American Institute of CPAs
1455 Pennsylvania Avenue, NW
Washington, DC 20004-1081

September 24, 2014

The Honorable John A. Koskinen,
Commissioner
Internal Revenue Service
1111 Constitution Avenue, NW
Washington, DC 20024

RE: IRS Guidance for Electronic Signatures on Form 8879

Dear Commissioner Koskinen:

In March 2014, the Internal Revenue Service (IRS) updated its guidance (see Attachment 1) for taxpayer electronic signatures on certain forms including Form 8878, *IRS E-file Signature Authorization for Form 4868 or Form 2350*, and Form 8879, *IRS E-file Signature Authorization*, and made such guidance available on www.irs.gov. The American Institute of Certified Public Accountants (AICPA) strongly supports the IRS's effort to develop standards allowing for electronic signatures on Form 8879, which would improve the paperless processing of individual tax returns. The ability to have electronic signatures throughout the tax return filing process will reduce compliance and administrative burdens currently facing taxpayers, tax return preparers and the IRS. However, we are concerned that the current electronic signature standards do not adequately address the need for confidentiality of taxpayer information nor do they appropriately accommodate the needs of different taxpayer groups.

Executive Summary

In this letter, we specifically address the standards issued with respect to taxpayer e-signature standards in "remote transactions," i.e., where the taxpayer is not appearing in person before the electronic return originator (ERO) with a valid form of personal identification. The updated guidance states that, with respect to remote transactions, the software being used must record certain data, including the taxpayer's computer Internet Protocol (IP) address, the taxpayer's login information (user name), and the method of identity verification, which includes the "taxpayer's knowledge based authentication passed results and, for in person transactions, confirmation that government picture identification has been verified." The guidance states that the ERO/tax return preparer must provide this information upon request to the IRS.

With respect to remote transactions, the guidance further provides that the ERO/tax return preparer must record the name, social security number, address and date of birth of the taxpayer and "verify that the name, social security number, address, date of birth and other personal information on record are consistent with the information provided through record checks with the applicable agency or institution, or through credit bureaus or similar databases."

It appears that a key underpinning of the updated guidance is the IRS determination, as articulated in the IRS Electronic Signature Guidance for Forms 8878 and 8879, that "the identity verification requirements must be in accordance with National Institute of Standards and Technology, Special Publication 800-63, Electronic Authentication Guideline, Level 2 assurance level and knowledge based authentication or higher assurance level."

Level 2 assurance includes dynamic knowledge-based authentication, which involves the process of verifying identity through record checks with credit bureaus or similar databases. Dynamic knowledge-based authentication uses basic identification factors about an individual (e.g., name, address, date of birth, social security number) to generate questions in real-time from public data records or the credit report corresponding to the individual identification factors provided. In this process, the individual is presented with a set of questions about their personal information drawn from public records or a credit report (e.g., the amount of the person's current monthly mortgage payment, a former address, a car that was owned in the past) and must choose the correct answer from the choices presented. For this type of authentication to occur in the tax preparation environment, the tax software vendor or ERO/tax return preparer generally needs to send taxpayer data to an identity verification vendor before the taxpayer is permitted to electronically sign the return.

AICPA Recommendation

We are writing to request that the IRS clarify that alternative methods of identity verification with respect to electronic signatures provided via remote transactions are permissible. The current requirement that the ERO/tax return preparer must authenticate the taxpayer's identify "consistent with the information provided through record checks with the applicable agency or institution, or through credit bureaus or similar databases" could be interpreted to mean that dynamic knowledge-based authentication is required in all cases of remote transactions. This interpretation appears supported by the section of the updated guidance that states that the software must record the positive results of the taxpayer's knowledge based authentication. The updated guidance also suggests that Level 2 "or higher assurance level" is adequate.

This requirement for dynamic knowledge-based authentication in cases of remote transactions is problematic for three reasons. First, introducing a third-party (the identity verification vendor) into the signing and e-filing process increases the risk of data privacy issues arising from the process. Second, the dynamic knowledge-based authentication process itself can compromise the trusted advisor relationship that CPAs have with their clients. Third, dynamic knowledge-based authentication is largely unworkable for the population of taxpayers that stand to most benefit from remote electronic signatures – business travelers, expatriates and children.

Due to these concerns, the AICPA believes that the IRS should work with stakeholders to develop some alternatives to dynamic knowledge-based authentication that would still provide the level of identity verification that is necessary for proper tax administration, while not unnecessarily exposing taxpayer data to new parties, impinging on the CPA-client relationship or excluding certain classes of taxpayers from the ability to remotely provide an electronic signature on Form 8879.

Alternatives for the IRS to consider include:

- Create an exception to the dynamic knowledge-based authentication requirement for Circular 230 Federally Authorized Tax Practitioners because of their unique status and the trusted advisor relationship they have with their clients.[1]
- Consider the taxpayer's identity as authenticated if the tax return preparer has a secure portal for interaction with the taxpayer-client requiring a unique strong password, or shared secret questions through which the client has provided the answer to verify the taxpayer's identity. In this manner, the CPA serves as a trusted third party source that can support the authentication of the client.
- Employ dynamic knowledge-based authentication by drawing only on data within the ERO/tax return preparer's own firewall as opposed to third-party databases, thereby eliminating the need to disclose sensitive data outside of their firewall. Some identification verification vendors offer methods of dynamic knowledge-based authentication that utilize the practitioner's own information systems as the source of the questions used in the authentication process. This method allows identification verification without resorting to the use of third party identity verification vendor, eliminating the need to disclose sensitive taxpayer information to an identity verification vendor and reducing the intrusion on the CPA-client relationship.

