



October 11, 2016

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 until June 23, 2017 of proposed changes to accessing the IRS Income Verification Express Service (“IVES”). We also seek an opportunity, during this interim period, to meet with the IRS to discuss alternatives to find a better match between threat levels and the security proposed to meet perceived threats. The IRS’ proposed security changes, with less than 30 days’ notice, is a problem for businesses and consumers alike that rely on fast approval of mortgage and other consumer decisions. We support secure access to IVES, but it has to be done thoughtfully and with enough time to prepare for changes. The IRS proposal before us does not meet either test.

1. Background and existing security protocols

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. As a former non-executive chairman of Freddie Mac you know how important home purchases are to the nation’s economic well-being and to improving the lives of individual consumers.

The planned Oct. 24 compliance date with the IRS' significant changes to access to IVES is too short according to our members, who play a critical part in helping consumers meet their financial and consumer needs. Also, we feel that the proposed security changes are not appropriate for commercial vendors such as our members. We would like to engage in a dialogue with the IRS to find ways to maintain secure IVES access in a way matches the needs of trusted and secure commercial vendors. As you know, significant IVES changes were [implemented recently](#) and more time to adjust is necessary.

The IRS' goal of ensuring downstream data security of citizens' data is laudable. Our members are all financial institutions as defined by the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3) and they are subject to data security standards of the GLBA Safeguards Rule, 16 CFR Part 314. Our members are also often subject to a range of other security standards and oversight including requirements found in the FCRA, Consumer Financial Protection Bureau ("CFPB") examinations focused on larger participants, and Sarbanes-Oxley required audits of company controls where a company is publicly traded on a U.S. exchange. Through contractual requirements and also voluntarily many of our members are compliant with the [ISO/IEC 27001 standard](#). The ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system ("ISMS"). Many of our members are also "service providers" as defined by Sec. 1002(26) of the Dodd-Frank Act, 12 U.S.C. § 5481(26). The CFPB has issued a [bulletin](#) (Bulletin 2012-03) describing their extensive expectations for banks and financial institutions to oversee these providers.

Proper identification of end users both at the corporate and individual levels makes sense. In fact, our members have already implemented robust end-user onboarding and access requirements as a result of the fact that they are defined as consumer reporting agencies under the Fair Credit Reporting Act, 15 U.S.C. §1681 *et seq.*

2. IVES access is critical to American consumers

The Internal Revenue Service's IVES 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. 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 government program offering qualified low-income consumers access to mobile phones. We appreciate the IRS's continued support of IVES. The IRS

changes in IVES access and the short timeframe to make this happen will disrupt consumers who seek speedy mortgage approvals, timely acceptance of a life insurance application, and quick authorization of a Lifeline phone.

3. The proposed changes to IVES access does not offer enough time for businesses

We respectfully request that the IRS delay until June 23, 2017, the proposed changes to accessing IVES. On or about Sept. 24, 2016, the IRS announced the security changes to take effect on Oct. 24. CDIA members are commercial vendors with IVES access. Our members have highly-trained staff to access IVES at many offices across the United States. The changes proposed by the IRS do not allow our members enough time to adequately prepare to meet the demands of the IRS throughout all qualified personnel across all enterprises. A delay of a few more months, with the changes already implemented from this past summer, will not likely pose any new or additional threats to IVES since the recently elevated levels of high security will remain will remain in place during this interim period.

Delaying the implementation of a new security system until after the 2016 tax filing season makes good sense. Making drastic changes now or during the filing season, on such short notice, with no prior testing or IRS customer support, does a disservice to consumers, the government, and businesses alike.

The most recent and already effective changes require participants to take additional measures to credential users and to provide additional information regarding all persons with authorized access to IVES. These systems are enough, coupled with additional security, to neutralize any threat during a delay period. Not only do we respectfully request an implementation delay, but we also want to engage in a constructive and meaningful dialogue with the IRS to find a more finely-tailored solution to meet the needs of securing the IVES access.

