IRS

TAXES + SECURITY TOGETHER

Electronic Tax Administration Advisory Committee

ANNUAL REPORT TO CONGRESS

June 2017

Publication 3415 (Rev. 6-2017) 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
Angela Camp
John Craig
Jacob Dubreuil
Thomas Lorek
Julie Magee
Kathy Pickering
Phillip Poirier, Jr.
John Sapp (Chair)
Deborah Sawyer
Joseph Sica
Mark Steber
Atilla Taluy
Doreen Warren (Vice Chair)

PREFACE

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 (IRS) 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:

- 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 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. This report provides background on the success of this collaborative partnership as well as recommendations for potential improvement.

As further background, 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 reflect this expansion of focus to provide strategic and tactical recommendations on combating IDTTRF.

Over the past 12 months, ETAAC has also expanded its membership from six to seventeen to broaden the experience of its members and add new stakeholder perspectives from the government, commercial and non-profit 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 A 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 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 tax fraud 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.

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY

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

Congress established ETAAC in 1998 principally to report on IRS' progress in advancing electronic filing (e-file) and its electronic tax administration strategy.[1] As a result, past ETAAC reports have focused on IRS' achievement of its 80% e-file goal and more recently included recommendations on IRS' electronic tax administration initiatives, such as online and mobile services. IRS continues to make progress in advancing e-file, which is addressed in more detail in the "Progress Toward 80% E-file Goal" section of this Report.

This year ETAAC is shifting the primary focus of its report to two areas that are foundational to the success and integrity of our nation's electronic tax system – the implementation of strong cybersecurity protections and the elimination of identity theft tax refund fraud (IDTTRF).

Cybersecurity and Identity Theft Tax Refund Fraud are a Continuing Threat

Americans are well aware of the cyberattack threat to our nation and their personal lives. We hear about these attacks almost daily, and many of us have had our personal information compromised or know someone who has. The most significant compromises have occurred in a variety of settings but principally outside of our tax system.[2]

Criminals use stolen personal information (such as names, social security numbers, birth dates, user names and passwords), coupled with other information readily available online and through social media, as the fuel for IDTTRF. Essentially, these criminals know so much about a given taxpayer that key elements of their fraudulent electronically filed returns are largely indistinguishable from those of the legitimate taxpayer.

IDTTRF is a tough problem for IRS and States to solve. Criminals are incented by the potential availability of billions of dollars in refunds, particularly driven by refundable tax credits intended to help low and moderate income Americans. The criminals are smart, nimble, motivated and well-funded.

America's voluntary compliance tax system and electronic tax filing systems exist, and succeed, because of the trust and confidence of the American taxpayers (and policy makers). Any corrosion of trust in filing tax returns electronically would result in reverting back to the less-efficient and very costly "paper model." That option is neither feasible any longer nor desirable. As failure is not an option, ETAAC strongly believes IRS must

[1] The Internal Revenue Service Restructuring and Reform Act of 1998. Pub. L. No. 105-206, 112 Stat. 685

[2] Examples of data breaches include the Office of Personnel Management (government), Anthem (healthcare) and LinkedIn (social media).

remain ever vigilant in combating IDTTRF and use the public-private collaborative model of trusted stakeholders whenever possible to gain advantage over fraudsters.

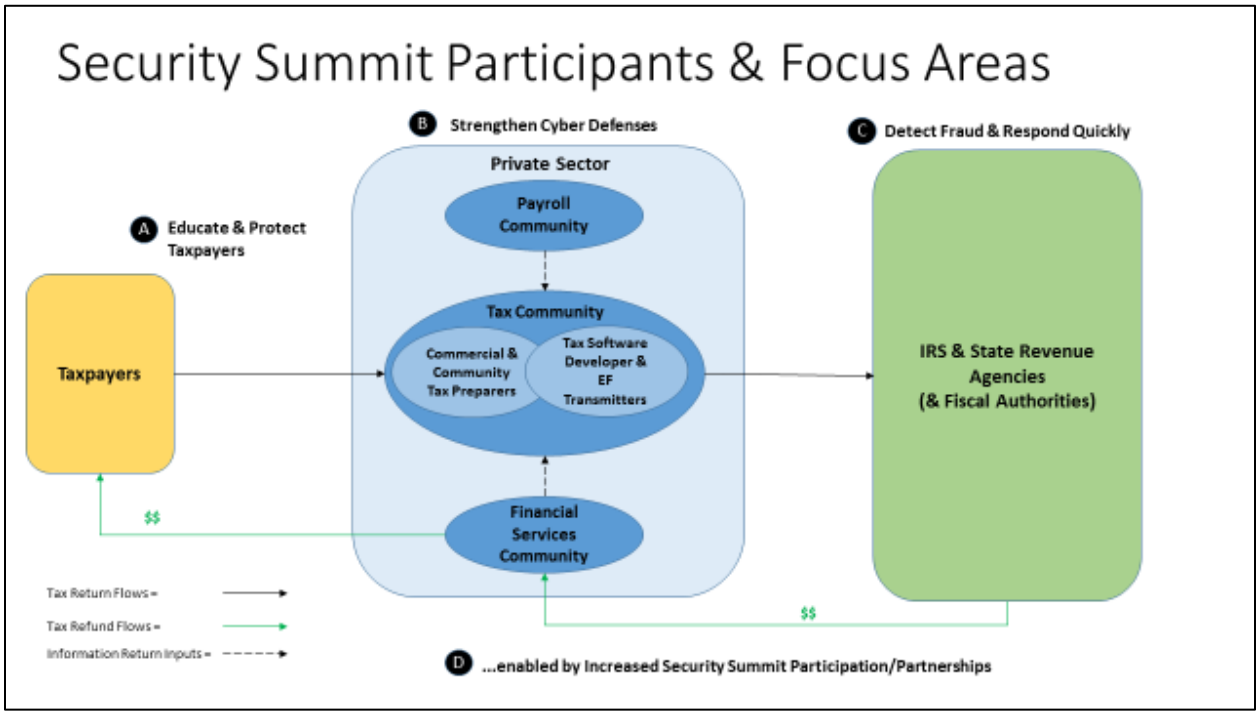
The IRS Security Summit is making significant progress

IRS leadership had the foresight to embrace an innovative approach a few years ago as IDTTRF accelerated. Leveraging the entire tax ecosystem, IRS brought together all the key stakeholder groups in 2015 to form the IRS Security Summit -- an initiative that focused on improving our cybersecurity posture, preventing IDTTRF and leveraging a public/private collaboration between IRS, State Departments of Revenue and Industry.[3] ETAAC believes the Security Summit is having a positive impact on these goals and should continue to be an IRS signature initiative.

Importantly, Congress approved $290 million in additional funding for the IRS for Fiscal Year (FY) 2016, to improve service to taxpayers, strengthen cybersecurity and expand their ability to address identity theft. The additional funding was vital in allowing the IRS to stay focused on efforts to combat IDTTRF within the IRS Security Summit and address additional needed resourcing. ETAAC believes Congress invested wisely with the additional appropriation and, given the Security Summit's progress made to date, supports continued congressional attention in this area.

The IRS Security Summit will get even better with Congressional Support

The Security Summit must keep pace with ever-evolving fraudulent activity aimed at misappropriating taxpayer refunds. ETAAC's recommendations are intended to contribute to the Summit's evolution. Of course, Congress' continued support will play a critical role in that success.



[3] More information about the nature, formation and achievements of IRS, States and Industry through the Security Summit is found in the "About the IRS Security Summit" section of this Report.

As illustrated above, ETAAC's principal recommendations generally fall into four broad categories:

A: Educate and Protect Taxpayers

- Improve authentication practices, including using innovative pilots
- Replace outmoded prior year AGI/PIN e-file signature verification[4]
- Increase taxpayer awareness by expanding employer outreach, leveraging social media, and extending targeted communications to diverse communities
- Engage tax professionals by updating IRS publications, increasing awareness/education, communicating standards and providing easy-to-use compliance tools

B: Strengthen Cyber Defenses

- Continue establishment of a common cybersecurity standard
- Expand federal, state and industry participation in cybersecurity area
- Create mechanisms to anticipate future IDTTRF and cybersecurity trends and threats, and to develop proactive responses

C: Detect Fraud and Respond Quickly

- Document and improve "industry leads" information sharing processes
- Implement the IDTTRF Information Sharing & Analysis Center (ISAC) by increasing participation, removing barriers to sharing and providing adequate funding

D: Increase Security Summit Participation and Partnerships

- Increase State and Tax Industry participation across the Security Summit
- Increase Financial Institution[5] (FI) participation in Security Summit and IRS "leads" programs
- Expand Payroll Community participation in the Security Summit

ETAAC's detailed recommendations and supporting assessments are found in the "Detailed ETAAC 2017 Recommendations" section of this Report.

[4] This refers to "Adjusted Gross Income" (AGI) and "Self-Select Personal Identification Number" (PIN).

[5] As used in this Report, "Financial Institutions" or "FI's" include the broad range of companies that provide financial products and services, e.g., banks, credit unions, prepaid card issuers, refund settlement product providers, etc.

Closing Thoughts

Security practices can have a significant impact on the tax experience and taxpayer behavior. Improving the taxpayer experience will require sustained creativity and focus for the IRS to build systems that are both secure and, conversely, easy to access and use from a taxpayer perspective. A system that is secure but that few can use will not be successful for IRS as it expands some of its key online services. IRS must strive to achieve a situation where services are both secure and easy to use and access.

IRS has done a remarkable job of managing a diverse group of tax system stakeholders including IRS, State Departments of Revenue and a broad range of different private sector stakeholders including tax preparation (both commercial and non-profit), financial services and payroll service providers. There is no doubt that coordinating the efforts of all these stakeholders presents communications and coordination challenges. However, the diversity of the tax ecosystem also offers some important strengths – it mitigates single points of failure, and the sheer number of stakeholders ensures multiple viewpoints and experiences that contribute to lessons learned and innovation. IRS' continued success will be dependent, in part, on its ability to manage and lead a diverse group of stakeholders.

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 Index (EFI) as a benchmarking tool for e-filing performance. The index utilizes groups of major returns as outlined in Appendix B, coupled with a specific calculation methodology.

During the 2017 filing season, the EFI methodology projects that for the first time the IRS will achieve the 80% e-filing goal for major return types. If sustained, this is a momentous achievement for the IRS, and ultimately for the American taxpayer.

Table 1: 2014- 2017 Electronic Filing Index

Electronic Filing Rate	2014	2015	2016 (Estimated)	2017 (Projected)
EFI	75.8%	77.8%	78.8%	80.1%

Source: Prior year EFI based on actual numbers as follows: 2014 - IRS Publication 6186 2015 Update – (revised 10-2015), 2015 - IRS Publication 6186 2016 Update (revised 12-2016) and 2016 from 2016 estimated numbers in IRS Publication 6186 2016 Update (revised 12-2016); See Appendix B for 2017 projection.

However, this projection should be tempered by the fact that overall total individual returns has decreased by 0.5% compared to May 2016. In addition, the volume projections used in the above calculation were produced prior to the 2017 filing season, which has had several unusual factors which may have impacted return volume. Although the overall individual e-file percentage has remained consistent with the prior year, additional analysis will need to be performed to determine the cause of fewer returns being filed this season and the potential impact on e-file and the continued use of the EFI methodology in future years.

Individual returns have the highest e-file rate year-over-year and represent over 77% of major returns filed. While the growth rate of individual e-file is slow, it is consistently gaining and it is safe to say e-file is now the "norm".

E-file percentages continue to increase for all major return types. Employment tax returns continue to be the next obvious target for IRS efforts to increase e-file, currently with the lowest e-file rate of all major return types.

Table 2: 2017 Projected Electronic Filing Index (EFI)

	2016 Estimated			2017 Projection			
	Total	**E-filed**	**EFI**	**Total**	**E-filed**	**EFI**	**Total Absolute Increase Rate**
Individual (Forms 1040, 1040-A, and 1040-EZ)	149,943,000	130,909,400	87.3%	151,934,300	134,262,400	88.4%	1.06%
Employment (Forms 94x)	29,839,000	10,914,300	36.6%	29,900,100	11,411,100	38.2%	1.59%
Corp Income Tax (1120,1120-A,1120-S), et al	6,869,800	5,239,200	76.3%	6,909,000	5,409,600	78.3%	2.03%
Partnership (Forms 1065/1065-B)	3,975,900	3,299,300	83.0%	4,065,500	3,459,800	85.1%	2.12%
Fiduciary (Form 1041)	3,209,400	2,573,400	80.2%	3,249,700	2,667,500	82.1%	1.90%
Exempt Organizations (Forms 990, 990-EZ)	571,800	354,400	62.0%	579,300	376,400	65.0%	3.00%
	194,408,900	153,290,000	**78.8%**	196,637,900	157,586,800	**80.1%**	1.29%

Source: Per IRS Publication 6186 2016 Update (revised 12-2016)

An overall assessment of e-file would not be complete without considering the significant contribution the public/private partnership the IRS has developed with state tax administrators and private industry partners, which has culminated in the success of e-file. These same relationships which have evolved parallel with e-file laid the foundation for the collaboration of the Security Summit which continues to protect both taxpayers and e-file initiatives.

ABOUT THE IRS SECURITY SUMMIT

Formation & Structure

By 2015, the levels of identity theft tax refund fraud (IDTTRF) had reached alarming levels. To address these challenges, IRS Commissioner Koskinen convened an unprecedented Security Summit meeting in Washington, D.C., on March 19, 2015 through the auspices of ETAAC. The 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. As a result, the focus of the meeting was to discuss common challenges and ways to leverage the tax ecosystem's collective resources and efforts to fight IDTTRF.

