Office of Chief Counsel
Internal Revenue Service
memorandum

CC:PA:01:MEHara
POSTS-113608-18

UILC: 6501.08-00, 6501.08-07

date: May 23, 2018

to: Gillian R. Dalton
Senior Program Analyst
SBSE Exam Policy
(Small Business/Self-Employed)

from: Blaise Dusenberry
Senior Technician Reviewer, Branch 1
(Procedure & Administration)

---

subject: Statute Extension By Consent - Use of Electronic Signatures and Delivery

This Advice responds to your request for assistance. This advice may not be used or cited as precedent.

ISSUES

1. May Internal Revenue Service (Service) employees and managers use electronic or digital signatures when signing or approving agreements to extend the period of limitation on assessment (statute extension consents)?

2. May taxpayers or representatives use electronic or digital signatures or stamps when signing statute extension consents?

3. May taxpayers or representatives use electronic transmission other than e-Fax (*i.e.,* secure email, transmission portals) to send statute extension consents signed either manually or electronically by taxpayers or representatives?

SUMMARY CONCLUSIONS

1. Service employees and managers may use electronic or digital signatures when signing or approving statute extension consents.

2. Electronic signatures are legally valid, but the use of electronic signatures presents a risk that in certain situations the signer may disavow the signature. If

the policy decision is made to allow taxpayers to sign statute extension requests electronically, we recommend adopting electronic signature procedures for electronic signatures by taxpayers that comply with guidance from the General Services Administration contained in *Use of Electronic Signatures in Federal Organization Transactions.* These requirements could be announced through Service published guidance, in publications or on the irs.gov website. Before implementing the use of electronic signatures, we recommend coordination with the IRS Identity Assurance Office, SE:W:IAO:IAG, and a full review of policy and administrative considerations at the appropriate management level to assess and mitigate those risks.

3. There is no legal impediment to taxpayers or representatives using electronic transmission other than e-Fax to send statute extension consents to the Service. Before implementing the use of electronic transmission technologies, we recommend coordination with the appropriate Service Information Technology (IT) offices including the cyber security office, and a full review of policy and administrative considerations at the appropriate management level to assess and mitigate those risks.

BACKGROUND

The Revision of Policy for Use of Fax in Taxpayer Submissions memorandum dated November 19, 2015 from the Deputy Commissioner for Services and Enforcement authorized the Service to accept statute extension consents (e.g., Form 872, *Consent to Extend the Time to Assess Tax*; and Form SS-10, *Consent to Extend the Time to Assess Employment Taxes*) via fax when the taxpayer has signed the consent manually was made clear. As a result of the revision you have received questions and requests regarding other possible methods of signature and delivery of the consent forms.

In particular, your office has received questions regarding:

- Use of electronic/digital signatures by management/employees when approving extension consents on behalf of the Service;
- Use of electronic/digital signatures or stamps by taxpayers/representatives consenting to the extension; and
- Use of electronic transmission other than e-Fax (i.e., secure email, transmission portals) to receive consents signed either manually or electronically by taxpayers and/or representatives.

You have asked us to identify any legal implications that should be considered when attempting to make policy decisions regarding use of electronic signature and delivery methods identified above.

LAW AND ANALYSIS

Extension of the Assessment Period: Forms 872 AND SS-10

I.R.C. § 6501(c)(4) provides that the time for assessing any tax other than an estate tax may be extended for any period of time agreed upon in writing by the taxpayer and the Service, as long as this agreement is entered into before the assessment period has expired.[1] Forms 872 are used as statute extension consents for such taxes as income tax, self-employment taxes, Federal Insurance Contributions Act tax on tips, gift tax, and Chapters 41, 42, or 43 taxes. However, Forms 872 are not used for all types of taxes; for certain taxes or special situations, other Service forms are used, including the Form SS-10, *Consent to Extend the Time to Assess Employment Taxes*.

Although the Form 872 and SS-10 state who should sign the forms, they do not stipulate the type of signature allowable.

Signature Requirements

Section 6061(a) of the Internal Revenue Code provides the general rule that any return, statement, or other document required to be made under any provision of the internal revenue laws or regulations shall be signed in accordance with forms or regulations prescribed by the Secretary. Although the Code does not define the term "signature," 1 U.S.C. § 1 provides that a "signature" includes a mark when the person making the mark intended it as a signature. Section 6061(b)(1) provides that the Service shall establish procedures for accepting signatures in digital or other electronic form. The Code does not provide detailed rules for the use of electronic signatures beyond authorizing their use in section 6061.

Electronic Signatures

In this memorandum, we conclude that Service employees and managers may use electronic signatures. The electronic form of signature, however, is simply data representing a sound, symbol, or process that is made or adopted by a person with the intent to sign a document.[2] To have an electronic signature legally sufficient to hold a person or entity to a document, a security procedure must be part of the process of affixing an electronic form of a signature to a document. A security procedure is used to verify that an electronic record, signature, or performance is that of a specific person (attribution) or for detecting changes or errors in the information in an electronic record (integrity). For example, in the context of a signing process, a security procedure might be used to verify the signer's identity.

