRS may need to develop more nuanced qualitative metrics regarding the impact of online self-assistance on taxpayer demand for in-person contacts.

We commend the IRS' progress and care in developing the digital channel as a service enhancement rather than service barrier. The IRS seems to be listening to the concerns of the Taxpayer Advocate and others that some taxpayers, often the most vulnerable, will face obstacles to service and ultimately to tax compliance if the Future State goes wrong or they lack access to service channels that best meet their needs.

Remote Identity Management is a key enabler of IRS Future State

Because it necessarily involves expanding online and mobile services, one of Future State's key enablers is the IRS' ability to remotely *identity proof* and *authenticate* taxpayers in a secure and reliable manner.[89]

Remote "identity proofing" is particularly challenging. It is the process by which the IRS collects, validates, and verifies information about a taxpayer to ensure the applicant is who they claim to be to a stated level of confidence.[90]

---

[87] IRS News Release "Tax Professionals Provide Insights on IRS Future State; Feedback Efforts Continue in 2017 as Online Account Shows Strong Early Use," Dec. 21, 2016 (https://www.irs.gov/pub/irs-news/ir-16-174.pdf). See also https://www.irs.gov/newsroom/irs-future-state

[88] IRS Data Book FY 2017, Table 19. Selected Taxpayer Assistance and Education Programs, by Type of Assistance or Program, Fiscal Year 2017 (https://www.irs.gov/statistics/soi-tax-stats-irs-data-book).

[89] References to "taxpayers" includes any representatives that taxpayers authorize to access taxpayer information, e.g., tax professionals and other service providers.

[90] See generally the NIST SP 800-63 *Digital Identity Guidelines* at https://pages.nist.gov/800-63-3/

NIST Special Publication 800-63A depicts the identity proofing process in the following graphic:

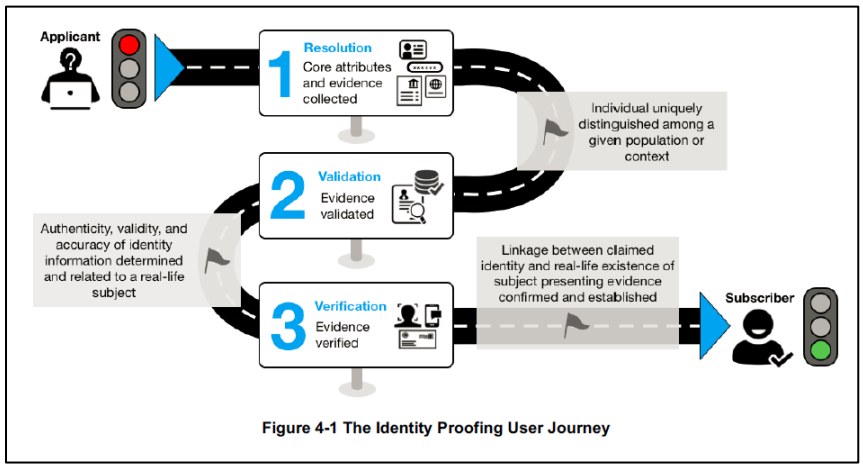


Figure 4-1 The Identity Proofing User Journey

By contrast, remote "authentication" is the process of determining the validity of one or more authenticators used to claim a digital identity. Where services involve return visits, successful authentication provides reasonable risk-based assurances that the person accessing the service today is the same person who accessed the service previously. The ongoing authentication of subscribers is central to the process of associating a subscriber with their online activity.

Digital Identity Management is challenging and continuously evolving

Digital identity management presents a technical challenge because it involves proofing and authenticating individuals over an open network, which presents opportunities for impersonation and attacks leading to fraudulent claims of a subject's digital identity.

Recently issued NIST SP 800-63-3 sets the federal government requirements for digital identity management by specifying "levels of assurance," and associated Identity Assurance Levels and Authentication Assurance Levels depending on the nature of information being accessed.

The IRS has several online services with different levels of assurance. Some services provide access to less sensitive information such as refund status whereas others enable a taxpayer to pay a tax bill online. Some services require the highest level of assurance because of the sensitivity of the information, e.g., Get Transcript Online, Get an IP PIN, IRS e-Services and the taxpayer online tax account.

Highly sensitive information services require a higher level of assurance. The IRS' current remote identity proofing solution is the Secure Access identity management platform. Generally, Secure Access requires the taxpayer to successfully complete a process of validating one's self using personal information, an email address, third party public information and a cell phone.

The IRS has a focused effort to implement digital identity management solutions

ETAAC engaged with Security Summit leaders to understand the current direction and progress of its identity management initiatives. Several insights emerged.