The following three work groups were formed at the first Summit meeting, and tasked to deliver detailed recommendations by June 2015 for implementation in time for the 2016 filing season:[6]

- Authentication Work Group: Tasked with identifying opportunities for strengthening authentication practices, including identifying 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 that would 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, participants recognized the need to create additional teams to enhance and expand their collaborative efforts, which resulted in the formation of one new subgroup and three additional work groups:

- Information Sharing and Analysis Center (ISAC) Sub-Group: As a sub-group of the Information Sharing Work Group, tasked with centralizing, standardizing, and enhancing data compilation and analysis to facilitate sharing actionable data and information.
- Financial Services Work Group: Tasked with examining and exploring additional ways to prevent and deter criminals from potentially accessing tax-time financial products, deposit accounts, and pre-paid debit cards.

[6] 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

- 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 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.

Each Security Summit work group has a co-lead from each of IRS, the states and industry.

Filing Season 2016 Results

Despite a short development window, Security Summit participants undertook an unprecedented number of actions in preparation for the 2016 filing season.[7] These actions had a substantial impact on curbing IDTTRF during 2016 as evidenced by the following:

- From January through April 2016, the IRS stopped $1.1 billion in fraudulent refunds claimed by identity thieves on 171,000 tax returns; compared to $754 million in fraudulent refunds claimed on 141,000 returns for the same period in 2015. Better data from returns and information about schemes meant better filters to identify identity theft tax returns.
- Thanks to leads reported from industry partners, the IRS suspended 36,000 suspicious returns for further review from January through May 8, 2016, and $148 million in claimed refunds; twice the amount of the same period in 2015 of 15,000 returns claiming $98 million. Industry's proactive efforts helped protect taxpayers and revenue.
- The number of anticipated taxpayer victims fell between/during 2015 to 2016. Since January, the IRS Identity Theft Victim Assistance function experienced a marked drop of 48 percent in receipts, which includes Identity Theft Affidavits (Form 14039) filed by victims and other identity theft related correspondence.
- The number of refunds that banks and financial institutions return to the IRS because they appear suspicious dropped by 66 percent. This is another indication that improved data led to better filters which reduced the number of bad refunds being issued.
- Security Summit partners issued warnings to the public, especially payroll industry, human resources, and tax preparers, of emerging scams in which criminals either posed as company executives to steal employee Form W-2 information or criminals using technology to gain remote control of preparers' office computers.

[7] See https://www.irs.gov/pub/newsroom/6_2016_security_summit_report.pdf

Filing Season 2017 Focus

For the 2017 filing season, the Security Summit's emphasis remained on authentication, information sharing and cybersecurity, and included the following initiatives:

- IRS partnered with the payroll industry to expand a pilot program to add a W-2 Verification Code to approximately 50 million forms in 2017, which helps validate the authenticity or validity of the submitted W-2.
- Industry provided additional data elements to IRS and States from returns to improve the authentication of the taxpayer and identify possible identity theft scams.
- The new Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC) launched in 2017, which will enable significant gains in detecting and preventing identity theft tax refund fraud and provide a real-time information sharing platform.
- The Security Summit's "Taxes. Security. Together." campaign launched with a focus on providing education and outreach to tax return preparers to ensure they have the information they need to protect themselves from cyberattacks and to protect taxpayer data.
- Twenty-three states worked with the financial industry and the IRS to establish an Automated Clearing House (ACH) Common Naming Convention so that state refunds could be identified. Nine States also implemented a program similar to the IRS program which allows questionable refunds to be identified and returned for additional review.

The impact of Security Summit actions in 2017 will be assessed in the coming months. Nevertheless, IDTTRF will continue to be major threat to tax administration given the large number of returns identified as false returns by fraud filters in IRS' processing systems.[8]

ETAAC Integration with the Security Summit

The Security Summit's efforts were institutionalized through the auspices of the ETAAC in 2016 when an amendment to ETAAC's charter expanded its scope to include identity theft. On an ongoing basis, ETAAC engages with the Security Summit through the attendance and participation of its members in work group activities. Additionally, ETAAC members proactively engage with Security Summit work group co-leads to keep abreast of Security Summit initiatives and IDTTRF developments.

[8] Testimony of Kirsten B. Wielobob, IRS Deputy Commissioner For Services & Enforcement before the House Ways and Means Committee, Subcommittee On Oversight on April 26, 2017. See https://waysandmeans.house.gov/wp-content/uploads/2017/04/2017.04.26-OS-Testimony-Wielobob.pdf

Looking Ahead – Sustaining the Momentum

At the time of its initial creation, the Security Summit was facing a clear challenge from IDTTRF. Fortunately, there were some equally clear opportunities in key areas (e.g., authentication, information sharing, and cybersecurity standards) that IRS, States and Industry pursued quickly. Now, after two years, we need to sustain the momentum of the Security Summit by taking the opportunity to step back and assess where the Security Summit is and where it needs to go.

ETAAC believes there are three strategic areas affecting the Security Summit that warrant further discussion – developing a simple clear strategy and agreed upon priorities, reviewing the structure of the Security Summit Work Groups to find any appropriate adjustments, and formalizing the Security Summit's operating mechanisms – particularly those that address forward looking strategic decisions (said another way, those that are "important, but not urgent"). ETAAC looks forward to discussing these points with IRS.

LIST OF ETAAC 2017 RECOMMENDATIONS

The following is a complete listing of ETAAC's 2017 recommendations, which are organized under specific themes to help readers understand their area of focus:[9]

ENHANCE AUTHENTICATION AND THE TAXPAYER EXPERIENCE

1. The IRS should analyze the ongoing effectiveness of the Security Summit's initiatives to identity proof and authenticate taxpayers and tax return filings, including a cost/benefit assessment of their impact on Identity Theft Tax Refund Fraud (IDTTRF) reduction and the taxpayer experience.
2. In light of past Security Summit successes, IRS should continue to invest in innovative and collaborative initiatives with Security Summit stakeholders and trusted third parties to identify and test enhanced identity proofing and authentication approaches, including accessing new sources of authentication data and testing new identity proofing technologies.
3. Given its associated exceptionally high e-file rejects, 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 IRS and States.

STRENGTHEN INFORMATION SHARING AND ANALYTICS CAPABILITIES

4. Working with Security Summit partners, IRS should document the Security Summit's current information sharing process (including Leads, Leads Feedback, Alerts and Rapid Response processes, and all active participants and information flow paths) to facilitate the identification and implementation of process improvements.
5. The IRS should encourage and enable greater participation in the IDTTRF Information Sharing and Analytics Center (ISAC) by the many stakeholders affecting the tax ecosystem.
6. The IRS should identify, analyze and mitigate barriers that preclude IRS information sharing with ISAC for the purposes of fighting IDTTRF.
7. Congress and IRS should adequately fund ISAC operations.

ENHANCE SECURITY & ENABLE SECURITY SUMMIT PROACTIVITY

8. The STAR Work Group should continue its current direction and collaborative approach to implement the National Institute of Standards and Technology (NIST) Cybersecurity Framework.
9. The STAR Work Group should identify and pursue opportunities to extend federal, state and industry participation in its initiatives and, where appropriate, expand its engagement with other Security Summit Work Groups.

[9] ETAAC's recommendations are not individually listed in order of relative importance, although the order of the specific themes generally reflects, in our view, their relative impact on stopping IDTTRF and improving security. The same "Recommendation #'s" carry over to the following section.

10. To mitigate the risk of stolen identities, IRS should evaluate, and change where appropriate, current regulations so as to increase the permitted use of Truncated Taxpayer Identification Numbers[10] on IRS documents.

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.[11]

EXPAND FINANCIAL INSTITUTION ENGAGEMENT

12. Based on fraudulent refund patterns, IRS should target those Financial Institutions (FIs) most vulnerable to IDTTRF deposits to engage their participation in the Security Summit and External Leads/Rejects programs,[12] while strengthening IRS' corresponding ability to handle increased suspect case volume.

13. The IRS should identify and work toward solutions with stakeholders to overcome key barriers to expanded FI participation in the Security Summit, External Leads/Rejects programs and ISAC.

IMPROVE TAXPAYER OUTREACH

14. The IRS should expand outreach and communication to diverse communities and advance its campaign to taxpayers set forth in IRS Publication 4524, Security Awareness for Taxpayers, to community-based consumer organizations by:

    - Partnering with organizations experienced in creating pro-security consumer education content for diverse communities.
    - Ensuring that its consumer education content and distribution efforts have a special focus on reaching diverse communities by collaborating with affinity groups serving populations targeted by scams such as immigrants, senior citizens and people with disabilities.
    - Collaborating with volunteer tax preparers (VITA and TCE programs), community-based consumer organizations, and local government agencies to disseminate security-focused consumer education materials that meets local needs.

15. Working through the Security Summit, the IRS should expand the "Taxes. Security. Together." awareness campaign to provide more outreach and key security messaging through employers and small businesses.

---

[10] Taxpayer Identification Numbers include Social Security Numbers (SSNs) and Individual Taxpayer Identification Numbers (ITINs).

[11] 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. (See the Detailed ETAAC 2017 Recommendations section for more background).

[12] These programs are described in more detail in the following section.

16. To facilitate information exchange with stakeholders regarding IDTTRF, the IRS should establish and support an internal community of practice (COP) for IRS employees serving in a relationship management role. The IRS Office of Communication and Liaison should house the COP and establish platforms for peer communication and learning opportunities.

IMPROVE TAX PROFESSIONAL OUTREACH, EDUCATION & COMMUNICATIONS

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 ERO's on the cyber and physical security risks facing them;
    - Provide a clear and full statement of the security regulations, standards and requirements applicable to a tax professional's participation in IRS e-file, and the potential consequences of failing to comply;
    - Provide simple, clear and actionable guidance on how to implement a security program, preferably consolidated into a single source publication; and,
    - Review, update and improve such content on a regular basis.
18. The IRS should take steps to make tax return preparers more aware that educational courses about internet and data security will qualify for IRS-recognized continuing education credits, assuming the course meets IRS standards for such education.
19. The IRS should amend Circular No. 230 "Regulations Governing Practice before the Internal Revenue Service" to make knowledge about, and implementation of, internet security and the protection of taxpayer data a requirement for all preparers subject to the rules of practice contained in the Circular.
20. IRS security alerts to tax professionals should be differentiated from other IRS communications (letterhead, font size, color, etc.) to highlight the urgency of the message and recommended actions.
21. The IRS should expand and enhance its current use of social media channels to more broadly and consistently communicate the "Protect Your Clients; Protect Yourself" campaign aimed at increasing security awareness among tax professionals.

INCREASE ELECTRONIC FILING

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

DETAILED ETAAC 2017 RECOMMENDATIONS

ENHANCE AUTHENTICATION AND THE TAXPAYER EXPERIENCE

BACKGROUND

Identity proofing and authentication are critical enablers to electronic tax

IDTTRF is based on the ability of criminals to acquire a sufficient amount of accurate personal information about taxpayers and, then, to file fraudulent tax returns in their names. Unfortunately, the identities of millions of taxpayers and their families have become widely available as a result of relatively recent data breaches.

To stop IDTTRF, the IRS and state revenue agencies must be able to determine the legitimacy of taxpayers and returns filed in their names. That determination is founded on the ability of IRS, States and Industry to (i) confirm that taxpayers are who they say they are ("identity proof") and, then, (ii) authenticate taxpayers and their tax filings on an ongoing basis. Identity proofing and authentication are also fundamental to the IRS' ability to expand its suite of online taxpayer services, and the IRS has implemented an improved "Secure Access" platform to enable taxpayers to be identity proofed and subsequently authenticated on an ongoing basis.[13]

The Security Summit has made significant progress in improving authentication

Working collaboratively, Security Summit participants have made significant progress in improving the ability of the IRS, States and Industry to authenticate tax return filings and, thereby, spot and stop fraudulent returns. Specific authentication-related actions taken in support of the 2016 filing season included: the implementation of enhanced customer identification and validation requirements to prevent account takeovers; industry collection and sharing of 20 data components from tax returns to improve fraud detection/prevention; and, the performance of data analysis and the provision of potential ID theft data to the IRS and States by large e-file providers.

These actions, coupled with other Security Summit initiatives, resulted in a meaningful reduction in IDTTRF during the 2016 filing season as evidenced by:

- A significant drop in Identity theft affidavits (a reduction of nearly 50% during first nine months of 2016 compared to 2015)

[13] See https://www.irs.gov/individuals/secure-access-how-to-register-for-certain-online-self-help-tools. Once registered through Secure Access, taxpayers can access IRS online services such as Get Transcript Online, Get an IP PIN and "your tax account." Not surprisingly, IRS has already detected active attempts to breach its Secure Access identify proofing and authentication platform. IRS, States and Industry must continuously assess innovations and alternative techniques to improve their existing identity proofing and authentication capabilities on an ongoing basis. Congress has expressed a strong interest in understanding the security of IRS online tools. See House Committee on Ways and Means letter dated April 28, 2017.

- An increase in the IRS halting fraudulent returns before entering the IRS return processing systems[14]
- A reduction in fraudulent refunds needing to be stopped by banks (>50% reduction, which reflects the IRS' improved ability to stop fraudulent returns before refunds are paid out)[15]

Based on these successes and other learnings, the Security Summit took several additional actions in anticipation of the 2017 filing season including: expanded IRS W-2 Verification Code collaboration to 50 million forms from 2 million forms; continued enhancement of password requirements for taxpayers and tax professionals; and, expanded collection and/or transmission by the tax industry to the IRS and States (37 new data elements for individual returns and 32 data elements from business tax returns).

