LIBRARY OF CONGRESS

Copyright Office

37 CFR Part 201

[Docket No. 2013-5]

Authentication of Electronic Signatures on Electronically Filed Statements of Account

AGENCY: U.S. Copyright Office, Library of Congress.

ACTION: Notice of proposed rulemaking.

SUMMARY: The U.S. Copyright Office ("Copyright Office" or "Office") is reengineering certain processes in its Licensing Division to enable cable systems operating under the statutory license governing the secondary transmission of over-the-air television broadcast signals to file Statements of Account electronically. As part of that process, the Office plans to adopt an identity authentication process that will allow for the use of electronic signatures. The Office proposes revisions to specific rules to account for the changes associated with the implementation of an electronic Statement of Account filing system and seeks public comment on the proposed process and regulatory changes to accommodate the use of electronic signatures.

DATES: Comments due [Insert date 30 days after date of publication in the **FEDERAL REGISTER]**. Reply comments [Insert date due 30 days after date of publication in the **FEDERAL REGISTER]**.

ADDRESSES: All comments and reply comments shall be submitted electronically. A comment page containing a comment form is posted on the Copyright Office website at *http://www.copyright.gov/docs/digsig.* The website interface requires submitters to complete a form specifying name and organization, as applicable, and to upload comments as an attachment via a browser button. To meet accessibility standards, all comments must be uploaded in a single

file in either the Portable Document File (PDF) format that contains searchable, accessible text (not an image); Microsoft Word; WordPerfect; Rich Text Format (RTF); or ASCII text file format (not a scanned document). The maximum file size is 6 megabytes (MB). The name of the submitter and organization should appear on both the form and the face of the comments. All comments will be posted publicly on the Copyright Office website exactly as they are received, along with names and organizations. If electronic submission of comments is not feasible, please contact the Copyright Office at 202–707–8380 for special instructions.

FOR FURTHER INFORMATION CONTACT: Andrea Zizzi, Office of the General Counsel, Copyright GC/I&R, P.O. Box 70400, Washington, DC 20024. Telephone: (202) 707-8380. Telefax: (202) 707-8366.

SUPPLEMENTARY INFORMATION:

I. INTRODUCTION

Section 111 of the Copyright Act ("Act"), title 17 of the United States Code ("Section 111"), provides cable operators with a statutory license to retransmit a performance or display of a work embodied in a primary transmission made by a television station licensed by the Federal Communications Commission ("FCC"). Cable system statutory licensees are required to file Statements of Account ("SOAs") and pay royalty fees to the Copyright Office. SOAs contain information on a cable operator's channel line-ups and gross receipts for the sale of cable service to the public. Payments made under the cable statutory license are remitted semi-annually to the Office, which invests the royalties in United States Treasury securities pending distribution of the funds to those copyright owners who are entitled to receive a share of the fees.

Since 2007, the Copyright Office has been implementing plans to reengineer the workflow of its Licensing Division ("Division") for the administration, processing, and

recordkeeping of electronically filed SOAs and related documents. The goals of this ongoing effort are manifold: (1) to facilitate the timely processing of SOAs; (2) to enable the Division to better manage its royalty investment accounts; (3) to expedite the availability of SOAs and other records for public inspection; and (4) to better control costs for those who participate in the statutory licensing system.

One of the key reengineering efforts is to digitize the royalty fee collections process. The Office is in the process of configuring and deploying a commercial off the shelf ("COTS") computer software package as part of an overall business process reengineering effort. The COTS package will support the development of an efficient electronic system for filing, managing, and retrieving Statements of Account, royalty payments, notices, amendments, and other documents related to the work of the Licensing Division. The COTS package will provide the Office with the capability to automate the reengineered processes and provide a platform for managing stakeholders' needs online. The Office has named the new electronic filing system "eLi" ("eLi" or "Electronic Licensing").

Central to the success of eLi is the establishment of a robust identity authentication system for the preparation and electronic filing of SOAs. This authentication will be accomplished through an electronic signature process. An authentication system for electronic filings is necessary because: (1) it establishes the identity of the individual(s) preparing the form; (2) it establishes the identity of the individual charged with the responsibility of certifying and signing the SOA during a secure online session; (3) it creates an electronically signed record in a format that accurately reflects the information provided by the cable system as submitted at the time of the electronic signing; and (4) it helps protect digital documents from tampering. In establishing eLi, the Office must revise its regulations to allow for the use of electronic

signatures as the means of verifying the identity of the individual signing the SOA[1] and linking that individual to a specific electronic record.[2] The Office requests comments on proposed regulations governing the electronic signature process for filing cable Statements of Account.