- NIST 800-63-3 is more than just a revision: NIST 800-63-3 is essentially a rewrite of the previous requirements and presents significant implementation challenges. The IRS is working closely with NIST to understand and apply these new requirements.
- Secure Access has its limitations: The IRS has constantly evolved its current Secure Access identity proofing platform,[91] which has its limitations.[92] For example, certain segments of the population may not be able to validate themselves digitally using Secure Access because of an insufficient public record or an inability to complete cell phone validation – currently only about 30% are successful.[93]
- The IRS is attacking the challenge with the right mindset: The IRS is taking a thoughtful approach as it looks for ways to both protect taxpayer data and, simultaneously, enable more taxpayers to identity proof remotely (or otherwise access needed online services). The IRS is open-minded about other solutions under development in the government and private sector spaces.[94]
- The IRS is working collaboratively in this area: Identity proofing is a challenge that requires significant resources. ETAAC agrees with the current approach of the Security Summit's Authentication Subgroup -- government agencies are best positioned to undertake the development and management of identity proofing platforms, while industry participants should focus on authentication platforms.

As noted in the Progress on ETAAC 2017 Recommendations section of this Report, the IRS intends to conduct further research into the AGI/SS PIN taxpayer signature model and partner with the Security Summit to determine the feasibility of replacing it. Given potential synergies, the IRS should consider making finding a replacement for the AGI/SS PIN taxpayer signature part of Security Summit authentication initiatives.

Collaboration, innovation and funding will be required

Identity management solutions are rapidly evolving. The IRS should continue to collaborate with key stakeholders to identify, test and implement new identity proofing and authentication solutions. This innovation effort should be done in a way that manages risks, but stakeholders should not expect zero defects. Innovation necessarily involves a mix of successes and failures.

Additionally, the IRS must be sufficiently funded to execute any tests and pilots.

[91] See, for example, "Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented," TIGTA Report Ref. No. 2018-20-007 (February 5, 2018).

[92] See National Taxpayer Advocate, Annual Report to Congress 2017, Volume 1, Most Serious Problem #3 (Online Accounts).

[93] See National Taxpayer Advocate, Annual Report to Congress 2017, Volume 1. p. 42.

[94] One relatively new government solution under development is "Login.gov." See https://login.gov/

The electronic filing of employment tax returns must be increased

The Form 94X[95] employment return series constitutes the largest number of tax returns filed with the IRS after the Form 1040 series (See Progress Toward 80% E-file Goal section of this Report). Substantially lower electronic filing rates for employment tax returns has been an issue for years. The estimated e-file rate for the Form 1040 series is approaching 90%. In contrast, the estimated e-file rate for employment returns (Forms 94X) languishes around one-half that amount. One impact of low Form 94X e-file rates is higher paper processing costs for the IRS. Based on certain assumptions, ETAAC estimates the IRS could save about $10 - $15,000,000 annually if the Form 94X returns were e-filed at the same rate as Form 1040.[96]

Increasing Form 94X e-file rates is not a new topic for ETAAC. Unfortunately, there is no silver bullet, and the IRS must overcome policy, process and systems barriers.[97] As ETAAC noted in 2011, increasing the electronic filing of Forms 94X requires that "the entire end-to-end e-file registration, filing and payment process be incredibly easy and convenient – it is in competition with a simple form, a pencil, an envelope and a stamp." At that time, ETAAC recommended that the IRS work with key stakeholders to increase IRS outreach and industry promotion of electronic filing, and simplify the application and filing process.[98]

In response to the IRS' March 2015 request for comment concerning ways to increase electronic filing of employment returns,[99] the American Payroll Association (APA) reinforced that the IRS should focus on streamlining its administrative processes. [100] APA also noted that employers will continue to file on paper unless and until the IRS' process is substantially less cumbersome and time consuming.[101]

Most recently, an ETAAC member from the payroll professional community did a quick pulse survey of about 50 colleagues at a payroll conference. Again, the pulse survey identified the need for the IRS to reevaluate and analyze its current e-signature requirements for the 94X series. Payroll professionals noted that there is no signature

---

[95] "Form 94X" refers generally to Form 940 Employer's Annual Federal Unemployment (FUTA) Tax Return, Form 941 Employer's Quarterly Federal Tax Return and related returns.

[96] Current shortfall in Form 94X e-file rate is ~14,000,000 returns @ $1/return based on following rough assumptions and data from IRS Publication 6186 2017 Update (revised 11-2017) : (i) ~31M total Form 94X returns filed annually (paper and e-file); (iv) ~27M Form 94X would be e-filed based on an 88% Form 1040 e-file rate; (iii) ~13M Form 94X returns are currently e-filed annually; and (iv) Form 94X per return net cost savings of $1.00 if returns were filed electronically vs. paper (rough estimate based on ETAAC's 2011 estimate of $1/return savings and most recent IRS information).

