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 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
government program offering qualified low-income consumers access to mobile phones.

**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.