II. BACKGROUND

A. Levels of Authentication

Today, cable companies may utilize a number of employees in the preparation of an SOA. The Office's regulations, however, require that the document be signed by a person of authority, *i.e.*, an owner, partner, or officer of the company who, by signing, certifies that the information in the SOA is complete and accurate. 37 CFR § 201.17(3)(14). For eLi filings, the Office seeks to adopt an identity authentication method that will identify each person involved in the preparation of the SOA, authenticate the identity of the person certifying the statement by his or her electronic signature on the document, and secure the information provided in the certified document.

The Office of Management and Budget ("OMB") manual, *E-Authentication Guidance for Federal Agencies*, [OMB 04-04], describes the four levels of identity assurance currently used for electronic transactions filed with the federal government that require authentication. In choosing which assurance level is appropriate to authenticate a particular kind of electronic government transaction, the agency must consider the risk factors involved and the level of security required for that transaction. Under the OMB framework, Level 1 provides the lowest

---

[1] *E-Authentication Guidance for Federal Agencies*, [OMB 04-04], § 1.3 (Dec. 16, 2003).

[2] According to Section 106(5) of the Electronic Signatures in Global and National Commerce Act (known as "ESIGN"), an electronic signature is defined as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." ESIGN, 15 USC § 7006(5) (2000). Under Section 2 of the Uniform Electronic Transactions Act (UTEA), the term "electronic signature means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." Unif. Elec. Transactions Act § 2 (1999).

security assurance and Level 4 provides the highest, with Levels 2 and 3 providing a mix of security and ease of access to protected documents.

Level 1 authentication methods do not require identity proofing, but they must provide some assurance that the party who electronically signed a protected document is the same individual who transmitted it. Level 1 methods allow a wide range of available authentication technologies to be employed and permit the use of any token methods of Levels 2, 3, or 4. Successful authentication requires that the electronic signer prove, through a secure authentication protocol, that he or she controls the token. The method does not permit plain text passwords to be transmitted across a network, nor does it require cryptographic methods that block offline analysis by eavesdroppers. Thus, at Level 1, long-term shared authentication secrets may be revealed to verifiers.[3]

Level 2 provides single factor remote network authentication. Successful level 2 authentication requires that the individual prove, through a secure authentication protocol that utilizes approved cryptology, that he or she controls an access token, such as a password or a PIN number. This kind of authentication method is designed to prevent security threats such as eavesdropper and online guessing attacks. However, the single authentication token is vulnerable to compromise via replay, on-line guessing, and verifier impersonation.[4]

Level 3 identity authentication will provide appropriate security for authentication of electronic signatures on Statements of Account. Level 3 provides multi-factor remote network authentication. At this level, identity proofing procedures require verification of identifying

---

[3] *See Electronic Authentication Guideline,* NIST Publication 800-63-1, version 800-63-1 (December 2011)("NIST Publication 800-63-1") at vii, http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf.

[4] *Id.* at vii-viii.

materials and information. Level 3 authentication is based on proof of possession of a key or a one-time password through a cryptographic protocol. As the second step, it requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or one-time password).[5]

Level 4 authentication generally applies only to those systems managing access to highly sensitive information. Level 4 is structured to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. Only "hard" cryptographic tokens are allowed. Level 4 also requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties.[6]

The Copyright Office has conducted an internal assessment of the protocols necessary to secure and certify electronically filed Statements of Accounts. The Office notes that SOAs are made readily available to the public for inspection, and has concluded that once filed, cable system SOAs and related documents do not contain highly sensitive or confidential information. Based upon these findings, the Office has determined that it need not implement the most exacting security protocol for the authentication of the electronic signatures, meaning that Level 4 would be unnecessarily burdensome, given the low security risk. At the same time, the Office has determined that it is necessary to implement an authentication mechanism that guarantees that a particular individual has performed a certain task. Unfortunately, neither Level 1 nor Level 2 authentication will provide sufficient "proof" to link an individual to a specific filing.

---

[5] *Id.* at viii.