[97] There is at least one "systems" challenge -- IRS' e-file system cannot accept Form 94X amendments.

[98] ETAAC 2011 Report, p. 26.

[99] See Federal Register Notice "Proposed Collection; Comment for Electronic Filing of Employment Tax Family (94x) Returns," 80 F.R. 12062, March 5, 2015.

[100] Letter from American Payroll Association to IRS dated May 1, 2015. APA is a nonprofit association of over 20,000 payroll professionals *responsible* for *paying* an *aggregate total* of about *one-third* of the *private sector workforce.*

[101] Similarly, ETAAC's 2015 Report stated that a "free file option for 94x returns [would] not materially impact the e-file rate for these returns, because it would not address what ETAAC considers to be the main barrier to electronically filing these returns, which is the e-signature process." p. 4.

verification with paper returns, yet the IRS currently requires an extensive authentication process to verify signatures on business tax returns. Tax filers suggested several existing processes could be leveraged to mitigate the current requirements.[102] Although free options were attractive, it was equally clear that any solution must also be easy to use because Form 94Xs are relatively simple forms that can be completed by hand in minutes and dropped in the mail.[103]

RECOMMENDATIONS

RECOMMENDATIONS #14 – 15: *Continue to enhance identity proofing and authentication*

> Recommendation #*14*: *The IRS should 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.*
>
> Recommendation #*15*: *The IRS should extend eligibility to obtain an Identity Protection Personal Identification Number (IP PIN) to all individual taxpayers.*

Support for Recommendations:

Remote identity proofing solutions have inherent limitations and challenges

Currently, taxpayers that successfully identity proof and authenticate themselves can gain online access to their tax accounts and other types of information. To be validated, the taxpayer must complete the IRS' Secure Access platform, which requires the taxpayer to pass through a series of validations.[104]

Unfortunately, taxpayers have difficulty navigating Secure Access, which is a major roadblock in increasing the utilization of online accounts. Some taxpayer demographics may not have the required information or tools. Granted, the IRS has created a backstop for taxpayers who cannot successfully complete Secure Access online by sending access codes by mail. But even this process presents its own challenges.[105]

The IRS should consider in-person identity proofing alternatives

Although it should continue to evaluate online remote options to identity proof, the IRS should also consider options to expand in-person identity proofing opportunities.

---

[102] Some quick ideas included: (i) Evaluating current e-services for tax professionals and the secure log-in processes for employers to enable the use of fillable forms or the ability to upload PDF forms for 94X returns; (ii) Utilize existing secure EFTPS portal for 94X filing; and (iii) Reassess the e-file authentication process to find a compromise between no signature verification on paper forms and an extensive signature verification on e-file business return forms.

[103] Attempting to substitute a new "free" electronic taxpayer experience that is more difficult than the current paper and pencil experience will not be successful.

[104] See https://www.irs.gov/individuals/secure-access-how-to-register-for-certain-online-self-help-tools

[105] The Taxpayer Advocate reports that the success rate drops to twenty seven percent for those opting for a letter. See National Taxpayer Advocate, Annual Report to Congress 2017, Volume 1. p. 42-43.

The IRS could leverage its existing physical locations for this purpose. As reported by the Taxpayer Advocate, the IRS has about 375 Taxpayer Assistance Centers (TAC).[106] However, the Taxpayer Advocate also identified the IRS' geographic footprint as one of the agency's "Most Serious Problems."

The IRS could consider leveraging the local offices of other government agencies. For example, the Social Security Administration reports that it has about 1,230 field offices – three times the number of IRS TACs.[107] Even so, getting to any federal office may be a challenge for some taxpayers, especially the elderly or low income.

Another option for the IRS to expand its effective footprint would be to create a "Trusted Third Party" program to expand the availability of in-person taxpayer identity proofing.

A comparable model already exists. The IRS previously created a Certified Acceptance Agent (CAA) Program to improve access to Individual Taxpayer Identification Numbers (ITINs). A CAA is a person or an entity (business or organization) who, pursuant to a written agreement with the IRS, is authorized to assist individuals who do not qualify for a Social Security Number but still need a Taxpayer Identification Number (TIN) to file their taxes. The CAA facilitates the application process by reviewing the necessary documents, authenticating the identity when possible and forwarding the completed forms to the IRS. Applicants to become a CAA must complete a rigorous application process, including submitting an application and finger print cards, as well as completing mandatory training.[108]

In the case at hand, most taxpayers expect their tax professionals or tax service providers (whether paid practitioners, software providers or volunteers in the VITA, TCE or LITC programs) to assist them with accessing information from the IRS. Since these third parties are reviewing physical identification documents already, or may have methods for confirming identity not readily available to the IRS, they represent a possible opportunity to help identity proof taxpayers. The IRS should evaluate this option and consider starting with a small pilot program to test the concept. Any program should also require that any tax partners meet the IRS' security requirements.

