



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

May 1, 2013

Mr. Steven T. Miller  
Acting Commissioner  
Internal Revenue Service  
1111 Constitution Avenue, NW  
Washington, DC 20024

RE: IRS Announcement 2013-8, *Recommendations for Proposed e-signature Standards*

Dear Mr. Miller:

The American Institute of Certified Public Accountants (AICPA) offers the following comments and recommendations in response to IRS Announcement 2013-8, *Recommendations for Proposed e-signature Standards* ("Announcement 2013-8"). These comments are also being submitted to the e-mail account identified in Announcement 2013-8. We understand that the comment/recommendation period has been extended until May 1, 2013.

The AICPA is the world's largest member association representing the accounting profession with nearly 386,000 members in 128 countries and a 125-year heritage of serving the public interest. Our members advise clients on federal, state and international tax matters and prepare 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 would like to express our sincere appreciation for the willingness of the Internal Revenue Service (IRS) to speak with us during a recent conference call. They graciously listened to our concerns and provided insight into the process and thinking behind the guidance set forth in Announcement 2013-8. The discussion has helped the AICPA leadership and our members who participated in the call better understand the IRS's objectives for the e-signature project.

Before we share our comments and recommendations, we want to commend the efforts of the IRS to more widely authorize the use of electronic signatures ("e-signatures") on tax returns and other documents. We also commend the IRS's efforts to develop a well-reasoned set of e-signature standards. The ability to electronically sign tax returns will reduce compliance and administrative burdens currently facing taxpayers, tax return preparers, and the IRS. We especially welcome the IRS's efforts to authorize the use of e-signatures for Form 8879, IRS *e-file* Signature Authorization. Such a change will streamline the paperless tax return preparation process for all interested parties. However, we remain concerned that the proposed e-signature standards set forth in Announcement 2013-8 may not adequately address concerns inherent in a system that must respect the confidentiality of taxpayer information. We are also concerned that implementing a single standard may fail to appropriately accommodate the needs of different taxpayer groups.

In this letter, we present the following four recommendations: (1) e-signature methods should protect taxpayer information and not interfere with the taxpayer-tax return preparer relationship; (2) e-signature methods should be flexible enough to accommodate the needs of a variety of taxpayers and tax preparation firms; (3) additional e-signature pilot programs are needed to better assess the appropriateness of different e-signature methods; and (4) proposed IRS e-signature guidelines should be published for public comment prior to adoption as final rules.

## **Background**

Announcement 2013-8 articulates the following five core signing requirements for the use of e-signatures:

1. A person (*i.e.*, the signer) must use an acceptable electronic form of signature;
2. The electronic form of signature must be executed or adopted by a person with the intent to sign the electronic record (*e.g.*, to indicate a person's approval of the information contained in the electronic record);
3. The electronic form of signature must be attached to or associated with the electronic record being signed;
4. There must be a means to identify and authenticate a particular person as the signer; and
5. There must be a means to preserve the integrity of the signed record.

These above requirements (*i.e.*, form, intent, association of signature and record, authentication of the signer, and integrity of the record) together form a sound signing process, and mirror the e-signature requirements discussed in detail in a joint 2013 report (the "Report") issued by the General Services Administration (GSA) and the Federal Chief Information Officers (CIO) Council at the request of the Office of Management and Budget.<sup>1</sup>

The Report asserts that e-signature requirements should be "technology neutral" and neither require nor presuppose that a particular type of technology be applied to the signing of electronic records.<sup>2</sup> Importantly, the requirements lack a mandate for a "one-size-fits all" approach.

We believe that the five core signing requirements represent a flexible framework under which the IRS can implement the use of e-signatures on tax returns and other forms. As discussed further in our specific recommendations below, the AICPA encourages the IRS to build flexibility into the e-signature standards it ultimately adopts. We understand that the IRS has piloted e-signatures on Form 4506-T, Request for Transcript of Tax Return, and Form 8655, Reporting Agent Authorization, and we understand the IRS is also piloting e-signatures on Form 8879, IRS *e-file* Signature Authorization. These pilot programs have used signature methods such as a personal identification number (PIN), click-through, tablet personal computers, a digital signature, and the electronic signature pad.

---

<sup>1</sup> See *Use of Electronic Signatures in Federal Organization Transactions*, Version 1.0 (January 25, 2013). For additional information, see Government Paperwork Elimination Act (GPEA) and the Electronic Signatures in Global and National Commerce Act (E-SIGN).