[6] *Id.*

The Office does believe that Level 3 authentication methods are well suited for the authentication of electronic signatures on SOAs and related documents. Level 3 methods are utilized by financial institutions[7] and government agencies[8] that have found level 3 methods to provide sufficient security for their work products and operating environments. The Office believes that a two-step authentication process will provide the necessary balance between ensuring the security of the information provided by the cable operator in the SOA while allowing remote authentication of the identity of the individual who has legitimate access to sign

---

[7] Level 3 authentication is prevalent among financial institutions. IDManagement.gov, *Trust Framework Provider Adoption* Process (*TFPAP) For Levels of Assurance 1, 2, and non-PKI 3* 28-36, http://www.idmanagement.gov/documents/TrustFrameworkProviderAdoptionProcess.pdf. In 2005, the Federal Financial Institutions Examination Council ("FFIEC") provided guidance, indicating that commercial banking/brokerage businesses have been using out of band authentication for years. Federal Financial Institutions Examination Council, *Authentication in an Internet Banking Environment* 11, http://ithandbook.ffiec.gov/media/28059/frb-sr_05_19.pdf. The FFIEC gave U.S. banks until the end-of-year 2006 to implement two factor authentication, which is part of the level 3 authentication system. Slashdot, *Banks to use two factor authentication by end of 2006*. http://it.slashdot.org/story/05/10/19/2340245/Banks-to-Use-2-factor-Authentication-by-End-of-2006.

[8] Among other government entities, the General Services Administration ("GSA"), the Internal Revenue Service ("IRS"), the Drug Enforcement Administration, and the United States Patent and Trademark Office have implemented level 3 for authentication purposes. The submission page for the GSA states that all submitted digital authentication certificate(s) must be level 3. General Services Administration eOffer/eMod, http://eoffer.gsa.gov/eoffer_docs/aces_information.htm.

The IRS requires level 3 or level 4 authentication. IRS Remote Access for Data Centers, http://www.irs.gov/privacy/article/0,,id=208067,00.html. Internal Revenue Service, *Modernized e-File (MeF) Guide for Software Developers and Transmitters* 171, http://www.irs.gov/pub/irs-pdf/p4164.pdf.

The Drug Enforcement Administration asserted that "the use of . . . Assurance Level 3 identity proofing and two-factor authentication . . . will provide security commensurate with the current paper-based prescription system, and will meet statutory obligations of the CSA." Drug Enforcement Administration, *E-Authentication Risk Assessment for Electronic Prescriptions for Controlled Substances* 32, http://www.deadiversion.usdoj.gov/ecomm/e_rx/risk_assessment_dea_218.pdf.

In 2008, the United States Patent and Trademark Office clarified that Level 3 authentication was needed for submission of documents other than an initial application. United States Patent and Trademark Office, *Legal Framework For EFS-Web* 4, http://www.uspto.gov/patents/process/file/efs/guidance/legalframework_2008.pdf.

and certify the SOA. "Two-factor" authentication, integral in the Level 3 security framework, provides the required level of confidence necessary to establish in a consistent and secure manner the connection between the signing individual and his/her action as it relates to electronically filed SOAs. Moreover, this level of identity authentication provides safeguards against fraud consistent with the criminal provisions under title 18 of the United States Code.[9]

There are different methods for implementing a "two-factor" Level 3 authentication process, and each has its strengths and weaknesses. In this category are key fobs,[10] digital certificates,[11] USB tokens,[12] smart cards,[13] biometrics,[14] out of band options, and virtual tokens.

---

[9] Title 18 U.S.C. 1001 states as follows:

> (a) Except as otherwise provided in this Section, whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully— (1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact; (2) makes any materially false, fictitious, or fraudulent statement or representation; or (3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry; shall be fined under this title, imprisoned not more than 5 years or, if the offense involves international or domestic terrorism (as defined in Section 2331), imprisoned not more than 8 years, or both. If the matter relates to an offense under chapter 109A, 109B, 110, or 117, or Section 1591, then the term of imprisonment imposed under this Section shall be not more than 8 years.

[10] A key fob is a small hardware device with built-in authentication mechanisms. The key fob controls access to network services and information. The user identifies his or her cell phone and/or email address to be used with the fob and the system to which he or she is accessing stores the information along with the user ID and other details.