The IRS should expand Identity Protection PIN (IP PIN) eligibility

The IRS uses the IP PIN to confirm taxpayer identity when it receives a return from an IP PIN holder. The IP PIN is intended to prevent IDTTRF criminals from obtaining a fraudulent refund using a legitimate SSN and to avoid delays issuing a legitimate refund.

Currently, taxpayers are eligible to receive an IP PIN if: (i) the IRS sent the taxpayer a CP01A Notice[109] containing his/her IP PIN, (ii) the IRS sent the taxpayer a letter inviting him/her to 'opt-in' to get an IP PIN, or (iii) the taxpayer filed a federal tax return last year as a resident of Florida, Georgia or the District of Columbia. The eligibility of FL, GA or

[106] See National Taxpayer Advocate, Annual Report to Congress 2016, p. 88.

[107] See https://www.ssa.gov/org/

[108] See https://www.irs.gov/individuals/international-taxpayers/how-to-become-an-acceptance-agent-for-irs-itin-numbers

[109] See https://www.irs.gov/pub/notices/cp01a_english.pdf

DC residents is part of an IRS pilot[110] and does not require that the recipient be an identity theft victim.

The National Taxpayer Advocate has recommended that the IRS "[e]xpand the IP PIN program by offering it to all taxpayers to proactively protect their tax accounts against tax related identity theft."[111]

ETAAC agrees with the Taxpayer Advocate – the IRS should expand IP PIN eligibility to any taxpayer who desires one. ETAAC views this as a proactive low-tech option to protect taxpayers.

RECOMMENDATIONS #16 – 18: *Enable the development of online tools*

> Recommendation #16: *The IRS should increase and deepen its collaborative engagement with stakeholders concerning the features, design and implementation of the IRS' digital services, including being more transparent about and publicly reporting on goals for both customer service metrics, stakeholder feedback and other key elements that inform its digital strategy.*
>
> Recommendation #17***:*** *The IRS should prioritize the development of an electronic means to submit and accept powers of attorney.*
>
> Recommendation #18***:*** *The IRS should continue its investigation and development of a lock/unlock feature for individual and business taxpayer accounts.*

Support for Recommendations:

Digital Services Collaborative Engagement

Research Efforts

The IRS seems to recognize the importance of stakeholder feedback and has taken steps to share the Future State strategy publicly and obtain valuable feedback in return. At the same time, the Taxpayer Advocate has articulated her concerns about the IRS' approach to studying taxpayer needs and preferences.[112]

The IRS' decision to form a Taxpayer Experience Coordinating Council, including the Taxpayer Advocate, is a step in the right direction to consolidate insights about taxpayer needs and preferences. The IRS' digital offerings can also be improved during development and implementation phases through targeted research and feedback from the discrete segments of taxpayers, tax professionals, and others that such tools intend to serve. Any single research method is inherently limited.[113]

---

[110] See https://www.irs.gov/identity-theft-fraud-scams/identity-protection-pin-pilot-program

[111] National Taxpayer Advocate, Annual Report to Congress 2017, Volume 1, Most Serious Problem #19, pp. 217-218.

[112] See Taxpayer Advocate, Fiscal Year 2018 Objectives Report to Congress, Volume 2, pps. 7-8.

[113] See generally National Taxpayer Advocate, Annual Report to Congress 2016, Volume 1, Most Serious Problem #7.

Taxpayer Field Testing

No matter how comprehensive, traditional research methods (surveys, focus groups, user experience labs, etc.) in support of product development only go so far. After a reasonable amount of traditional research, the IRS must engage collaboratively with taxpayers and other users by making actual solutions available for use. This type of taxpayer field testing has the benefit of seeing whether and how taxpayers actually use a product, which can be very different from how they say they will use the product.

For that reason, ETAAC supports the IRS' approach of launching "minimum viable" applications with limited initial functionality to capture taxpayer and user learnings in the field and make adjustments before more significant investments.

Leveraging Connected Services

ETAAC has previously commented on the IRS' opportunity to use collaborative partnerships to extend the reach and impact of IRS-provided taxpayer digital services.[114] Because it is difficult for consumers to change or adopt new behaviors,[115] services connected to a consumer's existing workflow (i.e., their preferred and/or established a way of doing things) stand a greater chance of higher adoption and usage. Some taxpayers will want to work directly with the IRS, while others will prefer to work through their existing tax service providers -- tax professionals or software tools.