Concerns about Dynamic Knowledge-Based Authentication

A. Data Privacy

Since the IRS released the electronic signature guidance, tax software vendors have started to release their products for signing the Form 8879. Because dynamic knowledge-based authentication requires verification with the identity verification vendor, the electronic signature process requires disclosure of sensitive tax return information, including social security numbers, to a third party. It is our understanding that some software vendors, in fact, disclose the entire tax return to the identity verification vendor during the taxpayer's e-signature process, in addition to the information necessary to perform the check. This disclosure of information raises concerns about clients' reasonable expectations with data confidentiality and the risks inherent in transmitting a tax return to a third party. Tax return preparers, who often are EROs, are subject to Internal Revenue Code (IRC) section 7216. To the extent tax return preparers use tax software vendors to handle the actual electronic transmission of tax returns to the IRS, those tax software vendors are also considered tax return preparers under the section 7216 regulations and such disclosures to the vendors are generally considered permissible without client consent. However, if those tax software vendors transmit taxpayer information to an identity verification vendor involved in the authentication process, there is a question of whether such disclosure requires prior client written authorization and consent.[2]

[1] It is not entirely clear whether the updated e-signature guidance currently recognizes the trusted advisor relationship that typically exists between a CPA and his or her client. For example, the guidance in the section titled "In-Person Transaction" states "[i]f there is a multi-year business relationship, you should identify and authenticate the taxpayer."

[2] For similar observations in the context of vendors in the IRS's Income Verification Express Services (IVES) program (related to Form 4056-T), see "The Income Verification Express Services Program Needs Improvements to

B. Client Relationships

Our concerns regarding data privacy and dynamic knowledge-based authentication are heightened by the trusted advisor relationship our members have with their clients. When clients interact with CPAs, they do not expect to have their personal data disclosed to third parties. CPAs provide a range of year-round professional services to their clients and often serve the same clients over the course of many years. Through common client acceptance procedures and ongoing relationships with their clients, our members have already verified the taxpayer's identity. Clients have high expectations that CPAs will treat their information as confidential and with the utmost discretion. Clients also expect a level of ease and convenience present in the CPA-client relationship. Subjecting clients to a series of invasive personal inquiries may raise questions as to why their private data has been disclosed to the identity verification vendor. Similarly, the questions or choices posed during the authentication process may include data that the client may not view as necessary or relevant to the tax return process. The client may worry about how such data was obtained and whether the questions posed are tantamount to electronic "phishing," which occur in identity theft situations. Because there are other less intrusive methods available to verify identity in connection with electronic signatures, we are not in favor of this impingement on the CPA-client relationship, and believe it is imperative that alternative methods of verification are made available.

C. Taxpayers without U.S. Public Records

In order for dynamic knowledge-based authentication to work, the taxpayer must have personal information available in the credit reporting bureaus or public records databases. Some of our members prepare the tax returns of U.S. citizens or resident expatriate employees working for multinational corporations. These taxpayers have filing requirements in the United States, but may have resided abroad and not paid bills or borrowed funds in the U.S. for long periods of time. These individuals often do not have sufficient U.S. public data built up to enable the identity verification vendor to authenticate their identity. The dynamic knowledge-based authentication requirement is not an option for taxpayers in these circumstances. Dynamic knowledge-based authentication limits these taxpayers' availability to take advantage of the immense convenience to electronically sign the Form 8879. Other illustrations of cases in which dynamic knowledge-based authentication are not practical would include children, recent entrants to the workforce such as university or secondary school graduates, immigrants, the elderly, and recently divorced spouses who have limited personal credit history.

* * * * *

The AICPA is the world's largest member association representing the accounting profession with nearly 400,000 members in 128 countries and a history of serving the public interest since 1877. Our members advise clients on federal, state and international tax matters and prepare

---

Better Protect Tax Return Information," Treasury Inspector General for Tax Administration, January 26, 2011, p. 6 ("Taxpayer information is at risk of theft or misuse when taxpayers submit requests for tax return information through third parties … Laws and regulations that protect taxpayer information do not always cover IVES program participants.")

income and other tax returns for millions of Americans. Our members provide services to individuals, not-for-profit organizations, small and medium-sized businesses, as well as America's largest businesses.

We appreciate your attention to this important matter. If you have any questions, please contact me at (304) 522-2553, or jporter@portercpa.com or Melanie Lauridsen, AICPA Technical Tax Manager, at (202) 434-9235, or mlauridsen@aicpa.org.

Sincerely,

Jeffrey A. Porter, CPA
Chair, Tax Executive Committee

Enclosure

cc: Debra Holland, Commissioner, Wage & Investment Division, Internal Revenue Service
Diane Fox, Director, Free File Program, Internal Revenue Service