[11] A digital certificate is an electronic document that uses a digital signature to bind a public key with an individual using such information as the name of a person or an organization. The certificate, obtained from Microsoft, VeriSign, or other firm, can be used to verify that a public key belongs to an individual.

[12] USB Tokens are designed to securely store an individual's digital identity. These portable tokens plug into a computer's USB port either directly or using a USB extension cable. When users attempt to login to applications via the desktop, VPN/WLAN or Web portal, they will be prompted to enter their unique PIN number. If the entered PIN number matches the PIN within the USB Token, the appropriate digital credentials are passed to the network and access is granted. PIN numbers stored on the token are encrypted for added security.

[13] A smart card, chip card, or integrated circuit card is any pocket-sized card with embedded integrated circuits. Smart cards support multiple authentication factors (PIN, fingerprint template, digitally signed photo), and provide a way to digitally sign and encrypt security documents, other data, communications and transactions. Smart chip-based credentials allow individuals to use their identities safely, quickly and widely and trust that their personal information remains private.

[14] Biometrics are technologies used for measuring and analyzing a person's unique characteristics. There are two types of biometrics: behavioral and physical. Behavioral biometrics are generally used for verification while physical biometrics can be used for either identification or verification. Fingerprint biometrics are common for

After considering cost factors, ease of use, infrastructure constraints, and the level of security provided, the Office expects to pursue either an out of band option or a virtual token option for digital authentication purposes. The Office's proposal is guided by the knowledge that banks, insurance companies, and federal agencies (*i.e.*, the Internal Revenue Service) have implemented these two methods and have found them to be effective.

Virtual tokens. A virtual token is a hash[15] of unique system characteristics paired with the standard username and password. Virtual tokens work by sharing the token generation process between a website and the individual's computer. They have the advantage of not requiring the distribution of additional hardware or software. In addition, since the user's computer communicates directly with the authenticating website, virtual tokens are resistant to "man-in-the-middle attacks"[16] and similar forms of online fraud. In most respects, virtual tokens function like the fob (physical) token noted above, but without the added costs. Some of the benefits of a virtual token authentication method are that the measure is simple to implement, its software is easy to configure, and neither the Office nor the user would require special equipment. However, a key drawback to using virtual tokens for identity authentication related to

---

digital authentication purposes and are best for devices such as cell phones, USB flash drives, notebook computers and other applications where price, size, cost and low power are key requirements.

[15] A "hash" is a unique and permanent code or value generated from the contents of an electronic document at the time of submission.

[16] "A "man-in-the-middle attack," also known as a bucket brigade attack, fire brigade attack, or sometimes a Janus attack, is a form of active eavesdropping in which the attacker (an impersonator) makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection. In fact, though, the entire conversation is controlled by the attacker, who intercepts all messages between the two victims and injects new messages.

SOA forms is that with this method, authentication can only be implemented from previously identified computers connected at a specific site.

Out of Band (Email/SMS). Out of band authentication is a security confirmation system that provides an added layer of protection to validate certain transactions. It uses a separate, discrete pathway ("out of band") to authenticate an individual's identity while performing online transactions. It can be performed either by text messaging or by email. When a user logs into a particular website, a numeric code is sent via Short Messaging Service ("SMS") to either a cell phone or email address on record. Upon receiving the code, the user must to enter it on a secure Web page to verify his authenticity.

Some of the benefits of out of band authentication techniques are: (1) they are easy to implement; (2) the software is simple to configure; and (3) they do not require specialized equipment. Another key benefit of out of band authentication is that unlike virtual tokens, out of band options do not require a participant to use the same computer at the same location, and therefore are more practical for some operators who have several different individuals working on a particular SOA. Out of band security is tied to a specific user but is not tied to a specific computer at a particular physical site. Because of this flexibility, the Office believes that the out of band option may be a more workable approach to implementing electronic signatures for most operators.

The SOA signature authorization method adopted by the Office must also comply with the Federal Information Processing Standards ("FIPS"). FIPS are standards developed by the United States federal government for use in computer systems by all non-military government

agencies and by government contractors.[17] The levels of the digital authentication discussed above, which are known as cryptographic modules, are outlined in FIPS 140.2. Based on the Office's understanding of virtual tokens and out of band methods, the Office tentatively concludes that these Level 3 authentication methods conform to FIPS.