---

[1] Treas. Reg. § 301.6501(c)-1(d).

[2] *Buckles Management LLC. V InvestorDigs, LLC.,* 2010 U.S. Dist. LEXIS 73000, *13 (D. Col. July 20, 2010) (holding that electronic record was not signed where the alleged signature was not "executed or adopted by a person with the intent to sign the record").

A “digital signature” is a term for a technology-specific process often used to authenticate identity and/or to verify the integrity of electronic records.[3] While the process is not always an electronic form of signature (notwithstanding its name), it has properties that make it particularly well suited for use as an electronic form of signature where it is expressly intended for that purpose. The digital signature process is often used as a security procedure to identify and authenticate a party, and/or to ensure an electronic record’s integrity. It can be used as part of a signing process in one of two different ways. First, a digital signature can be used as part of the signing process in conjunction with a separate electronic form of signature, such as clicking a button or typing one’s name. In such a case, the digital signature is not a signature in the legal sense, but rather is a security procedure that is used to satisfy the identification, authentication, and record-integrity requirements of the signing process. Second, a digital signature can be used as both the electronic form of signature and as the means to satisfy the identification and authentication requirements process by inserting a scanned image of the signer’s signature, which helps to identify and authenticate the signer.

1. May Service employees and managers use electronic or digital signatures when signing or approving statute extension consents.

Yes. The use of electronic or digital signatures by Service employees and managers when signing or approving agreements to extend the period of limitation on assessment statute extension consents) is legally sufficient. The risk of disavowal of a signature by a Service employee is extremely low, so procedures governing the use by Service personnel of electronic signatures for statute extension requests would present few hazards, so long as the Internal Revenue Manual is revised to set forth the procedures under which these letters and documents are electronically signed. Adopting these requirements in the IRM will assist Service litigators in meeting the requirements of the Federal Rules of Evidence in authenticating and admitting Service business records into evidence when the original signer cannot be located or left the Service, and protect the Service from taxpayer challenges that the electronic signature process is invalid or the document was not signed by the purported Service employee.[4]

---

[3] “Digital signature” has been defined as the result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation. National Institute of Standards and Technology, *Digital Signature Standard (DSS),* FIPS PUB 186-4 (July 2013).

[4] Federal Rules of Evidence 901(a) requires that all documentary evidence be properly identified and authenticated by presenting evidence showing that the document is what it purports to be. Authentication may require evidence proving the genuineness of signatures or a declaration from the document's custodian laying a foundation for admissibility. FRE 901(b)(1). Genuineness is provable based on the distinct characteristics of the signature, and the elements of these characteristics may be established by the facts surrounding the signature event. FRE 901(b)(4); *see* Glen Weissenberger, *Federal Rules of Evidence, Legislative History, Commentary and Authority*, § 901.17 at 641 (1999).

We recommend use of digital signature technology to electronically sign statute extension consents. As a policy matter, using a Service employee or managers scan of their signature on documents received by filers may also provide filers some additional sense of personal interaction dealing with the Service. Statute extension consents are often introduced into evidence in court,[5] and the Service bears the burden of introducing into evidence statute extension consents, valid on their face, that extend the period of limitations for assessment up to the date of mailing of the notice of deficiency.[6]

Introducing into evidence statute extension consents with scanned digital signatures faithfully reproducing the name of the Service employee may give those documents the air of authenticity that may assist in the court in determining that the Service has meet its burden of proof that the parties agreed to extend the period of limitations for assessment.

Digital signatures are already in wide use in the Service as an alternative to a handwritten form of signature. *See, e.g., Interim Guidance Memorandum for Electronic Approval of Enforcement Actions*, SBSE-05-01112-006; 5.6.1.6(3) *Advisory Actions* (10-25-2011)*;* I.R.M. 5.11.2.2.2(11)2 Preparing the Notice of Levy (10-26-2017); IRM 5.12.3.4.3.1(3) and (4) *Use of Electronic Signatures on Lien Certificates* (07-15-2015); I.R.M. 8.6.4.8(3) *Electronic Signature Use on Appeals Letters and Documents* (03-16-2015); IR.M. 20.1.6.1.3.2(1) Note *Managerial Approval for Assessment of Penalties* (07-26-2017); 25.3.5.8(7) *Assessment of Court Sanctions, Penalties, and Costs* (03-20-2012)*.*

2. May taxpayers or representatives use electronic or digital signatures or stamps when signing statute extension consents.

Electronic signatures are legally valid, but the use of electronic signatures presents a risk that in certain situations the signer may disavow the signature. This is especially significant in cases where the ability to assess tax liability is at stake and the amount of the assessment is large. As in all cases involving electronic signatures, whether alternative signature methods should be permitted in a specific situation should balance the convenience to the Service and the taxpayer against the risk that the taxpayer may disavow the document. If the policy decision is made to allow taxpayers to sign statute extension consents electronically, we recommend adopting the following electronic signature procedures for taxpayers that comply with guidelines set forth by the General Services Administration, Use of Electronic Signatures in Federal Organization Transactions (January 25, 2013).