RECOMMENDATION #1: The IRS should analyze the ongoing effectiveness of the Security Summit's initiatives to identity proof and authenticate taxpayers and tax return filings, including a cost/benefit assessment of their impact on Identity Theft Tax Refund Fraud (IDTTRF) reduction and the taxpayer experience.

Recommendation #1 Supporting Details

ETAAC agrees with the Authentication Work Group on the ongoing need to analyze the impact of its decisions and actions in the identity proofing and authentication areas. ETAAC believes that this analysis should include an assessment of three key impacts[16]:

(i) IDTTRF Reduction: *To what extent have Security Summit's specific identity proofing and authentication actions contributed, generally or specifically, to the reduction of IDTTRF?*

(ii) Taxpayer Experience: *How are Security Summit's specific identity proofing and authentication actions impacting the taxpayer experience (positively or negatively), and are they warranted based on their contribution towards IDTTRF reduction?*

(iii) Cost/Benefit: *What resource demands, costs and burdens are being incurred by the IRS, States and Industry[17] to implement these actions, and are they warranted based on their contribution towards IDTTRF reduction – or are their alternative investments or actions that would be more impactful and less burdensome?*

[14] IRS Press Release IR-2016-144 dated November 3, 2016, reported that IRS statistics showed a nearly 50 percent drop in the number of fraudulent returns that made it into the IRS tax processing systems, which reflected that the Summit's efforts are working up front in the tax process.

[15] The cause of this reduction needs to be analyzed. ETAAC believes the largest contributor is a reduction in fraudulent returns "getting through" processing. However, IRS should validate whether there have been any changes in how FI's are conducting their fraud analysis and reporting.

[16] Any analysis should assess the impacts of IRS' accelerated access to W2's and other information returns pursuant to the PATH Act.

[17] IRS should lead an effort to conduct this cost/burden estimate, which will require the cooperation and support of States and Industry. IRS does not control whether the data is provided by external partners.

RECOMMENDATION #2*:* In light of past Security Summit successes, the IRS should continue to invest in innovative and collaborative initiatives with Security Summit stakeholders and trusted third parties to identify and test enhanced identity proofing and authentication approaches, including accessing new sources of authentication data and testing new identity proofing technologies.

Recommendation #2 Supporting Details

Much of the Authentication Work Group's short term focus has been on improving the authentication of tax filings. Going forward, the Work Group also wants to increase its attention to finding promising approaches to better identity proof and authenticate taxpayers themselves. Based on its discussions, ETAAC agrees with the direction of the Authentication Work Group, and believes the following three areas warrant further consideration.[18]

1. Continue to Leverage Third Party Information Partnerships & Collaborations. The IRS and States already use third party information to authenticate taxpayers and tax return filings. Third party information also helps the IRS and States avoid or resolve "false positives" (e.g., where fraud filters inadvertently designate returns filed by legitimate taxpayers as potential fraud).

The Security Summit should continue to identify, test and, where appropriate, implement promising third party information sources and collaborations. The IRS needs the resources to strengthen and support the use of third party data. Examples of areas for the Security Summit to consider include: (i) accessing and using other government data, (ii) collaborations with payroll companies, such as the IRS' W2 Verification Code Pilot, and (iii) collaborations with Financial Institutions that have already developed fraud prevention technologies and systems.

Of course, the IRS and States must understand the impact of any identity proofing or authentication solutions on taxpayers, especially low income taxpayers. For example, some authentication models rely on third party public record information or specific technologies, such as cell phones. Many taxpayers do not have public records because they have no credit, don't own homes, etc., or may not be able to afford cell phones. It will be important to find solutions that do not inadvertently or unnecessarily block taxpayers from accessing online services.

2. Enhance Taxpayer Identity Proofing and Authentication Techniques. Understandably, much of the Authentication Work Group's initial "authentication" focus has been on identifying and analyzing potential attributes of a tax return

[18] ETAAC may provide illustrations of specific vendors or solutions, but is not endorsing any vendor-specific solutions or approaches. First, locking in on any specific solutions or approach at this time fails to recognize that the fraudsters are capable and nimble. They have adjusted, and will continue to adjust, their approaches to pursue any vulnerabilities in the protections implemented by the Security Summit. The Security Summit must be able to test multiple new approaches continuously and adjust them when necessary. Second, decisions about vendor-specific solutions are best made by IRS, States and Industry.

filing. The work group now believes that there's an opportunity to expand its work to include investigating alternatives to improve the ability to identity proof and authenticate taxpayers themselves.

ETAAC agrees. Examples of areas for the Security Summit to consider include:

> Leveraging Government-Issued Identification Documents. There are a variety of federal and state government-issued photographic identity cards that might be leveraged for taxpayer identity-proofing. The most ubiquitous government identity card is probably the state-issued driver's license. Numerous vendors appear to leverage this identification. For example, one vendor, MorphoTrust USA, has an "Electronic ID" service that verifies a person's identity by connecting it back to their photograph and identity record with their state's motor vehicle agency. Another vendor, Jumio, has a service called "Netverify® Trusted Identity" that combines computer vision technology, ID verification, biometric facial recognition, and document verification to identity proof consumers. Finally, a third vendor, IDology, has an identity proofing solution that gives consumers the ability to validate a photo ID, and can be linked to extract and correlate other data the consumer has input, as well as perform additional reviews such as deceased checks. In the tax area, Alabama has partnered with MorphoTrust USA to launch a new pilot program utilizing MorphoTrust's electronic ID (eID) to secure state tax refunds for the 2016 filing season. (See http://www.alabamaeid.com/).
>
> There are also federal photographic identity cards, e.g., Department of Defense (ID's for military and civilian employees/contractors), Department of State (passports) and U.S. Customs and Border Protection (Global Entry ID cards). There may be an opportunity to leverage these types of federal identification cards in the same way state drivers' licenses are being leveraged.
>
> Leveraging Other Identity-Proofing Solutions. In addition to identity cards, some solutions broadly leverage other data sources such as deceased checks.

3. Expanding Taxpayer-controlled Protections. There are other taxpayer-specific solutions that are not specifically identity-proofing or authentication services, but do create barriers to IDTTRF. One such approach that the IRS discussed with ETAAC is the concept of a taxpayer being able to "lock and unlock" his/her tax account. By way of illustration, the IRS has created a secure online taxpayer account where taxpayers can create an online account to view their account balance and payment history (See https://www.irs.gov/uac/view-your-tax-account). This online account leverages the IRS' Secure Account platform to identity proof the taxpayer before he/she can create an account. (See https://www.irs.gov/individuals/secure-access-how-to-register-for-certain-online-self-help-tools). Imagine that a "authenticated" taxpayer could leverage this functionality to block the filing of any tax returns in his/her name by "locking"

his/her account or, alternatively, "unlocking" his/her account when the taxpayer wants file his/her return.

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.

Recommendation #3 Supporting Details

A substantial percentage of individual tax returns are prepared and filed using do-it-yourself (DIY) tax return software.[19] The electronic filing of a self-prepared return requires the taxpayer to verify his/her signature by providing his/her prior year (PY) Adjusted Gross Income (AGI) or PY Self-Select PIN.

DIY taxpayers have evidenced significant difficulty in verifying their signature using the PY AGI or PY Self-Select PIN. In each of the 2015 and 2016 Filing Seasons, the IRS reported that approximately 3.5-4.0 million e-file rejects were attributable to errors by the primary taxpayer providing his/her PY AGI or PY Self-Select PIN. In the 2017 Filing Season (for which the "E-file PIN" described below was not available), ETAAC is roughly estimating that error code will increase to almost 6 million e-file rejects.

This situation creates burdens for taxpayers, who must search for their AGI/Self-Select PIN information and attempt to re-file electronically or, alternatively, abandon their attempt to electronically file and instead file on paper. This burden should not be underestimated. Additionally, paper filing prevents the IRS and States from receiving critical return information used to fight fraud that is only available with electronically filed returns. This PY AGI/Self-Select PIN situation must be remedied

Background on IRS Signature Verification for "DIY" Electronically Filed Returns

The advent of self-prepared returns using do-it-yourself (DIY) software raised the question of how to "sign" an electronically filed Form 1040. The IRS has pursued several approaches over time to address this challenge.

Initially, the IRS created a form (the 8453-OL) that taxpayers would sign and mail to the IRS after they electronically filed their return successfully. Requiring the mailing of a form meant that electronic filing was not truly "paperless" and, moreover, many taxpayers failed to file Form 8453-OL. Subsequently, the IRS eliminated the Form 8453-OL, and substituted two requirements – first, the creation of an electronic signature and, second, the "verification" of the signature using a "shared secret."

For the first step, the IRS created the Self-Select Personal Identification Number (PIN). For the second step, the IRS verified the signature by the taxpayer's entry

[19] ETAAC estimates that 40-45% of all individual tax returns are self-prepared and filed by taxpayers using DIY software. Only a very small number of returns are still prepared by hand, possibly as few was 2-3M.

of one of two pieces of information from his/her prior year (PY) return – either the taxpayer's PY adjusted gross income (AGI) or the taxpayer's PY Self-Select PIN. In the absence of this information, the IRS electronic filing system would reject the electronically filed return.

Unfortunately, over time, it became clear that many taxpayers struggled to remember or find their PY AGI or their PY Self-Select PIN. In response, the IRS added a third method for taxpayers to verity their signature – the IRS "Electronic Filing PIN" (EF PIN). To support this new verification option, the IRS created an online tool on irs.gov to enable taxpayers to enter various pieces of personal information to generate an EF PIN. Once obtained, taxpayers could use the EF PIN as an alternative to verify their five digit signature.

The current PY AGI/PIN model is not working and must be replaced

Several developments are driving the need to review and replace the current IRS signature verification model.

First, the EF PIN has been eliminated as a signature verification option, and the corresponding online tool removed from irs.gov in February 2016 as the result of a BOT attack resulting in over 100,000 EF PINs being compromised.[20] ETAAC believes the removal of the EF PIN has had a direct effect on the significant year-over-year increase in primary taxpayer AGI/PIN e-file rejects**.**

Second, most taxpayers don't remember their PY Self-Select PIN, and do not have an independent, consistent way to find it. Although their current software may carry over that information automatically, that backstop is removed when taxpayers shift software providers.

Third, many taxpayers don't have access to, don't know or can't find their PY AGI.[21] Even if they do find their returns, some taxpayers are confused as to which AGI to use.[22]

The IRS online tools where taxpayers might access their AGI information are under steady attack or have limitations. In 2016, the IRS determined that the IRS Get Transcript online tool was compromised, which exposed the tax information (including PY AGI's) of hundreds of thousands of taxpayers. [23] Although the Get Transcript online tool was restored with an upgraded authentication system, the system presents taxpayers with other challenges. The new tool requires a taxpayer to have a credit history (car loan, credit card, etc.) and a cell phone. These additional requirements make complete sense, and are becoming

[20] See https://www.irs.gov/uac/irs-statement-on-the-electronic-filing-pin

[21] Taxpayers may not be able to find their prior year return, they might not have kept a copy, or they may have gotten divorced and their ex-spouse may have the tax files, etc.

[22] IRS and some states determine which AGI is valid in different ways. For example, some jurisdictions consider the AGI from the initially filed return as the relevant AGI where an amended return is subsequently filed. However, other jurisdictions use the AGI from the amended return.

[23] See https://www.irs.gov/uac/newsroom/irs-statement-on-get-transcript. Recently, IRS reported a breach of the FAFSA tax data retrieval tool. See https://www.nytimes.com/2017/04/06/us/politics/internal-revenue-service-breach-taxpayer-data.html?_r=0

standard authentication practices. Unfortunately, many taxpayers (especially low income) don't have credit histories or cell phones, and even taxpayers with this information can experience challenges getting authenticated. Failing to get real time access to PY AGI via Get Transcript pushes a large percentage of taxpayers into the manual transcript ordering process, which takes 1-2 weeks.

Realistically, this delay pushes many taxpayers into paper filing – it's easier to mail the return than wait for their transcript. Paper filing does more than just create extra processing burden for the IRS and state revenue agencies. It exposes these agencies to greater risk of fraud, because an electronically filed return provides several data elements beyond the information in the return to help tax authorities stop fraud – that data is not present in a paper filed return.

Simply put, the current signature verification approach for DIY taxpayers is outmoded, overly dependent on PY AGI and needs to be reviewed and replaced. Fortunately, the techniques now being used to authenticate taxpayers and tax filings have improved significantly in the past two years because of Security Summit actions. We have opportunities to leverage this information to create a new "signature verification" technique, such as by using selected combinations of data now available in the MeF schema as the new "shared secret" to replace the current PY AGI/PIN model.

STRENGTHEN INFORMATION SHARING AND ANALYTICS CAPABILITIES

BACKGROUND: INFORMATION SHARING

Recent Efforts by IRS, States and Industry

The Security Summit Memorandum of Understanding establishes roles and responsibilities for the IRS, Industry and States to share suspicious activity, potential and confirmed identity theft tax refund fraud activity and to provide feedback on the effectiveness of the leads.