The IRS' collaborative efforts should include engaging with stakeholders who can help develop connected services where beneficial to taxpayers.

Transparency

Transparency underlies any successful collaboration by providing stakeholders with a clear understanding of the IRS' goals, insights and decision-making. Transparency also builds shared vision and confidence in both the IRS' strategy and approach. The IRS should publicly report its desired outcomes and research methodologies used to develop digital tools. Transparency includes providing a description of target users, product usage assumptions, and summary-level stakeholder feedback and service goals for customer service.[116]

Online Submission and Acceptance of Power of Attorney (POA)

Professional tax practitioners can become active and safe users of online services if the IRS invests early in providing a digital mechanism for POA and disclosure

---

[114] See ETAAC 2010 Report to Congress, pps. 21-22.

[115] "No matter how motivated consumers may be to try your product or service, or how unhappy they may be with their current situation, if you do not focus on a comprehensive plan for changing their behavior, then you are unlikely to have a significant influence on them." See https://hbr.org/2014/02/dont-persuade-customers-just-change-their-behavior

[116] "Without defining a comprehensive strategy with specific goals for customer service tied to the best in business and customer expectations, Treasury and IRS are not effectively conveying to Congress the types and levels of customer service expected by taxpayers and the capabilities and resources IRS requires to achieve those levels." See GAO Report 2015 TAX FILING SEASON: Deteriorating Taxpayer Service Underscores Need for a Comprehensive Strategy and Process Efficiencies, GAO-16-151, December 2015, pp.26-27.

authorization.[117] This solution would enable real-time input of Form 2848, Power of Attorney, and Form 8821, Tax Information Authorization, and thereby eliminate the delays (about 10 days) resulting from the IRS' current mail or fax processing model. A secure POA electronic submission system would also allow tax professionals to interact more effectively with the IRS on a daily basis as well as during efforts to resolve identity theft or other cybersecurity issues a taxpayer may face. This system could be provided as a standalone solution or, better yet, integrated with a taxpayer or tax professional online account. An integrated electronic solution would enable taxpayers and their authorized tax professionals to have a more seamless experience in executing and submitting POAs, accessing taxpayer account information and resolving issues**.**

ETAAC concurs with the National Taxpayer Advocate that practitioner account access should be restricted to individuals covered by Circular 230[118] or participating in an IRS sponsored programs such as VITA, LITC or TCE. These requirements are only one element of any minimum standard -- the IRS should also consider additional requirements related to data security and compliance.

TIGTA examined an earlier IRS e-services POA system and concluded that it possessed insufficient controls, which put taxpayer information at risk.[119] One concern was the inability to verify that the practitioner had obtained the taxpayer's signature on a Form 2848. Another was that submissions were accepted from any user of e-services, not just those allowed to represent taxpayers under Circular 230. TIGTA reported that over 899,000 Form 2848s had been submitted since 2004. The IRS discontinued the online submissions of Form 2848 in June 2013.

There is support for such a solution. Most recently, the IRS Advisory Council (IRSAC) supported an electronic POA solution.[120] Additionally, the National Taxpayer Advocate has supported enhanced practitioner online services with certain safeguards.[121]

The security of taxpayer information is a prime consideration, but the current manual processing model is susceptible to fraud as well. There should be ways to identify proof and authenticate tax professionals and taxpayers so that remote taxpayer consent/authorization can be gained with sufficient confidence. For example, the IRS could verify e-signatures through systems accessible by a taxpayer only after secure identity proofing. The IRS could also increase its confidence by controlling the types of

---

[117] See "Ensuring a Modern-Functioning IRS for the 21st Century" submitted on April 3, 2017, to House Committee on Ways and Means and Senate Committee on Finance. www.aicpa.org/advocacy/tax/downloadabledocuments/irs-service-improvement-practitioner-report.pdf

[118] National Taxpayer Advocate, Annual Report to Congress 2016, p. 58 (https://taxpayeradvocate.irs.gov/reports/2016-annual-report-to-congress). Circular 230 participants include Attorneys, Certified Public Accounts, Enrolled Agents, Enrolled Retirement Agents, and Annual Filing Season Program Participants.

[119] Treasury Inspector General for Tax Administration, Insufficient E-Services Controls May Put Taxpayer Information at Risk, June 29, 2012 (https://www.treasury.gov/tigta/auditreports/2012reports/201240071fr.pdf).

[120] IRSAC 2017 Public Report dated November 15, 2017, pp. 58-59 (https://www.irs.gov/pub/irs-utl/2017-irsac-public-report.pdf).