4. The proposed changes to IVES is not the best risk-based solution and we would like to engage in a dialogue to search for other possible solutions

During the interim period we propose to June 23, 2017, CDIA and our members would like an opportunity to engage in a dialogue with the IRS to find the best match of IVES security access to the threat level that might be posed to IVES access without additional protections beyond what is already in place.

The proposed security changes demanded by the Oct. 24 compliance date may be incongruous to commercial vendors and their tight security protocols. The IRS proposal is more in line with consumer to business transactions but not government to business transactions. CDIA members conduct a high volume of transactions. A text-message based multi-factor authentication solution would be impractical for CDIA members and the IRS. While the intent and risk reduction of the multifactor authentication requirement is understandable, we want to stand together with the IRS to protect user data and reduce risk of unauthorized data access. Interestingly, NIST has released a special publication that raised questions concerning the effectiveness of SMS-based two factor authentication.¹

Having an entire enterprise dependent on a few personal cell phones creates points of failure. Mobile devices can be lost or stolen and can sometimes be hard to locate when they are lost or stolen. Mobile devices are often tied to individuals and not corporations. Authorized mobile phone users fly on airplanes, go on vacations, and are not always in cell phone range. A number of businesses do not even allow cell phones in certain work sites.

We understand from a recent call between the IRS and some of our members that the IRS has discussed a one-time passcode process which is normally used at a point of sale to authenticate consumers entering into a one-time time transaction. The IRS has announced an exception process of requesting the use of a business cell phone, instead of a personal phone, but that process is by mail and has a five-to-seven-day delay built in. Even with the use of a business cell phone the IRS would require a passcode process every time the IRS mailbox is accessed. For businesses that process large volumes of 4506T requests, a point of sale tool makes little sense.

We also understand that the IRS will not offer any customer service, technical assistance, or a help desk to IVES account holders until Oct. 24. There is no test environment before the system goes live, either. The lack of support or testing from the IRS makes compliance even more challenging by the stated Oct. 24 deadline.

In short, the IRS contemplates security systems that do not fit the risk profile offered by large commercial businesses.

Added breathing room for IVES access changes would allow a dialogue between commercial vendors and the IRS. We strongly support safe and secure IVES access, but we want to find a better match between threat levels and security proposed to meet

¹ DRAFT NIST Special Publication 800-63B, *Digital Authentication Guideline, Authentication and Lifecycle Management*, <https://pages.nist.gov/800-63-3/sp800-63b.html>.

perceived threats. We request that verified, legitimate users with access credentials be offered a chance at a meaningful dialogue. We urge the IRS to meet with safe and sound stakeholders with long-term relationships and a demonstrated willingness to invest to work together to find real answers to real problems.

5. The IVES access changes will impose most harm on consumers seeking quick mortgage approval

The IVES access changes and the short time-frame under which the access changes are to be implemented will most likely slow down the mortgage approval process. This slowdown will most appreciably affect consumers looking to lock in a home and a loan in short order. With limited appreciable security improvement and substantial consumer frustration, the proposed IVES access changes will do more harm than good.

6. Conclusion

We respectfully request a delay until June 23, 2017 of proposed changes to accessing the IVES and request an opportunity to meet with the IRS to discuss alternatives to find a better match between threat levels and security proposed to meet perceived threats. Proposed security changes, with less than 30 days' notice, is a problem for businesses and consumers alike that rely on fast approval of mortgage decisions. We support secure access to IVES, but it has to be done thoughtfully and with enough time to prepare for changes. The IRS proposal before us does not meet either test. We hope to engage constructively, with thought and time, for a security resolution that will work for the IRS, consumers and businesses.

We welcome your assistance in this matter that is critical to consumers, businesses, and the government.

Sincerely,

A handwritten signature in blue ink, appearing to read 'E. Ellman', with a long horizontal flourish extending to the right.

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