Within the Security Summit, the Information Sharing Work Group works on identifying opportunities for sharing information that would improve the collective capabilities for detecting and preventing identity theft tax refund fraud. The Information Sharing Work Group collaborated to establish a requirement for industry e-file providers who file 2,000 or more returns to perform research and analysis and report any suspected identity theft abuse and fraud to the IRS and the states. The IRS published this requirement in IRS Publications 1345, *Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns,* and Publication 3112, *IRS E-file Application and Participation*, for 2016 Filing Season. For 2016, the state operating agreements have like-kind requirements for data sharing and lead reporting to the IRS. At the request of industry and states, the IRS acted as a conduit and facilitated industry data sharing with states via a Secure Data Transfer "flow through" process. This process developed as a baseline for processing year 2016 was used again for processing year 2017.

Information Sharing and Rapid Response

The focus of the Information Sharing Work Group is to share information regarding suspicious activity, recognized patterns and emerging issues within our tax ecosystem. In addition to establishing protocols for reporting suspicious activity and providing feedback, the work group established a Rapid Response Team (RRT) with IRS, State and Industry membership, which is tasked to share information concerning active security threats and incidents impacting the tax ecosystem.

One example of the operation of the RRT related to an incident relating to remote takeovers of tax professionals servers, which occurred in September 2016 -- a few months prior to the start of the 2017 filing season. In this case, the IRS was made aware of 19 incidents involving fraudsters remotely accessing tax professional servers for the purpose of filing IDTTRF returns. The IRS determined that it would re-issue an alert from April and reference the recent Tax Professional memo that instructs tax professionals to reconcile their PTIN accounts. On September 1, 2016, an RRT call was held to apprise IRS' Security Summit partners that another round of account takeovers was occurring and that a news release would be issued the next day that would alert the tax professionals and advise them to take appropriate security measures. The IRS also assessed the threat to determine if more tax professionals were impacted. The impacted EFINs (19) were shared with the states in accordance with IRC 6103(d).

Additionally, the Information Sharing Work Group took several other actions in anticipation of the 2017 filing season including:

- Collaborating with the Authentication Work Group to evaluate proposed additional data elements from electronic returns, and with industry and state partners to test the proposed data elements
- Improving existing information sharing guidance documents, reports and processes, including enhancing the analysis of leads to provide more meaningful communications between state and industry partners. These improvements provide stakeholders with information about emerging filing patterns and other actionable information on questionable filing activity that strengthens our ability to reduce identity theft tax refund fraud across all platforms. All reporting must be centralized and standardized among all ecosystem members.
- Providing information about prior year confirmed and suspicious identity theft account information to industry and states at the start of the filing season to enable Security Summit stakeholders with the opportunity to analyze the information and update their filters.[24]

Accomplishments & Current Focus

The 2016 Security Summit Annual Report, issued June 2016, reported that, as a result of leads reported from industry partners, the IRS suspended 36,000 suspicious returns for further review from January through May 8, 2016, and $148 million in claimed

[24] The IRS also will analyze and address industry lead reporting compliance with Publication 1345 and the requirement upon industry to provide identity theft data.

refunds; twice the amount of the same period in 2015 of 15,000 returns claiming $98 million. Industry's proactive effort helped protect taxpayers and revenue.

The number of people who filed affidavits with the IRS saying they were victims of identity theft dropped 50 percent during the first nine months of this year compared to 2015. (https://www.irs.gov/uac/newsroom/irs-security-summit-partners-expand-identity-theft-safeguards-for-2017-filing-season-build-on-2016-successes)

The Information Sharing Work Group used the 2016 filing season to capture lessons learned and apply them to the 2017 filing season. In 2017, guidance for industry leads reporting incorporated clearer communication elements to report patterns more effectively to all participants. Industry partners are providing leads at minimum on a weekly basis to the IRS and states and, in many cases, more frequently -- often including real time when suspicious activity is identified. The IRS is providing consistent feedback to Industry partners on effectiveness of the Industry Leads. The information sharing (both the Alerts reporting and Rapid Response process) that was instituted for the 2016 filing season was refined and updated for processing year 2017. Among other actions, the IRS engaged the newly formed ISAC to assist in streamlining information sharing.

RECOMMENDATION #4: Working with Security Summit partners, the IRS should document the Security Summit's current information sharing process (including Leads, Leads Feedback, Alerts and Rapid Response processes, and all active participants and information flow paths) to facilitate the identification and implementation of process improvements.

Recommendation #4 Supporting Details

The key objective of the ETAAC's recommended process documentation effort is to review and evaluate the current information sharing leads process to identify efficiencies and process improvement opportunities. ETAAC believes this effort should be led by the IRS and include several key actions:

- Map the current IRS Information Sharing leads activities as a baseline to conduct a process improvement effort.
- Work closely with Industry to refine analytic filters to ensure leads shared with states and the IRS by industry and other participants are actionable. By reducing the "false positives," Industry Leads will become more effective for the recipients.
- Collectively, evaluate the volume of data to ensure manageability and consider certain approaches to mitigate data overload and ineffective use and even non-use.
- Identify ways to improve the timeliness of the Industry Leads reporting to allow recipients to proactively stop confirmed fraudulent returns. In other words, the data submitted and use of that data, should be evaluated, validated, shared and monitored for better and more effective use of the valuable information.
- Ensure the Industry Leads reporting is transmitted in the most efficient and secure manner.

- Work collaboratively and facilitate discussions with States, the Federation of Tax Administrators (FTA) and Industry and explore ways to reduce the state barriers including challenges, limitations and specific legal restrictions to allow for more efficient use of the Industry Leads. The IRS can assist FTA with discussions with States to help address issues and work towards individual state resolutions.
- Work to promote state participation in the sharing of "confirmed fraud" with the IRS and Industry partners in whatever manner and permitted process that is available and appropriate.
- Identify ways to work closely with the states to share best practices on how to use Industry leads to identify fraudulent returns. The ISAC Analyst Community of Practice can facilitate this area.
- Work with the states and other interested parties to ensure full participation in the Alerts portion of the ISAC to eliminate the current need for duplicate Alerts reporting.
- Identify ways to improve the speed and ease of communications on schemes and risky activity identified via the Leads reporting efforts by better defining the paths and mechanics for information sharing. This would result in a more effective rapid response process for managing material issues of concern and risk.

BACKGROUND: INFORMATION SHARING AND ANALYSIS CENTER (ISAC)

Challenges to Information Sharing and Analysis

The Security Summit partners identified that information sharing is a critical element in the fight against identity theft tax refund fraud, and identified the following problems and barriers:

- No centralized platform existed for the IRS, States and Industry to collaborate, view fraud patterns, capture learnings and take action.
- Industry leads information was a "one way flow" from Industry to the IRS and States -- industry was not seeing information from the IRS and States that would enable it to see the whole picture of evolving patterns in the tax ecosystem
- Industry was not getting timely feedback confirming suspected fraud it had reported
- States had varying technological capabilities to access and utilize industry leads reporting information which resulted, in some cases an inability to utilize the leads reports.
- There were varying levels of capability for analysis of the leads by Industry and States depending on many factors for staffing and resources to historical experience.
- The lack of a centralized platform prevented stakeholders from learning from what others were seeing
- There was no value-added analysis shared on the leads provided, consequently, industry who provided the leads were unable to validate the

quality of the information provided or end result of benefit of the data submitted.

ISAC Establishment & Goals

The Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC) was formed to enable a significant reduction in identity theft tax refund fraud by:

- Providing a highly-secure, usable platform to share information about best practices, leads, and incidents among the IRS, States and Industry
- Developing analytics capabilities to measure current practices and predict and prevent identity theft tax refund fraud
- Creating an early warning system for IDTTRF schemes and cyber-security attacks via leads and alerts messaging (email blasts).

The ISAC is intended to build upon the existing Information Sharing Working Group leads program within the IRS to collect and analyze the leads that are currently submitted, and also to provide a centralized point for consolidating information. The information and analysis will assist stakeholders in defense of critical mission functions and increase the security of the tax ecosystem. The ISAC will eventually centralize, standardize, and enhance data compilation and analysis to facilitate sharing actionable data and information.

An ISAC pilot was deployed in January 2017, with the intent to continue operating through 2018. IRS engaged MITRE Corp (an FFRDC – federally funded research and development center) to be its Trusted Third Party (TTP) to assist in the development of the ISAC. The ISAC consists of two parts: the ISAC Operational Platform and the ISAC Partnership. The IRS owns and pays for the ISAC Operational Platform. However, the ISAC Partnership is a governance structure that makes recommendations to the TTP about the ISAC. The ISAC Partnership has representation from the IRS, Industry and the State Departments of Revenue; and is self-supported by the stakeholders, i.e. the IRS does not solely fund the partnership. Initial ISAC capabilities include a centralized location for sharing alerts, leads sharing, analyst community of practice, data visualization and private document sharing.

As a benchmark, the Security Summit studied other ISACs – notably the HFPP established by the Department of Health and Human Services (HHS) which works with its industry partners to curtail health care payment fraud, and the Federal Aviation Administration (FAA) which works with its industry partners on aviation issues. Both HHS and FAA use an ISAC work group to exchange ideas, schemes and trends.

Taxpayer privacy is a top focus of the Security Summit and ISAC. IRC Section 6103 governs IRS sharing of tax return information. State tax information privacy laws vary, but govern the sharing of data by States. IRC Section 7216 governs the use and disclosure of tax return information by the tax preparation industry. These laws, and supporting regulations, are carefully reviewed as each new step for ISAC is considered.

ISAC Accomplishments in 2017

The ISAC Pilot Program became operational in January 2017. Key activities in the effort to “stand up” ISAC included:

- Designation of an IRS Executive Official for ISAC oversight and leadership of the ISAC Operational Platform
- Establishment of a 15 person Senior Executive Board to manage the partnership, which includes five individuals from each of IRS, States and Industry
- Engaging a high degree of participation including 39 State and Industry members
- ISAC is now in the early stages of refining its processes, analyzing data and sending alerts.

Looking Ahead

The ISAC, Leads Sharing and the function of the Information Sharing Work Group should be evaluated to ensure efficient decision-making and operations. Additionally, ISAC findings and analysis should inform future requirements for leads reporting and authentication data elements to ensure practices being implemented are creating value, based on objective analysis and that the burden imposed on taxpayers and industry are not undue. Further, the ISAC should perform the function of being the sole central and pivotal manager of information within the confines of its charter.

RECOMMENDATION #5: The IRS should encourage and enable greater participation in the IDTTRF Information Sharing and Analytics Center (ISAC) by the many stakeholders affecting the tax ecosystem.

Recommendation #5 Supporting Details

The IRS and the ISAC Board should develop an established, clear way for new participants to join the ISAC. Greater inclusion and participation by all stakeholders in the tax ecosystem should be encouraged -- from existing stakeholders (IRS, States, Industry, and Financial Institutions) to new stakeholders (Payroll Processing Companies, Credit Companies and other organizations that impact the tax ecosystem).

State participation in the ISAC was initially delayed but, after key stakeholders (including ETAAC members and the ISAC Partnership Senior Executive Board members) engaged to clarify participation requirements, state participation has been steadily increasing. Given the current robust support for the ISAC and the intention that everyone participates in the ISAC, it will be important to keep all stakeholders engaged to promote a collaborative environment that supports full participation by all interested stakeholders. It is critical to the success of the ISAC to harvest lessons learned from this first iteration in order to be smarter about how to bring new stakeholders into the ISAC and to establish a way for new participants to join with appropriate understanding of communication and vetting among the existing stakeholders.

RECOMMENDATION #6: The IRS should identify, analyze and, where possible, mitigate barriers that preclude IRS information sharing with ISAC for the purposes of fighting IDTTRF.

Recommendation #6 Supporting Details

Potential limitations on IRS data sharing within the ISAC environment should be evaluated to ensure that, to the maximum degree permissible, adequate IRS data and information sharing is not an unnecessary obstacle or restriction to the ISAC, leads reporting and other identity theft tax refund fraud prevention initiatives. The removal or adjustment of such limitations, where appropriate, may require changes in legislation, regulations or policy.

Some illustrations of the types of IRS information that may be valuable to the ISAC to fight identity theft tax refund fraud include: (i) feedback on leads reports (whether the lead was confirmed fraud or confirmed not fraud), (ii) notification of compromised EFINS, and (iii) notification of compromised PTINS.

RECOMMENDATION #7: Congress and the IRS should adequately fund ISAC operations.

Recommendation #7 Supporting Details

The ISAC requires adequate funding and sufficient resources to ensure its future viability. Any ISAC funding should be allocated, partitioned and preserved to ensure its continuing availability to ISAC. The IRS estimates the IRS cost will be between $4-8M/year. Once operational cost drivers are more fully known, the IRS may refine its estimate.

ENHANCE SECURITY & SECURITY SUMMIT PROACTIVITY

BACKGROUND: CYBERSECURITY

Cybersecurity is a national priority

GAO has consistently identified federal information security as a high risk.[25] Similarly, the Treasury Inspector General for Tax Administration (TIGTA) has identified the security of taxpayer information and IDTTRF as the top challenges facing the IRS.[26]

Both IRS and Congress have taken steps to respond. The IRS has recognized the threat as a priority in the IRS Strategic Plan,[27] and engaged State and Industry leaders to create the Security Summit.[28] Congress has acted to provide supplemental funding to fight IDTTRF and improve cybersecurity.

ETAAC previously called for enhanced security practices in tax ecosystem

In its June 2009 Report, ETAAC reinforced the importance of security to electronic tax administration with a recommendation that "*IRS should work with the tax preparation industry and states to set high industry standards and determine the best model for the efficient, effective oversight of tax software services."* Subsequently, ETAAC formed the

[25] See GAO High Risk Series Report (GAO GAO-17-317).