[121] For example, see National Taxpayer Advocate, Annual Report to Congress 2016, Volume 1, p. 135. (https://taxpayeradvocate.irs.gov/Media/Default/Documents/2016-ARC/ARC16_Volume1.pdf).

professionals that can access taxpayer information. We support the IRS' efforts to identify and mitigate these risks through carefully designed pilots.

Account Lock/Unlock appears to have promise

In its 2017 Report, ETAAC supported the IRS' continued consideration of a taxpayer-controlled protection described as "Account Lock/Unlock."[122] ETAAC understands the concept to enable an authenticated taxpayer to lock and unlock his/her tax account to control the filing of any tax returns in his/her name. Essentially, a taxpayer could lock any online or mobile account for a variety of reasons including suspicion of identity theft, previous unauthorized access to their account, or other circumstances that make them feel insecure with the protection of their identity such as a recent divorce.[123]

The feature would be analogous to credit reporting agency sites that enable consumers to freeze their credit records.[124] In the tax situation, the lock might reject any tax return attempting to post to the taxpayers account and prevent posting of any other external transaction until the source could be properly verified through IRS protocols. At tax filing time the account could be unlocked for a brief period to allow filing and then re-locked. The lock would be available for both individual taxpayers and business tax filers. Properly implemented, account locking could contribute to a decrease in IDTTRF and an increase in taxpayer confidence.

Of course, Account Lock/Unlock is not without its challenges, including the potential to drive increased call volumes to the IRS. IRSAC identified several important considerations in its most recent report but, nevertheless, still supported the IRS' further consideration of the feature.[125] ETAAC agrees with IRSAC and supports the IRS' continued consideration of an Account Lock/Unlock feature.

RECOMMENDATION #19: *Increase the electronic filing of employment returns*

> Recommendation #19***:*** *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 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.*

Support for Recommendation:

Any initiative to increase Form 94X electronic filing will face stiff competition for funding and staff resources given the IRS' numerous priorities. Therefore, any effort must be

---

[122] See ETAAC 2017 Report to Congress, pp. 18-19.

[123] Internal Revenue Service Advisory Council, Small Business/Self Employed and Wage & Investment Subgroup, 2016 IRSAC Report, November 16, 2016, pp. 40-41. (https://www.irs.gov/pub/irs-utl/2016irsacfinalreport.pdf).

[124] See Experian's "Security Freeze Center" (https://www.experian.com/freeze/center.html).

[125] See IRSAC 2017 Public Report dated November 15, 2017, pp. 72-76. (https://www.irs.gov/pub/irs-utl/2017-irsac-public-report.pdf).

narrowly targeted to achieve meaningful outcomes at a cost reflecting the corresponding IRS and taxpayer benefit.

ETAAC's 2011 Report outlined some key focus areas[126] for the IRS to increase Form 94X e-file rates:

- Overcoming numerous misunderstandings in the Forms 94X filer community about the availability and risks associated with electronic filing.
- Simplifying a cumbersome, time-consuming enrollment and registration processes.
- Understanding the needs of the highly fragmented Forms 94X filer segments.
- Engaging with key stakeholders to find the most appropriate, cost effective approaches to increase Forms 94X electronic filing.

These points remain relevant and ETAAC believes that the following focused, collaborative approach can yield positive results.

The IRS should attack this initiative with a public/private partnership in two phases

As a first step, the IRS should leverage its current public/private partnerships to establish a collaboration with stakeholders representing all segments of the filer community (Reporting Agents, tax professionals and employers/payroll professionals[127]) and the tax and accounting software/transmitter community. State engagement should be considered given some appear to have successful employment return e-file programs.[128]

Currently, there still appears to be numerous misunderstandings in the filer communities about e-file risks and benefits, software capabilities, registration processes, etc.

Phase One of the collaboration should focus on improving the IRS' content and communications by (i) developing more understandable, targeted content and messaging to overcome misunderstandings about Form 94X electronic filing, and (ii) implementing a proactive strategic outreach effort using both IRS and third party communications channels.

By way of illustration, the IRS seems currently focused on using www.irs.gov to communicate on this issue. The top organic search result for the simple question of "How can I e-file my employment tax returns" refers one to an IRS web page about e-filing Form 94X returns.[129] Many (if not most) payroll professionals who file for their

[126] ETAAC 2011 Report to Congress, p. 32.

[127] IRS discussions suggest that the total Form 94X filings (paper and e-file) are roughly distributed across the segments: (i) 30% from Reporting Agents, (ii) 30% from professionals, and (iii) 40% from small businesses/employers. IRS should know which of these three segments has the lowest e-file rate.