<sup>2</sup> The actual e-signature processes that must be put in place are detailed in the National Institute of Standards and Technology (NIST) Special Publication 800-63-1.

In Announcement 2013-8, the IRS stated its intent to “implement consistent standards for IRS partners and external stakeholders.” The AICPA agrees that consistency is a worthy objective; however, we request that the IRS exercise caution in implementing e-signing standards. Should e-signature standards be drafted too narrowly in the interest of consistency, such standards may hamper the widespread adoption of e-signatures on IRS documents, should taxpayers and tax return preparers find such standards impracticable or too burdensome. Our four recommendations below address these concerns.

### **Recommendations**

#### **(1) E-signature methods should protect taxpayer information and not interfere with the taxpayer-tax return preparer relationship.**

Announcement 2013-8 generally provides that there must be a means of authenticating the identity of the individual signing the electronic record. We understand that the Form 8879 e-signature pilot program, which is currently underway, involves the use of a dynamic knowledge-based means of authentication. 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 question about their personal information drawn from public records or a credit report (e.g., a former address, a car that was owned in the past) and must choose the correct answer from the choices presented. The aim is to require the individual to respond to personal information within the individual’s specific knowledge and not information that could be otherwise accessed (for example, through the individual’s personal effects, such as a wallet). For this reason, this protocol is sometimes referred to as “out of the wallet” authentication. For this type of authentication to occur in the tax preparation environment, taxpayer data would generally need to be sent from the tax software vendor or tax return preparer / electronic return originator (ERO) to a third party identity authentication vendor for the taxpayer to electronically sign the return. This process raises a number of concerns with respect to the taxpayer-tax return preparer relationship and inappropriately adds to the cost of compliance for taxpayers and tax return preparers.

First, we are concerned about the data privacy implications of such a process and a client’s reasonable expectations concerning data confidentiality. Tax return preparers, who may also be EROs, are subject to IRC section 7216. In addition, CPAs are subject to the ethical standards of their state boards of accountancy and State data privacy laws, which impose a requirement on practitioners to maintain the confidentiality of client information received in the course of the professional relationship, absent client consent. 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 other third parties involved in the authentication process, such as credit reporting agencies, as precursor to confirming the taxpayer’s identity, such disclosure may be impermissible absent prior client

consent to use an “authentication vendor” where such vendors are not considered tax return preparers subject to the section 7216 regulations.<sup>3</sup> This potential consent issue is also disconcerting in light of the requirement in the section 7216 regulations to identify a specific recipient of disclosed information during the consent process, in particular given that the tax return preparers utilizing any tax software solution would likely not have the ability to know the names of the authentication vendors in advance during any consent process. Moreover, the taxpayer’s data may be disclosed offshore during the authentication process, and the taxpayer would not have the ability to withhold consent to such a disclosure with respect to a tax return preparer’s disclosure of tax return information outside of the United States.

Second, we are concerned about the impact that a dynamic knowledge-based authentication process could have on taxpayer-CPA client relationships. CPAs often have a year-round relationship with their clients, serving as a trusted advisor on financial matters expanding beyond taxes. Such clients have high expectations that CPAs will treat their information as confidential and with the utmost discretion. When clients interact with CPAs, they do not expect to have their personal data disclosed to third parties. Accordingly, clients may wonder why their private data has been disclosed to a vendor and look to their CPA for answers. Similarly, the question or choices posed during the authentication process may include data that the client has never disclosed to the CPA, leaving the client to question how such data was obtained and whether the presentation of such information to the taxpayer is tantamount to electronic “phishing,” which may give rise to identity theft situations. Finally, if the client is unable to complete the e-signature procedures, they may ask their CPA for assistance with filing a paper copy (and perhaps be frustrated about paying additional fees to compensate the tax return preparer for the unanticipated time). The above discussion highlights some of the concerns that may arise during the verification process and the potential confusions that may result when a client asks their tax return preparer to explain and defend disclosures of personal data to vendors not directly accountable to the practitioner or the IRS.

Because there are sufficient e-signature alternatives available to the IRS, we believe a dynamic knowledge-based authentication should not be the only, or even the preferred, option. For example, instead of using e-signature methods that raise issues of data disclosure and client privacy concerns, the IRS could 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. This would reduce the need for intrusion into the relationship between tax return preparer and client. Alternatively, the IRS could create its own portal through which the taxpayer could obtain a verification code which the taxpayer, in turn, could submit to the preparer for inclusion in the return. This method has the advantage of virtually eliminating the need for the preparer to act as a part of the IRS compliance process and would leave the process to the parties to which it more appropriately belongs, *i.e.*, the IRS and the taxpayer community.