[26] See https://www.treasury.gov/tigta/management/management_fy2017.pdf

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

[28] The tax preparation Industry plays a critical role in securing our federal and state tax systems given that all, or nearly all, federal and state electronically filed individual returns are created by and transmitted through its systems.

ETAAC Software Subcommittee Security & Privacy Work Group ("ETAAC Security Work Group") consisting of IRS, State and Industry representatives to make detailed recommendations concerning cybersecurity. After almost 1 ½ years, the ETAAC Security Work Group issued a final report with detailed cybersecurity recommendations,[29] which was adopted by ETAAC in its 2011 Annual Report to Congress.

Security Summit has made significant progress toward improving cybersecurity

Shortly after the establishment of the Security Summit in 2015, the IRS created the Strategic Threat Assessment and Response (STAR) Work Group, which is comprised of a highly collaborative group of IRS, State and Industry[30] representatives. The mission of the STAR Work Group is to improve the tax ecosystem's security posture by adopting a security framework and methodology to assess threats and develop strategic responses. Its currently stated roles and responsibilities are to:

- Adopt and refine an IT security-related framework that improves the security capabilities for each partner in the tax system, regardless of such things as size, level of technology, business model and whether they are government or private sector.
- Develop an assessment methodology to help organizations in identifying, addressing and resolving their own security risks in an orderly, cost-effective and consistent manner.
- Act as the clearinghouse for the other Security Summit work groups and participants by reviewing, identifying, coordinating and communicating IT and security-related best practices through people, processes and technology.

One of the most important initial actions of the STAR Work Group was its agreement to align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), which is foundational to promote the protection of information technology (IT) infrastructure and reduce cybersecurity risk across the ecosystem. Additionally, the Group agreed to focus initially on tax software vendors, which is consistent with ETAAC's past recommendation to focus on the electronic tax ecosystem. Recently, the STAR Work Group expanded to engage payroll providers given the connection between Form W2 and IDTTRF, and the need to protect W2 data. The newly formed Payroll Subgroup complements the previously formed Tax Subgroup.

Looking ahead, the STAR Work Group is focused on developing a cyber-threat assessment of the tax ecosystem, incorporating changes in NIST guidance and continuing implementation of the Cybersecurity Framework.[31] Some of its 2017 priorities include: Continuing external engagement with States and Industry, as well as with other federal agencies; Continuing the implementation of the NIST Cybersecurity

[29] The Security Working Group's final report is publicly available online in the GSA FACA database. See http://www.facadatabase.gov/committee/historymeetingdocuments.aspx?flr=91433&cid=1648&fy=2011

[30] The initial focus for industry participation was on the tax software and preparation community, which has since been expanded to include payroll service providers.

[31] This action is consistent with the direction of the White House's Executive Order titled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" issued on May 11, 2017.

Framework (CSF) via select NIST Special Publication (SP) 800-53 security controls (3 year phase in); Analyzing the results of Self-Assessments delivered in early 2017; Determining Independent Assessment and Compliance Options; and, Developing a tax ecosystem threat assessment

The STAR Work Group has taken a sound approach to address ETAAC's previous recommendations to establish appropriate security standards to protect the tax ecosystem, and has made significant progress in a very short time. As explained below, we need to expand its efforts, which will likely require increased resources to be successfully accomplished.

RECOMMENDATION #8: The STAR Work Group should continue its current direction and collaborative approach to implement the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Recommendation #8 Supporting Details

ETAAC is encouraged by the significant progress of the STAR Work Group to foster a collaborative effort by the IRS, States and Industry to take concrete actions to reduce IDTTRF and enhance cybersecurity. ETAAC fully supports the STAR Work Group's direction, and wants to reinforce several elements of its approach that ETAAC believes are the key enablers of that progress:

1. IRS Leadership. The IRS' continued leadership in sponsoring and shaping the Security Summit is critical to its success, including the high level of attention and resources that IRS' top leaders have committed to the Summit. Through its convening authority, the IRS has created awareness, focus, collaboration and commitment across a broad base of disparate stakeholders.
2. Collaborative Approach. The implementation of the NIST Cybersecurity Framework across the broad tax ecosystem is a significant change management effort that requires open communications and a willingness to listen and adapt.[32] The STAR Work Group's current approach fosters open communications and debate, and has created a dynamic process where stakeholders can continuously assess and enhance the ongoing implementation of the NIST Cybersecurity Framework. Given the high level of current engagement across the STAR Work Group, ETAAC believes that the current voluntary, collaborative approach, at least in the short term, is the best approach to accelerate better security outcomes sooner rather than later.
3. Single Standard. The STAR Work Group should continue its work to arrive at a single common security framework that can be adapted and applied across a broad range of federal, state and industry stakeholders. A common

[32] Developing and implementing a common security framework across public and private stakeholders is a significant undertaking, and numerous "lessons learned" will be generated. Each organization has a unique information technology environment, and multiple factors contribute to determining what risk(s) may be present within an environment and what might be required to demonstrate full compliance with a NIST security control. Factors that need to be taken into consideration include, but are not limited to: hosting environment; application architecture; organizational size and structure; 3rd party service providers; usage of commercial and/or open-source technology.

framework will provide a clear focus for constrained security resources, retain a measure of commonality even when the standard is adapted for application across a broad range of stakeholders with different risk profiles, enable resources to be leveraged across multiple jurisdictions, and facilitate the capture and application of common lessons learned across all stakeholders. In contrast, ETAAC believes the application of multiple security frameworks by the IRS and States would inhibit the benefits described above.

4. Focus on Electronic Tax Ecosystem First. ETAAC agrees with the STAR Work Group's decision to focus its initial attention on the electronic tax ecosystem. The key industry players in this space include Software Developers, Transmitters and Online Providers (as defined in the IRS e-file Program). ETAAC also agrees with the STAR Work Group's decision to expand its focus to payroll service providers given the critical need for secure Form W2 data.
5. Phased Implementation. ETAAC agrees with the STAR Work Group's phased implementation of NIST controls over a three year period, adjusting as necessary.
6. Self & Independent Assessment. In the short term, ETAAC believes that the STAR Work Group should continue to focus on building a robust self-assessment capability among stakeholders. This includes helping stakeholders understand, apply and validate the effectiveness of their controls, and identifying barriers to success that can be shared and overcome by the collective group and used to develop best practices. Longer term, despite its potential cost, independent assessment[33] must be considered as a supplement to self-assessment. The STAR Work Group should continue its discussions about whether, when and how to incorporate independent assessments into any security oversight model.
7. Methods for IRS Validation. Irrespective of the type of assessment model, IRS must have a method for monitoring and guiding the implementation and operation of the NIST Cybersecurity Framework. The STAR Work Group should have discussions about the optimum way for the IRS to carry out this responsibility.
8. Build Capability. There is no lack of content in the security area, but much of it is overwhelming and complex. The STAR Work Group should develop an understanding of how to work with a diverse group of enterprises and, along that journey, create "living" tools to help companies prioritize and implement enhanced security standards. Examples include self-assessment templates, simple security implementation guidelines for small preparers, etc.

RECOMMENDATION #9: The STAR Work Group should identify and pursue opportunities to extend federal, state and industry participation in its initiatives and, where appropriate, expand its engagement with other Security Summit Work Groups.

[33] Independent assessment includes third party assessments, as well as internal assessments by qualified groups, for instance such as independent departments having Internal Audit responsibilities, etc.

Recommendation #9 Supporting Details

In addition to its current focus, ETAAC agrees with STAR's desire to expand its focus to encompass the following areas over the coming years:

1. Expand Participation and Membership
    a. Increase Participation of MOU Signatories. The STAR Work Group has a high degree of engagement with Security Summit MOU signatories. For example, nearly 70% of industry participants in the Security Summit voluntarily conducted and submitted self-assessments on their implementation of the NIST security controls. That "first year" participation is very good considering the demands of preparing for and executing a tax filing season, but STAR is striving for 100% participation from MOU signatories. We support the STAR Work Group's decision to develop an engagement strategy for industry participants in the Security Summit who are currently less engaged, including identifying and overcoming barriers to participation.
    b. Expand Engagement outside of the current Security Summit Members. Not all companies are signatories to the Security Summit MOU. We support the STAR Work Group's decision to develop an engagement strategy to increase industry participation beyond those that are signatories to the Security Summit. Additionally, we support STAR's efforts to increase the participation of other federal agencies and states.
    c. Expand to Preparer Security. Once it achieves sufficient progress in the electronic tax ecosystem, the STAR Work Group should determine whether and how to engage with the tax preparer community to improve its security posture.
2. Increase Engagement with Other Work Groups. The STAR Work Group has some unique technical skills. ETAAC believes that the overall Security Summit would benefit from broader engagement by the STAR Work Group with other Security Summit Work Groups. For example, there may be insights that STAR could bring to the Authentication Work Group. Similarly, STAR could have a role codifying and implementing the initiatives of other working Groups, such as the "Trusted Customer" requirements.

BACKGROUND: TRUNCATED TINS

IRS return documents (forms, schedules, etc.) contain sensitive taxpayer information for individuals and family members. Criminal elements have targeted the theft of sensitive taxpayer information contained in physical records or on computer hard drives in tax offices and entities required to file taxpayer information returns.[34] This highly sensitive data, especially Social Security Numbers (SSN), are used to file fraudulent tax returns.

[34] "*Increasingly, tax professionals are being targeted by identity thieves. These criminals – many of them sophisticated, organized syndicates - are redoubling their efforts to gather personal data to file fraudulent federal and state income tax returns*." See https://www.irs.gov/individuals/protect-your-clients-protect-yourself last updated March 21, 2017

These documents may or may not be filed with IRS and must be retained by tax professionals for multiple years, both electronically and in physical paper records.[35] As a result, these files are at continuing risk of being stolen or compromised by criminals or employees.

RECOMMENDATION #10: To mitigate the risk of stolen identities, the IRS should evaluate, and change where appropriate, current regulations to increase the permitted use of Truncated Taxpayer Identification Numbers (TTINs) on IRS documents.

Recommendation #10 Supporting Details

Using TTINs as a potential remedy & Recent Form 8879 Illustration

One potential approach to reduce the risk of stolen SSNs from tax preparer records is to allow the use a truncated taxpayer identification number(s) (TTIN). The TTIN is generally the last four digits of the primary SSN. There is precedence for this approach -- the IRS has permitted the use of TTINs on other tax documents.[36]

Presently, however, there are regulatory barriers to taking this action more broadly.[37] An incident this filing season with TTIN's on Form 8879 illustrates this current barrier. In this case, the IRS became aware that some software packages were truncating the SSN's on Form 8879 for preparer "file copies" as a security measure to protect taxpayer SSNs. The IRS issued the following guidance:[38]

> *"The IRS recently became aware of instances with preparer software where SSNs are being redacted or truncated, specifically on the Form 8879, IRS e-file Signature Authorization.*
>
> *The following is the existing Treasury guidance concerning treatment of SSNs as it applies to the Form 8879:*
>
> - *Treas. Reg. section 1.6109-4(b)(2)(ii) prohibits the use of a TTIN* on a statement or document if the form or instructions specifically require the use of a social security number (SSN). The instructions to the Form 8879 instruct the ERO to "[e]nter the name(s) and social security number(s) of the taxpayer(s) at the top of the form."*

---

[35] One illustration of a document prepared but not filed with IRS is Form 8879 – the IRS efile Signature Authorization, which expressly requires the taxpayer(s) full social security number. Preparers are advised "*Don't send Form 8879 to the IRS unless requested to do so. Retain the completed Form 8879 for 3 years from the return due date or IRS received date, whichever is later."*

[36] See, for example, Internal Revenue Bulletin: 2014-31, July 28, 2014, TD 9675, *IRS Truncated Taxpayer Identification Numbers. See https://www.irs.gov/irb/2014-31_IRB/ar07.html*

[37] IRS Reg. 301.6109-4(2)(iii) expressly indicates "*A TTIN may not be used on any return, statement, or other document that is required to be filed or furnished to the Internal Revenue Service*." For more regulations in this area, see https://www.gpo.gov/fdsys/pkg/CFR-2015-title26-vol20/pdf/CFR-2015-title26-vol20-sec301-6109-4.pdf

[38] This guidance was contained in an IRS email dated March 21, 2017 and titled "Important Information Regarding Form 8879" and sent to the "*W&I MeF MailBox".

- *Treas. Reg. section 1.6109-4(b)(2)(iii) also prohibits the use of a TTIN* on any return, statement, or document that is required to be filed with or furnished to the IRS.*

Because the Form 8879 and its instructions require the use of a taxpayer's SSN and because, if requested by the IRS, the Form 8879 is a form required to be furnished to the IRS, the use of TTINs on Forms 8879 is not authorized by Treas. Reg. section 1.6109-4(b)(1).*

Please immediately confirm your software does not currently truncate or redact SSNs on forms that do not allow such in the forms instructions, and on forms that are filed with or may be furnished to the IRS. If you find your software has such redaction, please correct this issue immediately.

More guidance will be forthcoming from IRS concerning what steps must be taken for those Forms 8879 that have been produced to date with a redacted or truncated SSN.

**truncated taxpayer identification numbers (TTINs)"*

A few days later, the IRS advised that it would not require any corrective action because elements present on each tax return submission could be used to associate a Form 8879 with the correct taxpayer's Form 1040, thereby enabling the IRS to verify the taxpayer's signature if necessary.[39]

The broad use of TIN's on IRS documents increases the risk of IDTTRF

The IRS has recognized the risks and opportunities in this area, and has already revised regulations to permit the use of TTINs on certain IRS forms. In the recent incident with Form 8879, IRS action suggested that in some instances it has other data elements on tax return submissions that can be used to verify the taxpayer. Moreover, in connection with the Security Summit, the IRS has steadily increased the amount of information or resources it uses to identity proof or authenticate both taxpayers and tax returns.