[128] ETAAC understands that several states (including Michigan, Illinois, Iowa and Montana) have online options for filing certain employment tax returns, and may be able to provide insights regarding technical and policy approaches at the federal level.

[129] See https://www.irs.gov/businesses/small-businesses-self-employed/e-file-form-940-941-or-944-for-small-businesses

employers would find this content highly technical and confusing: What alternative under "Option 2" is right for me? What does it involve? What is an ERO? The IRS needs clearer, simpler content developed with feedback from the Form 94X filer community.[130]

The IRS should also supplement its current reliance on www.irs.gov with a carefully planned outreach effort that leverages third party channels able to reach the target audience.

Phase Two of the collaboration should focus on streamlining the IRS' policies and procedures that create unnecessary barriers to increase e-filing of Form 94X by: (i) focusing on the Form 94X filer segments with the lowest e-file rates, and (ii) identifying the immediate policy barriers to e-filing for that filer segment, including the IRS' current e-signature requirements.

To be successful, all stakeholders need to think out of the box and actively question why any particular process or policy that causes such low e-file rates should be acceptable. There has to be a better way.

ETAAC recommends against a Form 94X e-file mandate at this time

Finally, ETAAC recommends against any policy solution that involves a mandate to compel the electronic filing of Form 94X returns unless and until the IRS significantly simplifies its Form 94X filer registration and enrollment processes. Forcing employers, and particularly small businesses, to go through the current cumbersome experience is not advisable.

[130] As it develops the content, IRS should also identify and consider any obvious improvements to its current registration processes.

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' 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 the IRS, the tax industry and state tax administrators as a major initiative to combat Identity Theft Tax Refund Fraud (IDTTRF), which was named the IRS Security Summit. Subsequently, 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 report and in future reports, ETAAC will continue to reflect this expansion of focus to provide strategic and tactical recommendations on combating IDTTRF.

ETAAC has 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, solo tax practitioners, tax software companies, financial services industry and low-income and consumer advocacy groups. 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.

Finally, on occasion, ETAAC may seek background insights from policy leaders, industry, and state departments of revenue. Using all of this information, ETAAC

formulates its annual report. 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 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 etaac@irs.gov.

Appendix B

ETAAC Member Biographies

John Ams - Mr. Ams is the Executive Vice President and Chief Operating Officer of the National Society of Accountants in Alexandria, VA. He 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. At NSA, a professional society whose members practice in the areas of accounting and taxation, he is 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 the 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.

Robert Barr - Mr. Barr serves as Senior Vice President and Chief Digital Officer with First Command Financial Services in Ft. Worth, Texas where he is responsible for leading the organization's digital transformation journey focused on devising and executing digital strategies that grow brand loyalty and advocacy through omni-channel service and support. Bob joined First Command after a thirty-eight year career in progressively responsible technology sales, marketing, consulting and general management roles for a number of highly successful U.S. based B2B and B2C digital businesses for organizations in consumer goods, natural resources, media and entertainment, manufacturing, financial services and both federal (IRS) and state (SC Department of Revenue) government. Academically, Bob earned his B.S. from the University of South Carolina, Magna Cum Laude, Phi Beta Kappa, his M.B.A. from The Wharton School at the University of Pennsylvania and completed the Advanced Management Program at Harvard Business School

Shannon Bond - Ms. Bonds 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. John 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 - Luanne Brown has served as the Director of Payroll Services for Grand Valley State University for the last 11 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 Vice President on the American Payroll Association Board of Directors. At the local level, Brown has been a member of the APA's West Michigan Chapter since 1999 and is currently serving her second term as the chapter's president. 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 20 years of experience in the tax industry. Camp has 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. Camp joined Intuit five years ago to pursue an opportunity in which her focus is to drive tax administration and policy from the point of view of a software provider. Over the past year and a half, Camp has been the key point of contact for Intuit within the IRS Security Summit and working both internally and externally on implementation of the Summit work group initiatives. Camp is also a board member for the NACTP.

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 - Jenine 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 - Michael 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 - Courtney Kay-Decker was appointed Director of the Iowa Department of Revenue by Governor Terry Branstad in January 2011 and continues to serve in that role under Governor Kim Reynolds. At the Department, Decker has focused on improving administrative rules, guidance and processes to simplify and reduce compliance burdens for Iowa taxpayers. Decker currently serves on the board of directors of the Federation of Tax Administrators 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 - Suzanne 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 - Ms. Pickering is the executive director of The Tax Institute (TTI) and vice president of regulatory affairs for H&R Block. With almost 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, Kathy 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 corporate structure, 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, Kathy leads the relationship-management strategy with the IRS and state taxing agencies. Kathy 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 Poirier – Mr. Poirier is a Senior Fellow with the Center for Social Development at Washington University in St. Louis, and a periodic Consultant with Prosperity Now (formerly CFED). His work 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. He is also a volunteer tax preparer in the IRS Volunteer Income Tax Assistance (VITA) program. He previously served as a Vice President at Intuit Inc., where his responsibilities included legal, compliance and business development roles. Mr. Poirier also served in the U.S. Navy and Naval Reserve for nearly three decades, retiring as a captain, and was former chair of the IRS Electronic Tax Administration Advisory Committee (ETAAC), a congressionally mandated IRS advisory board. 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.