---

<sup>3</sup> 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 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.”)

This approach equally would level the playing field between those members of the taxpayer community who engage a paid preparer to prepare the return and those individuals who prepare the return on their own. As a second alternative, the IRS could institute a method of identification verification that relies on information from the taxpayer's tax return itself, similar to the self-select PIN method currently allowed for taxpayers entering a PIN directly on the return. However, this method, which again could insert the paid preparer into the compliance process is not without problems as it could place pressure on the professional relationship between a CPA and his or her taxpayer-client (it is easy to think of a circular inquiry from a CPA asking the taxpayer for last year's adjusted gross income to verify identity, and in return, the taxpayer asking the CPA to double check the taxpayer's return from last year that the CPA also prepared).

**(2) E-signature methods adopted by the IRS should be flexible enough to accommodate the needs of a variety of taxpayers and tax preparation firms.**

As we noted above, the five core signing requirements proposed by the IRS allow the possibility for the IRS to take a flexible approach in implementing an e-signatures program. We would encourage the IRS to adopt a principles-based framework that builds upon the five core signing requirements as opposed to a rules-based framework that dictates which methods of e-signatures are acceptable. Tax return preparers should have the flexibility to choose the e-signature method most appropriate for their customer base, and the IRS must develop methods suitable for various taxpayer populations. For example, many of our members have practices that prepare tax returns for expatriate employees within large multinational corporations. These individuals may or may not be U.S. citizens and may or may not be currently residing within the United States. Given their geographic dispersion, they are also a group of taxpayers that stand to benefit immensely from the electronic signing of prepared tax returns. Dynamic knowledge-based authentication may not work for these individuals, because they may not have information in U.S.-based public records or credit reports. Other illustrations of cases in which dynamic knowledge-based authentication may not be 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.

To address the full range of taxpayers that would benefit from e-signatures of returns, we recommend the IRS work with the various stakeholders, including unenrolled tax return preparers, CPAs, attorneys, and enrolled agents, as well as the tax software vendors to better understand the full breadth of the taxpayer community that these stakeholders serve.

**(3) Additional e-signature pilot programs are needed to better assess the appropriateness of different e-signature methods.**

If the IRS is to adopt e-signature processes flexible enough to be useful throughout the practitioner community, it would benefit from piloting e-signatures among a wider variety of taxpayers, tax return preparers and tax preparation software firms. We think the IRS should broaden its program to include pilots with CPA firms, including accounting firms serving complex taxpayer-client populations. Having a robust pilot program would lead to e-signature

methods that are more widely adopted by the tax practitioner community and therefore better serves the needs of both the IRS and taxpayers.

**(4) Proposed IRS e-signature guidelines should be published for public comment prior to adoption as final rules.**

Prior to implementing any formal guidance regarding e-signature verification, the IRS should provide adequate advance notice of its broad-based principles approach, or set of rules prior to their finalization and permit public comment on the proposals with the expectation that these public comments would be considered and the principles or rules modified prior to finalization. We would also strongly urge the IRS to consider the procedural issues related to e-signatures. For example, if a taxpayer is unable to successfully complete the authentication procedure, will the taxpayer be able to paper-file a return? If the taxpayer is unsuccessful in completing the authentication procedure after a certain number of attempts, will the taxpayer be blocked from e-filing either temporarily or for that tax year? If a taxpayer is unsuccessful in completing the authentication procedure on the day the return is due and mails a paper copy to the IRS the next day, will the return be delinquent with the associated late-filing penalties and other consequences of a delinquent return?

\* \* \* \* \*

We appreciate your attention to this important matter. If you have any questions, please contact me at (304) 522-2553, or [jporter@portercpa.com](mailto:jporter@portercpa.com); Anita C. Soucy, Tax Executive Committee Liaison to the IRS Practice & Procedures Committee, at (202) 378-5590, or [asoucy@deloitte.com](mailto:asoucy@deloitte.com); or Kristin Esposito, AICPA Technical Tax Manager, at (202) 434-9241, or [kesposito@aicpa.org](mailto:kesposito@aicpa.org).

Sincerely,

A handwritten signature in black ink, appearing to read "Jeffrey A. Porter". The signature is fluid and cursive, with the first name "Jeffrey" being the most prominent part.

Jeffrey A. Porter, CPA  
Chair, Tax Executive Committee