Under the circumstances, ETAAC believes that the IRS should evaluate opportunities and, where appropriate, permit the use of TTIN's on IRS documents filed with the IRS or otherwise retained by tax professionals. Any implementation of this recommendation should be done in active collaboration with States and Industry.

BACKGROUND: BEING PROACTIVE

One element of the mission of the STAR Work Group is to improve the tax ecosystem's security posture by adopting a methodology to assess threats and develop strategic

[39] In a March 25, 2017 email titled "Follow up Information for Form 8879s with redacted SSNs" sent to the *W&I MeF MailBox, the IRS stated in part that *"After meeting with IRS Counsel, it was determined that, for Form 8879s thus far produced with redaction or truncation of SSNs, no corrective action is needed. There are elements present on each tax return submission that can be used to associate a Form 8879 with the correct taxpayer's Form 1040, allowing the Service to verify, if necessary, that the taxpayer signed the penalties of perjury statement on the Form 8879 in satisfaction of the requirement that the return be executed under penalties of perjury."*

responses. Anticipating where the criminals will go next is essential. We need to be proactive; that is, skate to where the puck is going to be, not where it is at the moment.

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.

Recommendation #11 Supporting Details

Our fraud and cybersecurity threat is motivated, capable, well-funded and nimble.

The mission of the STAR Work Group includes assessing threats and developing strategic responses – in other words, being proactive. Given that mission, the STAR Work Group must continue to capture lessons learned and spot trends in fraud threats and cybersecurity risks. Then, we must leverage these learnings to build a capability that allows us to detect where the criminals are shifting their attention to take advantage of vulnerabilities in our security and fraud prevention efforts. ETAAC believes that part of building that capability includes implementing operating mechanisms that enable Security Summit stakeholders to brainstorm and anticipate IDTTRF and security trends. An illustration of a potential operating mechanism would be a "Red Team" exercise[40] or some other conflict simulation model.

EXPAND FINANCIAL INSTITUTION ENGAGEMENT

BACKGROUND

Financial Institutions are critical to successfully fighting IDTTRF

To succeed, criminals must successfully obtain the money issued by the revenue agency – most frequently in the form of an electronic direct deposit but also, to a lesser extent, the deposit of a mailed paper check or even its cashing.

Financial Institutions (FIs) play a critical role in blocking IDTTRF because they provide the accounts and refund settlement products that taxpayers use to receive refund deposits whether by electronic direct deposit or the deposit of paper checks. Significantly, FI's have unique visibility into several key indicators of potentially fraudulent activity including account creation, account activity (frequency, timing and types of deposits and withdrawals) and repayment performance.

FI's also have legal obligations relating to "know your customer" requirements (including the associated implementation of Customer Identification Program procedures, usually referred to as CIP) and must report suspicious bank account activity to Treasury's Financial Crimes Enforcement Network (FinCEN). Simply put, FI's are well-positioned to identify and report suspicious patterns and trends. Building increased FI awareness of IDTTRF and deeper relationships with the IRS and state DORs will enhance FI's ability to stop payment and return the related suspect funds back to the agencies for further diligence rather than further release them out into the public where they may never be recovered.

[40] See https://en.wikipedia.org/wiki/Red_team

The IRS and States have had active outreach programs to obtain and expand FI participation in the Security Summit. For example, both the IRS and States have solicited FI participation in programs that enable FI's to identify and return suspicious refunds. At the federal level, IRS' refund recovery program focused on FI's has two components: "External Leads" and "R17."

- IRS' External Leads Program creates a process whereby FI's report key information concerning questionable deposits identified by them to the IRS External Leads Group. Upon receipt of a lead, IRS External Leads screens and validates the associated lead and account information. Where potential fraud is validated, the IRS will request that the FI return the suspicious refund electronically via Treasury's Bureau of Fiscal Service (BFS).
- Under the R17 Opt-In Rejected Direct Deposit Process,[41] the IRS and BFS have teamed with NACHA and the Electronic Payments Association to enable FI's to use a repurposed Automated Clearing House (ACH) Reject Reason Code to reject direct deposits involving questionable tax refunds.

The IRS currently estimates over 6,000 FI's receive federal refund direct deposits. Active FI participation in IRS programs varies – approximately 700 FI's are participating in the IRS External Leads program and approximately 330 FI's are participating in the IRS' R17 program.[42]

IRS has made significant progress in increasing FI participation in the Summit

In recognition of FI's role in stopping IDTTRF, the Security Summit created the Financial Services Work Group (FSWG). In addition to IRS and States, FSWG participation includes numerous banks, prepaid card providers, refund settlement product providers and other financial services providers companies, as well as industry trade groups.[43]

At its inception, the FSWG undertook to examine and explore additional ways to prevent and deter criminals from potentially accessing traditional financial products as well as tax-time financial products. The focus of specific actions taken in support of the 2016 filing season was working with FI's to (i) refine the definition of Ultimate Bank Account (UBA)[44] to help determine final destination of refunds, and (ii) establish naming convention for state tax refunds and a process for FI's to return suspicious state tax refunds to states.

FI participation in the FSWG has allowed the IRS to recover fraudulent refunds that may have slipped through its fraud filters. Based on those successes, FSWG took several actions in anticipation of the 2017 filing season including: expanding the definition of

[41] Reason Code17 (R17) is used for returns with name mismatches, ID Theft and questionable refunds. R17 ensures a uniform approach in the rejection of questionable IRS refunds, thereby protecting law-abiding taxpayers while reducing the instances of taxpayer fraud. Determination of validity and final dispensation of a refund remains with the IRS pursuant to its review process. R17 is open to financial institutions that participate in the IRS External Leads Program or that are NACHA's direct members.

[42] Many states have comparable leads and reject programs.

[43] Current examples include the Network Branded Prepaid Card Association, the BITS Financial Services Roundtable and the Electronic Payments Association.

[44] UBA helps identify actual owners of an account.

UBA to include all refund transfer products, including gift and pre-paid cards, paper checks and direct deposit; conducting several "test and learn" pilot programs to enhance ways of identifying and stopping fraudulent or questionable refunds; identifying best practices used to identify fraudulent refunds and sharing that information with other financial institutions; and working with 23 states to create an External Leads Program (modeled after IRS' program) to allows FI's to help identify state tax refunds that appear fraudulent and return them to states for validation and review rather than depositing them.

RECOMMENDATION #12: Based on fraudulent refund patterns, the IRS should target those Financial Institutions (FIs) most vulnerable to IDTTRF deposits to engage their participation in the Security Summit and External Leads/Rejects programs, while strengthening IRS' corresponding ability to handle increased suspect case volume.

Recommendation #12 Supporting Details

There is no silver bullet to deal with refund delivery issues associated with IDTTRF.[45] The IRS and States must have robust FI participation in the Security Summit and in their leads and R17 programs. Based on its discussions, ETAAC believes the following four areas warrant further consideration by the Security Summit.

1: Identify and Engage with FI's Being Targeted by Criminals. FI's come in various categories, sizes and levels of resources and sophistication. Product feature and related services vary as well. They are not all the same, and criminals know that. As a result, it's essential for the IRS to analyze and understand where and how criminals are receiving fraudulent refunds. The IRS should understand:

Fraudulent Refund Delivery: *What methods are criminals most using to transmit (direct deposit, mailed checks) and receive (direct to bank accounts and prepaid, indirectly via refund settlement products, mobile check deposit) fraudulent refunds?*

FI and Product Targeting: *What are the characteristics of the FI's and financial products being targeted by criminals?*

Vulnerabilities: *What specific institutional, procedural or product/service vulnerabilities are being exploited by criminals?*

2: Increase Targeted FI Outreach to Increase Participation in Security Summit & Leads Programs. The IRS should develop and execute a coordinated, targeted outreach effort process to increase FI awareness of and participation in Security

[45] IDTTRF's association, if any, with specific products may be less about the characteristics of a given product, and more about how companies execute their "customer identification processes" (CIP) or specific business models. Any suspected correlations must be carefully studied and validated, including understanding the impact on low and moderate income taxpayers, before any action is taken. Moreover, technology is rapidly changing. Today's "banking product of choice" for fraudsters could easily be some other product tomorrow. New banking models and money transfer/payment products are introduced every year, and fraudsters will exploit vulnerabilities whether it's virtual banks or mobile check deposit via a smart phone.

Summit and External Leads/R17. Any outreach should leverage IRS, State and Industry (both trade groups and individual companies) resources.

The logic underlying our recommendation is two-fold. First, there are thousands of FI's and it's not realistic or sensible for the IRS and States to pursue all of them for participation in Security Summit and External Leads/R17 programs. Instead, the IRS and States should target specific types of FI's for participation based on their risk profile. Second, the IRS should collaborate with States and Industry to find the best way to engage with targeted FI's, and use their collective resources as part of a coordinated outreach effort. The IRS doesn't have the resources to solicit FI participants on its own.

3: Enable FI's with Off-the-Shelf Toolkits. FSWG should create "off the shelf" tools to assist FI's, which could include model policies, procedures and tools (templates, checklists, etc.), staff training, and best practices. Tremendous learnings are being gained in the Security Summit about the best way for FI's to identify suspect refunds and to participate in External Leads/R17 programs. Those learnings need to be captured and systematically applied so that newly participating FI's can accelerate their path to effectiveness.

4: Strengthen IRS' Ability to handle increased Leads/Rejects. The IRS needs the resources to strengthen its back-end services that support the External Leads/R17 programs. Those back end services including the "account treatment" groups that will be handling increased FI reporting as FI participation in External Leads/R17 increases, as well as other affected internal support services such as criminal investigations and IT.

RECOMMENDATION #13: The IRS should identify and work toward solutions with stakeholders to overcome key barriers that preclude FI participation in the Security Summit, External Leads/Rejects programs and ISAC.

Recommendation #13 Supporting Details

Based on its discussions, ETAAC believes the following two areas warrant further consideration by the Security Summit.

1: Identify and analyze barriers to increased FI participation or program effectiveness. ETAAC has identified several potential barriers affecting whether and how effectively an FI will participate in Security Summit and IRS and State external leads and R17 programs.

By way of illustration, one potential barrier appears to be information sharing. On the one hand, the effectiveness of IRS and State External Leads or R17 Programs could be enhanced if FI's passed along additional information about the account holder of record. On the other hand, some FI's have indicated that their effectiveness in fighting fraud is hampered by IRS or State inability to share fraud or identity theft related information. [46] There is no question about the

[46] ETAAC has not investigated or determined whether the information that might benefit FI efforts to fight fraud is restricted from disclosure pursuant to 26 U.S. Code Section 6103 or some other provision of law or regulation, or if this is more of a resource issue (that is, IRS doesn't have enough staff to analyze and distribute this type of information, even if disclosure to the FI is permissible).

primacy of protecting taxpayer privacy by controlling the use and disclosure of their information. However, any potential barriers in this area should be carefully analyzed to find opportunities that protect taxpayer privacy while also improving fraud prevention (which also adversely affects taxpayers).

What specific FI-provided information do IRS and States believe would enhance the effectiveness of their external leads and R17 programs?

What specific revenue agency information do FI's believe would enhance their fraud prevention efforts?

What laws, regulations or internal practices restrict the disclosure of information by IRS and States to FI's? What is the impact if the information is not personally identifiable, i.e., aggregated or otherwise anonymized?

Another potential barrier raised by FI's relates to their ability to return federal and state refunds without liability to affected customers. It appears that state government agencies may have restrictions on their ability to "indemnify" FI's if, in fact, a refund suspected of being fraudulent and returned to the revenue agency is later determined not to be fraudulent. FI's typically will not return such funds without an indemnity and some states appear to be restricted from providing them. Funds without these protections will eventually escheat (sometimes in error) back to the U.S. or individual state general treasuries without the benefit of knowing they may have been related to fraudulent activity. This is an area that warrants closer examination.

What indemnity restrictions exist at the federal and state level?

Finally, another barrier relates to "third party banks" involved in the refund flow between a revenue agency and the ultimate bank account in which the refund will be deposited. By way of illustration, the refund of a taxpayer that uses certain refund settlement products will pass through two bank accounts – first, a temporary bank account created by the bank offering the refund settlement product (the "first party bank") and, second, the ultimate bank account of another bank (the "third party bank") to which the refund (net of fees for the preparer) is transmitted by the first party bank. At this time, the R17 Program is designed to reject suspicious refunds where the funds are originating directly from a government agency, such as Treasury. However, in the case of a third party bank, the refund is originating from the first party bank not the government. As a result, third party banks cannot currently participate in the R17 Program.

Are there opportunities to work with oversight bodies, such as NACHA,[47] to find ways for third party banks to participate in R17?[48]

[47] The National Automated Clearing House Association develops operating rules and business practices for the nationwide network of automated clearing houses (ACHs) and other areas of electronic payments.

[48] In some cases, the "fix" may be in program design or back end programming. For example, a refund received by a third party bank may have already had certain fees deducted. R17 is a reject of the full refund by the first party bank. If they desire to enable third party banks in R17 type programs, IRS and

ETAAC is not suggesting that the above three barriers are the most important for Security Summit to address. FSWG should undertake to identify the most impactful barriers warranting further evaluation, whether these or others.

