October 25, 2017

The Honorable John Koskinen  
Commissioner, Internal Revenue Service  
1111 Constitution Avenue, NW  
Washington, D.C. 20224

RE: Changes to the IRS Income Verification Express Service (IVES)

Dear Commissioner Koskinen:

I write on behalf of the members of the Consumer Data Industry Association (“CDIA”) to respectfully request a delay of the October 29, 2017 implementation date of proposed changes to accessing the IRS Income Verification Express Service (“IVES”). Our request for a delay now is for the same reasons for the delay we expressed in our attached communication to the IRS in October 2016. Beyond our baseline concerns with the multifactor authentication (“MFA”) protocol the IRS is proposing; our members are also concerned that the IRS has not provided sufficient time for user-acceptance testing. We urge the IRS to continue a dialogue with industry to determine a path forward that will both protect taxpayer data and ensure a robust system for the secure delivery of vital tax transcript data into the mortgage lending market.

The attached concerns, developed in 2016, still apply today. Our concerns with the MFA protocol remain and we want to emphasize that it is vital that businesses should not be required to use personal mobile devices to manage sessions where they retrieve tax transcripts resulting from the submission of 4506-T forms. The personal mobile device requirement is in direct conflict with accepted data security management best practices for B2B, B2C and B2G data centers.

Personal mobile devices are not under the control of corporate information security programs. These devices cannot be subjected ongoing and point-in-time audits by the company. The devices can and will be used outside of work and in ways that can pose extreme threats via the implantation of malware/malicious code and other cybersecurity risks that are all too common and for which the company cannot audit.
Personal mobile devices cannot be shut down remotely by the company if they are stolen or lost. Personal devices can be used by multiple people in a single family, including less than responsible parties. Ultimately, what may be appropriate for individual taxpayer transcript requests is not a scaled and not an appropriate B2G MFA solution. In fact, what the IRS is proposing is a fundamental security threat.

Beyond the risks associated with the MFA protocol, our concerns are also focused on ensuring the uninterrupted flow of tax transcripts. Timely tax transcript delivery is vital for the safety and soundness of mortgage underwriting practices in the United States at both the primary and secondary market levels. With the Federal Reserve beginning to shrink its significant balance sheet of mortgage-backed securities, the country’s money supply for lending will turn to a broader range of investors which will expect near-perfect underwriting performance. We need only look back at the Great Recession to know just how important it is to have the right data considered when it comes to mortgage lending. We urge further dialogue between the IRS and industry, rather than forcing the imposition of an MFA protocol designed for point-in-time taxpayer transactions.

This past October 2016 we were pleased when the IRS put on indefinite hold the implementation of the MFA protocol that wasn’t designed for and posed risks related to B2G high-volume 4056t-related transactions. We were grateful for your attendance at an October 26, 2016 meeting where you demonstrated your personal interest in finding the right answer to protect taxpayers, and ensure safe and sound loans. We agree these are both important priorities. At this meeting, you stated that the IRS needed to work with industry to “…most effectively identify who the users are” and “…defeat risk and manage the compliance burden for users.” Debra Holland, the Commissioner of the IRS’s Wage and Investment Division led this meeting. Ms. Holland asked industry for suggestions on alternatives to the “cell phone method” and how long industry would need to implement solutions. We continue to believe that this is the right question on which to focus.

This October 2016 meeting led to the creation of what became known as the IVES Participants Forum. Industry was very encouraged by the creation of the Forum which ensures a fullsone dialogue informs the IRS’s views on effectively securing taxpayer data. Understandably, the Forum did not kick off meetings until later in 2017 after tax filings had been handled. On August 11, 2017, the IRS notified the Forum participants of their intention to hold an August 30, 2017 meeting to discuss the possibility of using PII truncation strategies to mitigate data security risks. CDIA members participated in this meeting. As a follow-up IRS personnel requested written input on PII truncation. Input on the IRS proposal and submission of alternatives were due on September 13, 2017. CDIA submitted a letter which is attached. CDIA members also met with IRS
personnel on September 13, 2017 to discuss their ideas with the goal of continuing to work through options consistent with your statements made during the October 26, 2016 meeting.