John Sapp - Mr. Sapp has served a key role at Drake Software since 1995, with roles ranging from Chief Financial Officer to Vice President of Drake's Sales, Marketing, and Education 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, and he has been a Certified Public Accountant since 1987.

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 the 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.

Atilla Taluy - Mr. Taluy founded FileYourTaxes.com in 1995 as the original cloud based tax software provider to individuals and subsequently, to the tax professionals. In addition to his duties with FileYourTaxes.com, Mr. Taluy contributed as an architect of policy and technology for the electronic tax industry. He was an active participant in the current Security Summit process and an active member of CERCA, FS-ISAC, NACTP, OASIS, and other industry and government committees. He also served as a director of CERCA, and a charter member of the Executive Committee of the Free File Alliance, Inc. Mr. Taluy simultaneously obtained Bachelor of Science degrees in Mechanical and Electrical Engineering and performed his Masters work at Oklahoma State University.

Doreen Warren - Ms. Warren is the Idaho State Tax Commission's Public Information Director, in charge of the newly formed Taxpayer Resources Unit. She began her career at the Tax Commission in 1990, and joined Revenue Operations in 1996 as the motor fuels subject matter expert and project coordinator for many division projects including the implementation of the state's Modernized e-Filing program in conjunction with the IRS. Doreen was hired as the Revenue Operations administrator in 2008. She started her position as the Public Information Director in July, 2016. In addition to her duties for the Tax Commission, she currently represents state interests on a number of IRS Security Summit fraud work groups. Doreen's education includes an associate degree in computer science, 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 of all major tax returns.

In its projection for the current year, IRS Publication 6186 must necessarily rely on historical information as the foundation for its estimates and projections. For example, the projections for 2018 in Publication 6186 are based on information available as of August 2017.

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 88% for the entire 2018 filing season.

Below is an explanation of ETAAC's three-step process to project the full-year electronic filing rate for individual returns for 2018.

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 20, 2018, which ETAAC calculates to be 90.94%.

Table 3: Tax Year 2017 Individual Income Tax Returns Actual through April 20, 2018

Cumulative statistics comparing 04/21/2017 and 04/20/2018			
	04/21/2017	**04/20/2018**	**YOY % Change**
Total Receipts	135,638,000	136,919,000	.9%
E-file Receipts	122,164,000	124,515,000	1.9%
E-file Rate	90.07%	**90.94%**	.87%

Source: From "Filing Season Statistics for Week Ending April 20, 2018" published by IRS at https://www.irs.gov/uac/newsroom/filing-season-statistics-for-week-ending-april-20-2018

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 / early May (primary filing season) with the actual e-file rate for the full-calendar-year filing season for each of the two preceding years -- 2016 and 2017. Then, ETAAC uses the average degradation rate experienced over the previous two years to forecast degradation for the current year. Using this approach, the e-file degradation rate for the 2018 filing year is forecast to be 3.3%. (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

	04/22/2016	**12/30/2016**	**Change**	**04/21/2017**	**12/29/2017**	**Change**	**Two Yr Avg.**
Total Receipts	136,528,000	152,544,000		135,638,000	152,235,000		
E-file Receipts	122,546,000	131,851,000		122,164,000	132,319,000		
E-file Rate	89.8%	86.4%	-3.4%	90.1%	86.9%	-3.2%	**-3.3%**

Source: From various links on "2018 and Prior Year Filing Season Statistics." See https://www.irs.gov/newsroom/2018-and-prior-year-filing-season-statistics

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 20, 2018 data, ETAAC's projected 2018 full-year e-file rate for the individual tax return family is 87.64%. This ETAAC projection is consistent with IRS' 2018 projection of 88.8% in IRS Publication 6186.

Table 5: 2018 Individual Returns Electronic Filing Projection

	Current @ 4/20/18	**Avg. Degradation Rate**	**ETAAC 2018 Projection**
Total Receipts	136,919,000		
E-file Receipts	124,515,000		
E-file Rate	**90.94%**	**-3.30%**	**87.64%**

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

This page left intentionally blank