2: Remove or mitigate barriers to increased FI participation or effectiveness. Once it identifies the most impactful barriers, FSWG should evaluate opportunities to remove or mitigate those barriers. Those "fixes" may require legislative or regulation changes in some cases but, in other cases, there may be an easier "workaround" to mitigate the problem.

IMPROVE TAXPAYER OUTREACH

BACKGROUND

The Security Summit's "Taxes. Security. Together." awareness campaign has demonstrated the effectiveness of dialogue, information exchange and collaboration with external stakeholders to aid in the reduction of IDTTRF.

ETAAC commends the IRS and its Summit partners for launching this public campaign to increase awareness about the need for computer security, and to ensure taxpayers have the information they need to protect themselves from cyberattacks and safeguard their personal information. ETAAC further commends the work of the Taxpayer Communications Work Group and encourages it to take more steps to broaden taxpayer communication and outreach to diverse communities, employers and community-based organizations.

RECOMMENDATION #14: The IRS should expand outreach and communication to diverse communities and advance its campaign to taxpayers set forth in IRS Publication 4524, Security Awareness for Taxpayers, to community-based consumer organizations by:

- Partnering with organizations experienced in creating pro-security consumer education content for diverse communities.
- Ensuring that its consumer education content and distribution efforts give special focus to reaching diverse communities by collaborating with affinity groups serving populations targeted by scams such immigrants, senior citizens and people with disabilities.
- Collaborating with volunteer tax preparers (VITA and TCE programs), community-based consumer organizations, and local government agencies to disseminate security-focused consumer education materials that meets local needs.

RECOMMENDATION #15: Working through the Security Summit, the IRS should expand the "Taxes. Security. Together." awareness campaign to provide more outreach and key security messaging through employers and small businesses.

States must change their internal policies to accept the "reject" of a partial refund by a third party bank (as well as have the staff to track and manage account adjustments).

RECOMMENDATION #16: To facilitate information exchange with stakeholders regarding IDTTRF, the IRS should establish and support an internal community of practice (COP) for IRS employees serving in a relationship management role. The IRS Office of Communication and Liaison should house the COP and establish platforms for peer communication and learning opportunities.

Recommendations #14, #15 and #16 Supporting Details

IDTTRF is a risk to all taxpayers and IRS external stakeholders, particularly those in diverse communities where English may not be the primary language and to small businesses. Moreover, those taxpayers and stakeholders most at risk are often the ones hardest to reach through traditional IRS communication channels. This communications challenge is compounded by the increasing segmentation of media and communication channels coupled with an increasing trend for consumers to rely on trusted individuals within their social networks. For these reasons, messages must be tailored to specific audiences, and be transmitted through trusted community partners.

ETAAC agrees with IRS' past and current efforts to provide key messaging for taxpayers. However, given the prevalence of IDTTRF scams targeting immigrants, senior citizens, small business, employers and people with disabilities, the IRS must also work with the organizations that serve and communicate with these populations for the Taxes, Security, Together campaign to be effective.

There are also opportunities for the IRS to work with Volunteer Income Tax Assistance (VITA) programs, community-based consumer organizations, local chambers of commerce and local government agencies to disseminate security-focused consumer education materials to deliver outreach to communities in their primary languages in actionable, understandable ways that help consumers reduce their risk of IDTTRF, including through employers and small business.

At the same time, IDTTRF represents an enterprise-wide challenge that requires the IRS to exchange information across the agency quickly and create dialogue with a more diverse set of stakeholders. The development of a COP can help build the IRS' human resource capacities to engage new stakeholders and communicate more effectively in the new media environment. The COP could broaden the reach and effectiveness of the current summit communication strategy by reaching stakeholders not previously engaged through the summit.

IRS Communication and Liaison should be able to cost effectively manage and support the COP and stakeholder-focused collaboration using the peer communications and learning opportunities technology currently in use. While relationship management is broader in scope than IDTTRF, the COP creates a staff infrastructure that allows a nimble and effective response to emerging threats throughout the tax ecosystem. The effectiveness of the COP will rely on the IRS having adequate funding to maintain modern, secure, and more resilient IT architecture, a priority listed in the President's Executive Order on Cybersecurity.

IMPROVE TAX PROFESSIONAL OUTREACH, EDUCATION & COMMUNICATIONS

BACKGROUND: OUTREACH

Tax professionals – including return preparers and electronic return originators (EROs) – are key elements in the e-file system and need both up to date information and education about security threats

Almost 60% of individual taxpayers currently engage a paid preparer to prepare their federal income tax return for them.[49] In turn, more than 90% of these returns were e-filed in 2016, making the integrity of the e-filing process a matter of the utmost importance to every participant in the tax system: taxpayers, tax return preparers, and the IRS.

Current Security Summit efforts have identified issues but more can be done

The Tax Professional and Communication work groups of the Security Summit have worked to deliver messaging to both taxpayers and preparers, launching a "Taxes. Security. Together" campaign to increase awareness among both consumers and tax professionals about the need for computer security and provide tips on how to protect their personal information. The work groups have collaborated with the IRS Criminal Investigation Division on preparing content for presentation at the Nationwide Tax Forums to highlight the increasing threats for tax professionals and how to better protect themselves. Additionally, the IRS Communications staff has delivered a series of press releases focusing on numerous security issues designed to limit identity theft during the tax season.

These IRS actions served to alert tax professionals to the need for data protection. That effort should be supplemented with efforts to provide information about minimum security standards and how best to secure confidential data.

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 ERO's on the cyber and physical security risks facing them;
- Provide a clear and full statement of the security regulations, standards and requirements applicable to a tax professional's participation in IRS e-file, and the potential consequences of failing to comply;
- Provide simple, clear and actionable guidance on how to implement a security program, preferably consolidated into a single source publication; and,
- Review, update and improve such content on a regular basis.

Recommendation #17 Supporting Details

[49] Internal Revenue Service Filing Season Statistics for 2016 available at https://www.irs.gov/uac/newsroom/filing-season-statistics-for-the-week-ending-december-30-2016

Many tax return preparers and EROs lack the expertise to adequately secure data and protect their infrastructure. Despite being responsible for highly confidential personally identifiable information, many tax preparers are not technology experts and need additional clarity. IRS Publications do not provide understandable, actionable guidance.

IRS Publication 1345 states that, "While all Providers must be on the lookout for fraud and abuse in IRS e-file, EROs must be particularly diligent while acting in their capacity as the first contact with taxpayers filing a return."[50] It does not provide any information on what to do to prevent its systems from being vulnerable to the theft of taxpayer data.

Similarly, IRS Publication 3112 states that, "Providers must have security systems in place to prevent unauthorized access by third parties to taxpayer accounts and personal information" and includes a reference to the Gramm-Leach-Bliley Act (GLB), codified at 15 U.S.C. §§ 6801-6827.[51] It is unclear what sanctions, if any, are in place and what having security systems in place means in the context of being an ERO. EROs are governed by IRS publications and regulations (e.g., IRS Publication 1345) as e-file providers, which subjects them to potential sanctions for compliance failures including being barred as an e-file provider. Enforceable standards would create clarity for EROs regarding their existing obligations and what they should be expected to show to demonstrate they are meeting those obligations.

IRS Publication 4557, Safeguarding Taxpayer Data, does provide valuable information in this area but it, too, does not provide sufficient guidance or actionable information. For example, Publication 4557 refers to Publication 1345 and the latter publication's six mandated security standards for EROs. If such standards are applicable to tax return preparers due to the provisions of GLB, it is highly unlikely the vast majority of preparers could understand them. One standard mentioned in Publications 1345, for example, requires that an ERO "possess a valid and current Extended Validation Secure Socket Layer (SSL) certificate using SSL 3.0 / TLS 1.0 or later and minimum 1024-bil RSA/128-bit AES." EROs and tax return preparers are confused by descriptions such as these.

While many steps have been taken by the IRS to increase awareness of security requirements, there remains an absence of a clear message about minimum standards for and actionable steps that should be taken by tax professionals. By leveraging industry expertise and adapting existing materials (e.g. FTC guidance, IRS documentation, Security Summit communications and Publication 4557[52]), IRS could develop more useful publications with clear statements of applicable standards and implementation content and tools that would be invaluable to tax professionals.

[50] IRS Publication 1345, p. 11

[51] IRS Publication 3112, p. 18

[52] IRS Publication 4557 Safeguarding Taxpayer Data, A Guide for Your Business, (2016) Washington, DC: IRS https://www.irs.gov/pub/irs-pdf/p4557.pdf pp. 7-13

BACKGROUND: EDUCATION

The IRS Should Require Security Training for Tax Professionals

Security Summit participants have developed valuable information about internet security, data protection, and the myriad ways that thieves try to steal taxpayer data. Tax return preparers can benefit from taking annual education courses in this area, including insights developed by the Summit. In addition, tax return preparers should be expected to have competence in the secure storage and handling of the confidential information provided to them by taxpayers.

RECOMMENDATION #18: The IRS should take steps to make tax return preparers more aware that educational courses about internet and data security will qualify for IRS-recognized continuing education credits, assuming the course meets IRS standards for such education.

RECOMMENDATION #19: The IRS should amend Circular No. 230 "Regulations Governing Practice before the Internal Revenue Service" to make knowledge about, and implementation of, internet security and the protection of taxpayer data a requirement for all preparers subject to the rules of practice contained in the Circular.

Recommendation #18 and #19 Supporting Details

Many tax return professionals are required to obtain annual continuing education as a condition of maintaining an active credential as an attorney, Certified Public Accountant or Enrolled Agent. The IRS also requires participants in its Annual Filing Season Program to obtain continuing education.

We commend the IRS Return Preparer Office for its recognition that education in safeguarding taxpayer data is an important focus for tax professionals. The Office announced, in January 2017, that identity theft and data security programs focused on enhancing tax professional awareness of protecting client data may qualify for continuing education credit. However, this announcement was posted only on the IRS website, on a page that is difficult to locate, and did not receive any further publicity by the agency, which resulted in few preparers knowing about this announcement.

We note that the IRS does not currently have the legislative authority to regulate tax return preparers with respect to their tax return preparation activity. However, since any preparer who files more than ten returns is generally required to e-file such returns, knowledge about identity theft and data security is of vital importance. Even with respect to tax professionals that IRS may currently regulate because they "practice" before the agency, existing regulations establishing the standard of care that tax practitioners must meet when advising on and preparing tax returns do not require any particular competence with respect to internet security.

Specifically, Treasury Circular 230,[53] which contains the regulations governing practice before the IRS, does not contain any provision requiring a tax

[53] Treasury Department Circular No. 230 (Rev. 6-2014).

professional subject to its terms to have any particular competence or knowledge with respect to the protection of taxpayer data. For example, §10.35 of the Circular states that, "Competent practice requires the appropriate level of knowledge, skill, thoroughness, and preparation necessary for the matter for which the practitioner is engaged," but does not otherwise refer to any competence with respect to the ability to competently maintain the confidentiality of taxpayer information. Furthermore, §§10.50-52 of the Circular, which collectively provide the sanctions that may be imposed on a preparer for and list the types of incompetent or disreputable conduct that may be sanctioned do not address data security.

BACKGROUND: COMMUNICATIONS

IRS Security Alerts require immediate attention

The IRS and its Security Summit partners have spent considerable time and effort to identify evolving scams, phishing emails and other attempts to steal taxpayer data. ETAAC commends this effort, especially IRS' issuance of numerous emails and press releases designed to provide early warning to tax professionals and EROs about these threats. However, when these warnings are commingled with other IRS communications without differentiation, there is currently no quick or easy way to separate the messages that warrant immediate attention from messages that may be opened as time allows.

Expand social media channels

In 2016, as part of the IRS Security Summit, the IRS launched a campaign aimed at increasing awareness among tax professionals called "Protect Your Clients; Protect Yourself."[54] This was a follow-up effort to the "Taxes. Security. Together." public awareness campaign for taxpayers.

This campaign was a significant step forward in providing fact sheets and tips on security, scams and identity theft prevention measures aimed at tax professionals and steps they can take to protect client data and their businesses.

ETAAC applauds the IRS and the Security Summit for these efforts and recommends they be more widely available.

RECOMMENDATION #20: IRS security alerts to tax professionals should be differentiated from other IRS communications (letterhead, font size, color, etc.) to highlight the urgency of the message and recommended actions.

Recommendation #20 Supporting Details

In light of the speed with which stolen information can be used to prepare and file fraudulent returns, it is essential for any information about new scams or cyber threats to be disseminated to and within the tax preparer community as quickly as possible. We commend the IRS for its many communication efforts in this regard. The IRS "Protect Your Clients; Protect Yourself" security awareness program for tax professionals has provided a focus for communications and is a

[54] https://www.irs.gov/individuals/protect-your-clients-protect-yourself

convenient repository for security-related alerts, news releases, fact sheets, and other pertinent information on the IRS website at https://www.irs.gov/individuals/protect-your-clients-protect-yourself.

However, tax return preparers have complained that all IRS communications have the same "look" whether promulgating urgent security alerts that need immediate attention or issuing other routine communications such as tax tips, filing reminders or interest rates.

RECOMMENDATION #21: The IRS should expand and enhance its current use of social media channels to more broadly and consistently communicate the "Protect Your Clients; Protect Yourself" campaign aimed at increasing security awareness among tax professionals.

Recommendation #21 Supporting Details

Tax professionals, like many others, have multiple channels for information relevant to their practice. While the IRS has gone to great lengths to utilize many communication channels such as Facebook, Twitter, YouTube and Tumblr, there may be opportunities to better leverage these channels to provide information about the protection of client information and communicating the important role tax professionals play in the protection of taxpayer data against cybercriminals.