---

[5] See, e.g., *Kinsey v. Commissioner*, 859 F.2d 1361, (9th Cir. 1988); *Piarulle v. Commissioner*, 80 T.C. 1035 (1983).

[6] *Cindirch v. Commissioner*, T.C. Memo. 1984-294. *See also Rutter v. Commissioner,* T.C. Memo. 1986-407; *Mantzel v. Commissioner*, T.C. Memo. 1981-169.

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 requirements could be announced through Service published guidance, in publications or on the irs.gov website. The guidance should include examples of acceptable electronic signature procedures to assist filers in meeting these requirements.

Because of the inherent authentication issues with the use of digital signatures or physical stamps by taxpayers, we do not recommend their use by taxpayers in signing statute extension consents. Use of a stamp, whether digital or physical, to sign a document makes it difficult for the Service to determine whether the signature has been executed by the person represented by the stamp. Allowing taxpayers to use digital or physical stamps or other alternatives to a handwritten signature without an enforceable authentication regime may increase the chance of a fraudulent signature and deprive the Service from using forensic evidence and handwriting analysis to identify the maker of a signature. *See, e.g., Nichola v. United States*, 72 F.2d 780 (3d Cir. 1934) (tax evasion conviction reversed).[7] The Service cannot realistically enforce the requirement that the taxpayer personally affix the digital or physical stamp, so secretaries, other support staff, or unauthorized agents might affix the digital signature or stamp instead of the taxpayer.

Before implementing the use of electronic signatures, we recommend coordination with the IRS Identity Assurance Office, SE:W:IAO:IAG, and a full review of policy and administrative considerations at the appropriate management level to assess and mitigate those risks.

[7] "The generally accepted rule is to the effect that the mere fact that a letter (other than a reply letter) purports to have been written and signed by the person in question is insufficient to establish its authenticity and genuineness. * * * This rule is especially applicable where the letter is typewritten or printed and the signature is attached by a rubber stamp or stencil, or is typewritten or printed." *Nicola*, 72 F.2d at 782.

3. Whether taxpayers or representatives may use electronic transmission other than e-Fax (i.e., secure email, transmission portals) to send statute extension consents signed either manually or electronically by taxpayers or representatives.

There is no legal impediment to taxpayers or representatives using electronic transmission other than e-Fax (*i.e.,* secure email, transmission portals) to send statute extension consents to the Service. Courts have held consistently that, although statute extension consents are not contracts, contract principles apply,[8] and delivery of contract documents by electronic means are well established under commercial law.[9]

The issues surrounding use of electronic transmission are operational and technical because consents contain particularly sensitive taxpayer information and data breaches involving the Service have gained widespread attention as the breaching of Service data has become as simple – or as complex – as gaining access to its restricted networks.[10] Although the Service has tried to impose security standards on its stakeholders,[11] these standards have not prevented malicious actors from breaking into return preparer files to engage in refund fraud.[12]

Before implementing the use of electronic transmission technologies, we recommend coordination with the appropriate Service Information Technology (IT) offices including the cyber security office, and a full review of policy and administrative considerations at the appropriate management level to assess and mitigate those risks.

---

[8] See *Piarulle v. Commissioner*, 80 T.C. 1035, 1042 (1983); see also *Bilski v. Commissioner*, T.C. Memo.1994–55, *affd.* 69 F.3d 64 (5th Cir.1995).

[9] *Shattuck v. Klotzbach*, 14 Mass. L. Rptr. 360, 2001 WL 1839720 (Mass. Super. Ct. 2001) (e-mail messages (1) constituted signed writings sufficient to satisfy the statute of frauds, since they each contained a typewritten signature at the end; and (2) were collectively sufficient to show that the parties had reached an agreement). *See generally* John E. Theuman*, Annotation, Satisfaction of the Statute of Frauds by E-mail,* 110 A.L.R. 5th 277 (2003).

[10] The number of data breaches continues to increase. This can be attributed to the fact that the world's volume of data has been growing exponentially year after year, giving cyber criminals a greater opportunity to expose massive volumes of data in a single breach. Digital Guardian, *The History of Data Breaches,* https://digitalguardian.com/blog/history-data-breaches, retrieved April 27. 2018.

[11] See Publication 1345, *Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns*. The Service has mandated six security, privacy, and business standards to better serve taxpayers and protect their information collected, processed and stored by Online Providers of individual income tax returns. The security and privacy objectives of these standards are: setting minimum encryption standards for transmission of taxpayer information over the internet and authentication of Web site owner/operator's identity beyond that offered by standard version SSL certificates; periodic external vulnerability scan of the taxpayer data environment; protection against bulk-filing of fraudulent income tax returns; and the ability to timely isolate and investigate potentially compromised taxpayer information.

[12] See, e.g.,https://krebsonsecurity.com/2018/02/irs-scam-leverages-hacked-tax-preparers-client-bank-accounts/ (retrieved May 3, 2018).

Please call (202) 317-5417 if you have any further questions.