Though the IRS indicated their intention to move forward with securing taxpayer PII as early as August 30, 2017 and expressed a continued interest in the MFA protocol previously discussed, our members assumed that discussions of how to secure taxpayer PII would continue via the Forum. In fact, discussions of PII truncation options continued into September, but these were apparently uncoupled from the MFA protocol decision. It was only on October 16, 2017 that our members were formally notified that the MFA protocol would become effective on October 29, 2017. We are now five days away from this date. Though our members' concerns about the current MFA protocol remain, our members are attempting nonetheless to code solutions. However, the test site wasn't available until just this past week and it is incomplete in terms of executing a full user acceptance test, including understanding session limits which may affect production time schedules tied to consumer's mortgage loans and whether multiple concurrent sessions will be permitted. Further, the IRS has not provided a formal requirements document for coding and system design purposes which leaves each of CDIA's members having to make assumptions about how to design a system to download tax transcripts.

For the reasons stated above and those discussed in the attached CDIA communications we urge the IRS to continue dialogue and not implement a program which poses data security risks for taxpayers.

Sincerely,

Eric J. Ellman
Senior Vice President, Public Policy & Legal Affairs

Enclosures
Talking Points Supporting
A Delay in IRS Implementation of IVES Access Changes

Request

The IRS should put on indefinite the planned Oct. 24 date for multi-factor authentication protocol for enterprise level access to tax transcripts. During this interim period the IRS and CDIA members should have a constructive dialogue to allow for tax transcript transmission to businesses with meaningful data security standards.

The Importance of Ensuring Data Security of Personally Identifiable Information

CDIA agrees with the IRS that ensuring the security of personally identifiable information on tax transcripts is a vital priority. CDIA members manage data security through enterprise-level systems with data security experts.

Our members are also subject to a variety of laws, regulations and contractual obligations which inform our thinking in terms of the design of our programs, including the Gramm-Leach-Bliley Act Safeguards Rule, the Sarbanes-Oxley Act’s Information Technology Security, oversight as a third-party vendor per requirements established by the Consumer Financial Protection Bureau (CFPB), and contractual obligations to implement the data security standard established by ISO/IEC 27001.

CDIA members’ data security programs already protect against the risks the IRS is attempting to address through its implementation of a new multi-factor authentication (MFA) standard.

The Importance of Tax Transcripts

The tax transcripts system contributes vitally to meet the needs of American consumers in several critical areas. First and foremost, IVES provides important income data to the mortgage underwriting process. IVES is critical for the quick turnaround to get mortgages approved in a time that consumers expect and demand. Coming out of the Great Recession it was clear that lax underwriting standards, and in particular self-reported income, played a major role in destabilizing loan portfolios. New regulations issued by the CFPB require mortgage lenders to consider a consumer’s ability to pay. Income validation is a key to accomplishing this key underwriting duty. Tax transcripts ensure income is verified and there is no private-sector substitute. Second, IVES plays an important part in the life insurance underwriting process. Third, IVES helps qualify low-income consumers for a number of services, including Lifeline, a
Analysis of the Effects of the IRS Multi-factor authentication (MFA) Proposal

Our members order and retrieve tens of thousands of tax transcripts every single day. The IRS proposes that the single set of user credentials currently issued to CDIA members be tied to a personal mobile device so that a text-delivered code can be sent in order to log into a session. While the IRS has not issued system specifications/details of how this will work if this means that only a single session can be run rather than concurrent sessions and this session is tied to a single user then our testing confirms that no more than an average of a few hundred tax transcripts can be downloaded per day per CDIA member. The mortgage market will freeze up if this is the result which will put a serious drag on GDP performance.

There are less than 14 days until the new MFA protocol is activated. No system specifications have been issued by the IRS which makes planning for system changes almost impossible. It also makes it impossible for us to even consider how technology could be deployed to improve on the estimated maximum standard of a few hundred transcripts per day.

MFA and Mobile Devices - A Serious Security Threat

CDIA is not concerned with the need to deploy an MFA protocol. We are concerned with the choice made which does not align with enterprise-to-enterprise best practices. The IRS MFA protocol is best suited to managing risks when a consumer is accessing records held by the IRS.