For example, the IRS has several Facebook pages, but they do not contain the same important and consistent messaging provided at IRS.gov on security matters. The IRS could establish a mirror site on Facebook page or update existing Facebook sites with a link to IRS.gov so the information becomes more readily available to tax professionals. This linkage would also provide the added benefit of providing consistent messaging already available on IRS.gov.

INCREASE ELECTRONIC FILING

BACKGROUND

The IRS Modernized *e-file* System (MeF) is well established as the primary system for the receipt and processing of income tax returns filed with the IRS and the States. The IRS receives over 135 million Form 1040 individual tax returns annually, of which about 120 million are received and processed by the MeF. Taxpayers and the IRS are benefited by continued efforts to increase electronic filing.

RECOMMENDATION #22: The IRS should implement the ability for taxpayers to electronically file an amended return (Form 1040X, Amended U.S Individual Income Tax Return) through the IRS Modernized e-file (MeF) System.

Recommendation #22 Supporting Details

The IRS annually receives almost 4 million amended tax returns on IRS Form 1040X. Currently, MeF is not designed to receive Form 1040X, and all amended returns are filed by taxpayers on paper.

ETAAC has recommended in the past that the IRS continue to work toward the completion of MeF for all form types, including the remaining ancillary forms for

the 1040 family, including the Form 1040X. ETAAC realizes that implementing 1040X would require resources and funding to implement. However, we believe that the addition of Form 1040X to MeF would provide several key opportunities.

First, implementing Form 1040X into MeF avoids the need for taxpayers, tax professionals and the IRS to rely on paper and manual processes to correct mistakes on previously filed tax returns.

Second, adding Form 1040X to MeF would help the IRS achieve its Congressionally-mandated target of achieving 80% electronic filing rates for all major forms of tax returns.

Third, many states have already moved forward in developing an electronic process for the 1040X. If the IRS implemented this capability in MeF, there would be a consistent transmission channel of amended returns for both federal and state amended returns. That would provide a more seamless experience for taxpayers and create a lesser burden on the IRS and state revenue agencies.

Finally, Form 1040X could become a platform for criminals engaged in IDTTRF in the future. Implementing Form 1040X in MeF would ensure the IRS receives more attributes associated with the tax return.

In summary, adding Form 1040X would enable a seamless experience for taxpayers and tax professionals filing Federal and State returns, and would reduce burden on the IRS. We strongly encourage the IRS to prioritize the electronic filing of this form, and collaborate with the States in its implementation.

APPENDIX A

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 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.

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.

Jacob Dubreuil - Mr. Dubreuil is a Consulting Manager for Revenue Solutions, Inc. Mr. Dubreuil has worked with several tax and revenue agencies over the last 10 years in implementing modernized Integrated Tax Systems (ITS), Modernized E-file (MeF), non-filer compliance campaigns, refund fraud detection and streamlining processes for efficiency. For the last 7 years, Mr. Dubreuil has provided technical analyst support to

the Federation of Tax Administrators E-Standards Group under contract with the FTA. This group is responsible for guiding States on the MeF platform using best practices and schema standards set forth by the States, IRS and Industry.

Thomas Lorek - Mr. Lorek is the Deputy Chief Information Officer at the Indiana Department of Revenue. Mr. Lorek, in his ninth year with the Department, is responsible for the day to day operations of the IT department covering application development, production support, and data warehousing. He was the solution architect for the Department's individual income tax fraud program, which launched in 2014, and has to date stopped over $100 million in fraudulent refund requests from being distributed. He holds a Bachelor of Science degree from Loras College in Dubuque, IA, and an MBA from Anderson University in Anderson, IN.

Julie Magee - Ms. Magee was appointed Alabama Revenue Commissioner by Gov. Robert Bentley in January 2011, overseeing the collection of $9.8 billion in revenue annually. During her tenure as Commissioner, Magee has had the distinction of serving in leadership roles in the Federation of Tax Administrators, the Multistate Tax Commission, and the Southeastern Association of Tax Administrators. Magee's service to taxpayers and the business community also includes her work with several significant commissions, task forces, and advisory councils, and she provided expert testimony to the U.S. House Judiciary Committee's Subcommittee on Regulatory Reform, Commercial and Antitrust Law in June 2015. She is also an active participant on the Authentication and the Financial Services workgroups that are part of the IRS Security Summit, working with the IRS and industry partners to prevent ID theft and tax fraud. As head of the Department of Revenue, Magee serves on the Governor’s Emergency Relief Fund, helping families and individuals across the state recover from devastating storms. Prior to her appointment as revenue commissioner, Magee was vice president of the Mobile-based InsTrust Insurance Group. Her 20-year career in the business community focused largely on competitive sales and market expansion in the insurance industry.

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 Volunteer and Consultant with the Center for Enterprise Development (CFED). He is also Senior Fellow at the Center for Social Development at

Washington University in St. Louis. 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 policy development and public private partnerships, and as acting general counsel for the company. 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.

Deborah Sawyer - Ms. Sawyer's background includes 15 years in the banking industry as a Personal Trust Administrator, and 19 years as a Tax Advisor for H&R Block. She currently runs two businesses which include Your Tech Girl, which specializes in computer repair and security, and Your Tax Girl, a tax preparation service.

Joseph Sica - Mr. Sica, Chief Public Policy Officer for Green Dot/Tax Products Group, has been affiliated with tax time financial products and combating fraud in the tax system for the last 28 years. In the earliest days of e-filing, Mr. Sica worked with the IRS to develop and pilot refund loans as an incentive for people to file electronically. Prior to IRS having increased fraud detection capabilities, he started the Fraud Service Bureau in 1994 in which banks in the tax loan industry electronically exchanged data to identify fraud and shared results with the IRS. Years ago, Mr. Sica changed his primary focus in the tax industry from technology to related policy affairs and assisted in coordination of dialog between the industry and the IRS. As such, he is a co-founding board member and past chair of the Council for Electronic Revenue Communications Advancement (CERCA). Mr. Sica is also a co-founder member and past vice-chair of the American Coalition for Taxpayer Rights (ACTR), a tax industry policy group seeking to preserve taxpayer choices. Recently, he has worked with industry, state revenue departments and the IRS in connection with establishing the IRS Security Summit taking co-lead roles in the Information Sharing and the Financial Services work groups. Mr. Sica completed Executive Development work at The Wharton School in 1996.

Mark Steber - Mr. Steber, Chief Tax Officer with Jackson Hewitt Tax Service, is responsible for several key initiatives to support overall tax service delivery and quality assurance. Mr. Steber serves as a Jackson Hewitt liaison with the Internal Revenue Service, States, other government authorities, Walmart, other retail entities, and banking partners. With over 30 years of tax experience, Mr. Steber is widely referenced as an expert on consumer income tax issues and especially electronic tax and data

protection issues. Mr. Steber has been an active participant in the IRS Security Summit Initiative since the founding of the effort in early 2015. He has been involved with all the work groups including the Information Sharing Group, Authentication Work Group and Strategic Threat Assessment and Response (STARS) group and subsequent new groups including the Tax Pro Subgroup of the Security Summit. Mr. Steber is active with various industry groups, including ACTR and CERCA, and has worked directly with leadership members in many instances. In prior years, he served on the IRS Electronic Tax Administration Advisory Committee and was Chairman in 2012.

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, Atilla contributes as an architect of policy and technology for the electronic tax industry. He has been and is an active participant in the current Security Summit process and is an active member of CERCA, FS-ISAC, NACTP, OASIS, and other industry and government committees. He served as a director of CERCA, and a charter member of the Executive Committee of the Free File Alliance, Inc. Atilla, 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 B

EFI ANALYTICAL METHODOLOGY

This Appendix explains ETAAC's methodology for analyzing and projecting the Electronic Filing Index (EFI).

THE ELECTRONIC FILING INDEX

ETAAC has used several measures over the years to report and measure the electronic filing (e-file) rate.

To create a consistent measure of this goal, standardize cross-year comparisons, and facilitate analysis, ETAAC developed the electronic filing index (referred to as EFI, or Index) for use in its annual report to Congress. The Index aggregates and assesses the electronic filing rates of a defined set of major tax returns and includes a methodology for projecting e-file rates based on season-to-date information about the main driver of electronic filing rates – the individual tax return.

The Index computes a specific electronic filing rate for each specified return family, as well as an overall composite rate representing the overall electronic filing rate for all major return families in the Index.

Importantly, because certain information in IRS Publication 6186 (which is revised and published each fall) is estimated, ETAAC's Index may shift slightly from year to year as IRS updates its estimates with actual filing season results. In addition, this past season presented several scenarios that bring to question the overall assumptions pertaining to volume projections made prior to a particular filing season. This may result in unforeseen errors in these projections.

RETURN FAMILIES

The Index is computed using IRS Publication 6186's reported information for designated forms in six major return families:

Individual Income Tax
Forms 1040, 1040-A, and 1040-EZ

Employment Returns
Forms 940 and 940-PR, Forms 941 and 941-PR/SS

Corporation Income Tax
Forms 1120 and 1120-A Form 1120-S

Fiduciary
Form 1041

Exempt Organizations
Form 990-EZ
Form 990

Partnership
Forms 1065/1065-B

Substantiation for the continued use and accuracy of the EFI methodology can be seen in results from the 2016 filing season. ETAAC's June 2016 report projected an e-file rate of 86.6% for the 2016 filing season for individual returns (Forms 1040, 1040-A, and 1040-EZ), and an EFI of 78.0% for all major returns. Based on IRS data for the 2016 filing season, published in December 2016, the actual e-file rate for individual returns was 87.3%, and the e-file rate for all major returns was 78.8%. Given the accuracy of the EFI methodology in projecting EFI rates, this 2017 ETAAC report uses the same projection methodology.

However, in future years ETAAC will continue to evaluate the EFI considering factors elaborated in this report and within the tax ecosystem which may impact the accuracy of the projections.

Table 3: 2016 EFI Projection vs IRS Data

	2016 EFI Projection vs. IRS Estimates		
	EFI Projected	Estimated	Variance
Individual (Forms 1040, 1040-A, and 1040-EZ)	86.6%	87.3%	.7%
Business (94x, 1120, 1065, 1041, 990 families)	49.4%	50.3%	.9%
All Major Returns	78.0%	78.8%	.8%

ESTIMATING THE ELECTRONIC FILING RATE

As noted above, the current-year filing season data contained in IRS Publication 6186 is estimated. ETAAC has relied on these estimates to project an EFI for the current year. ETAAC has modeled a projection methodology to forecast the current-year Index based on two components.

Component 1: Individual returns (Form 1040 series)

ETAAC projects total filing season e-file rates for individual returns by extrapolating current filing season year-to-date information into full-year estimates, based on how the individual return e-file rate has historically trended in the May-October period.

Based on this methodology, ETAAC estimates that the e-file rate for individual returns will be approximately 86.5% for the entire 2017 filing season, translating to an overall Index of 80% for all major return types for the 2017 filing season.

ETAAC follows a four-step process to project the full-year electronic filing rate for individual returns.

Step 1: Estimate the 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 May 5, 2017.

Table 4: 2017 Individual Income Tax Returns Actual through May 5, 2017

Cumulative statistics comparing 05/06/2016 and 05/05/2017			
	2016	**2017**	**% Change**
Total Receipts	139,620,000	138,945,000	-0.5%
E-file Receipts	123,401,000	123,239,000	-0.1%
E-file Rate	88.4%	**88.7%**	0.3%

Source: From "Filing Season Statistics for Week Ending May 5, 2017" published by IRS at https://www.irs.gov/uac/newsroom/filing-season-statistics-for-week-ending-may-5-2017

Step 2: Estimate the historical e-file degradation rate through the remainder of the year. This is accomplished by comparing the e-file rate for the first four months of the year through early May (primary filing season) with the actual e-file rate for the full-calendar-year filing season for 2015 and 2016. Then, ETAAC uses the average degradation rate experienced over the past two years to forecast degradation for the current year. Using this approach, the e-file degradation rate for the 2017 filing year is forecast to be 2.1%. ETAAC will continue to monitor the degradation rate to note whether it has any significant year-to-year changes.

Table 5: Historical Partial-Season Data vs. Full-Season Data

	5/8/2015	**12/30/2015**	**Change**	**5/6/2016**	**12/30/2016**	**Change**	**Two Yr Avg.**
Total Receipts	137,312,000	150,991,000		139,620,000	152,544,000		
E-file Receipts	120,253,000	128,784,000		123,401,000	131,851,000		
E-file Rate	87.6%	85.3%	-2.2%	88.4%	86.4%	-1.9%	2.1%

Source: From "Filing Season Statistics for Week Ending Dec. 30, 2016" published by IRS at https://www.irs.gov/uac/newsroom/filing-season-statistics-for-the-week-ending-december-30-2016 and "Filing Season Statistics for Week Ending May 6, 2016" published by IRS at https://www.irs.gov/uac/newsroom/filing-season-statistics-for-week-ending-may-6-2016

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 the May 2017, cutoff, the projected full-year e-file rate for the individual tax return family is 86.58%.

Table 6: Individual Electronic Filing Rate Projection

Current E-file Rate (Through 05/08/2017)	Current	Projection Rate	2017 Projection
Total Receipts	138,945,000		
E-file Receipts	123,239,000		
E-file Rate	**88.70%**	-2.12%	**86.58%**

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

This page left intentionally blank