Enterprise-level MFA protocols most often employ other strategies such as the use of digital certificates and white-listing IP addresses. US CERT, housed at Carnegie Mellon, is the leading authority on insider threat analyses. In its Common Sense Guide to Mitigating Insider Threats technical paper, US-CERT notes that at the enterprise level, log-in credentials are housed on secured servers. The IRS MFA requirement that personal mobile devices be used appears to make this option impossible and risks increased insider threat risks.

The mobile device strategy also works against best practices in information security by requiring that personal mobile devices be allowed into data centers. CDIA members and their business customers often prohibit mobile devices in data centers. The IRS MFA protocol exposes other consumer data to risks because personal mobile devices
include cameras which can take pictures, the ability to download data surreptitiously, the ability to download malware, the ability to record and the ability to transmit via text and email. NIST makes an illustrative point in its paper, *Guidelines for Managing and Securing Mobile Devices in the Enterprise* (Draft) about the substantial security threats posed by mobile devices to enterprise data systems. These threats come from, among other things, audio and video recording capabilities, Wi-Fi and Bluetooth connectivity, compactness of the device making it easy to hide, built-in features for synchronizing local data with a remote location, storage, and more.

Not only is the IRS’ MFA approach an unacceptable risk for proper data room security management, but it is unfair for individual employees to be required to use a personal device for a corporate purpose (and to have it modified assuming modifications could mitigate the risks outlined above).

**Summary**

For the reasons noted above, the IRS should put on indefinite the planned Oct. 24 date for multi-factor authentication protocol for enterprise level access to tax transcripts. During this interim period the IRS and CDIA members should have a constructive dialogue to allow for tax transcript transmission to businesses with meaningful data security standards.
IRS Form 4506-T: Problems with and Solutions for the Possible Redaction of PII

Problem: As part of its ongoing effort to further protect taxpayer PII, the IRS has proposed a few changes to the transcript responses it provides for 4506-T requests. These changes include:

- Only displaying the first four letters of the taxpayer last name, and no other parts of it. Ex: “John” instead of “Mary A. Johnson”
- Only displaying the street name without street number. Ex: “Main” instead of “1234 Main Street, Anytown, CO 008811”

Need to protect PII in the right way:

CDIA agrees that ensuring the security of personally identifiable information is a vital priority. CDIA members manage data security through enterprise-level systems with data security experts. Yet, we do not believe the IRS’ proposed redaction of PII in the Form 4506-T solves the root of the issue.

The IVES process begins with fax batches being submitted by IVES participant’s containing multiple 4506-T requests. The responses from the IRS are then posted to a web mailbox as HTML transcripts. This necessitates a matching activity for every response. Removing the only elements, we can use to match responses to requests (for final delivery back to clients/lenders) introduces a level of ‘guessing’ into the process that will never be 100% certain, and thus includes an increase in risk that taxpayer PII may be shown to a party that shouldn’t see it (ex: John Smith at 123 Main St with SSN 123-45-6789, and Jane Smith at 456 Main St with SSN 321-54-6789, could potentially look like the same people).
Proposed solutions: We are grateful to the IRS for engaging in a dialogue with CDIA members about our concerns with possible PII redaction in Form 4506-T. We have proposed some preliminary solutions for discussion. Our alternative solutions are:

- Pursue a different method of order submission and fulfilment: Moving away from faxes and web mailboxes to a web service or other systemically “integratable” method would allow for a more secure data flow. There are also significant opportunities for the reduction of errors and turn times when this sort of solution is in place.
- Introduce a new unique ID for every request so that we can use it to definitively link requests to responses.
- Only apply redaction to some of the fields currently proposed: The reason for this is it will allow for certainty in matching responses to requests, thus minimizing the risk of PII being presented to a party that should not see the data.

Consumer Data Industry Association (CDIA)

CDIA members serve a vital role in ensuring that risk management data necessary for mortgage loan underwriting and administration is available to all financial institutions including both the nation’s smallest community banks and credit unions as well as financial institutions operating on a nationwide basis.

CDIA is an international trade association, founded in 1906, of more than 130 corporate members. Its mission is to enable consumers, media, legislators and regulators to understand the benefits of the responsible use of consumer data which creates opportunities for consumers and the economy. CDIA members provide businesses with the data and analytical tools necessary to manage risk. They help ensure fair and safe transactions for consumers, facilitate competition and expand consumers’ access to a market which is innovative and focused on their needs. CDIA member products are used in more than nine billion transactions each year.