B. Proposed Identity Authentication Procedure

Access to eLi will be predicated on security-based user roles that allow each cable operator to control who has the authority to prepare various elements of the SOA. Cable operators have advised the Office that under the filing system currently in place, often the person who signs/certifies the paper SOA is not the same person or persons charged with doing other preliminary tasks related to the preparation of the SOA and the issuance of the required royalty payment. Under either of the proposed Level 3 electronic identity authentication systems, each person needing access to the document during the preparation phase would be able to gain access to the body of the SOA document, while the system would only give electronic access to the certification page of the SOA to the person of authority who was pre-designated by the cable operator to be the signer. Regardless which authentication method is ultimately chosen, "approval" of an SOA will mean the simultaneous certification and signing of the document by the appropriate official.

---

[17] Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce must approve standards and guidelines for Federal computer systems that are developed by the National Institute of Standards and Technology ("NIST"). *See* NIST Publication 800-63-1, http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for government-wide use. NIST develops FIPS when there are compelling Federal government requirements, such as for security and interoperability, and there are no acceptable industry standards or solutions.

The Office envisions that the digital authentication and signing process would work with either a virtual token or an out of band system. In closely evaluating the two systems, we concluded that the out of band option would be the more practical one, and propose adopting that option. Under either Level 3 option, the person(s) responsible for preparing an SOA on behalf of a cable system would be able to log onto eLi using a previously established user name and password, and the system would authenticate each one as a "preparer." The same procedure would be followed by any reviewer of the "draft" SOA, such as a company officer or attorney.

After the preparers and reviewers have produced a completed version of the body of the SOA in eLi, the person charged with signing and certifying the document on behalf of the cable system would follow a different procedure to electronically approve and sign the document. The signer could be a person who prepared the document or could be someone else with statutory authority to sign it. Like others with access to the SOA, he or she would log onto eLi using a previously established user name and password, and the system would "identify" him or her as the signer authorized to complete the certification process. ELi would then send the signer a code that provides access for a virtual token or out of band authentication of the signer's identity.[18] Once the signer has successfully completed the authentication process, he or she would then follow a procedure to obtain, electronically approve, and electronically sign the final version of the SOA.

The Copyright Office anticipates that the system will display a "notice of consent to electronic records," and the signer would have to "accept" the terms of the notice of consent. Once accepted, the system would display the SOA for approval. The signer would have the

[18] If we adopt an out of band authentication method, the authentication code would be sent via email correspondence to the signer's pre-identified mailbox.

opportunity to review the SOA, enter an "S-signature"[19] and his title, and then complete the transaction by entering a "key" to indicate that the SOA is being electronically signed.

ELi is being designed to save the details about the electronic signature process for each SOA filed. It will use the electronic "key" to generate hash from the contents of the electronically filed SOA. The hash of the SOA will help ensure that the approved SOA is not changed after approval. The electronically-signed document will identify the signer of the document, the date the document was signed, and the information provided at the time of submission.

C. Proposed Regulations

To effectuate the process for electronic identity authentication as a part of eLi, the Office proposes new regulations governing the electronic signing and certification process. Currently, Section 201.17(e)(14) provides that each Statement of Account filed under Section 111 shall contain the handwritten signature of the owner of the cable system or a duly authorized agent of the owner, if the owner is not a partnership or a corporation; or a partner, if the owner is a partnership; or an officer of the corporation, if the owner is a corporation. The signature must be accompanied by (1) the printed or typewritten name of the person signing the SOA; (2) the date of signature; (3) if the owner of the cable system is a partnership or a corporation, the title or official position held in the partnership or corporation by the person signing the SOA; (4) certification of the capacity of the person signing; and (5) a declaration of the veracity of the

[19] An S-signature is a signature, made by electronic or mechanical means, that is inserted between forward slash marks.

statements of fact contained in the SOA and the good faith of the person signing in making such statement of fact.

Under eLi, an electronic signature will be substituted for the handwritten signature, and the other requirements will remain in place for filing a SOA. ELi will include a two step authentication procedure to identify the person completing the certification process. As explained above, the person with authority to certify the accuracy of the information in and sign the SOA will access the certification Section of the SOA using the two step authentication process, approve the form, provide his or her title or official position in the organization, and sign the form using an electronic "S-signature." This process will also apply to the filing of SOA amendments.

1. Purpose and Scope

The proposed Section will be placed at the end of Section 201.17(e) as a new Section (e)(15), because the electronic signatures on an electronically filed SOA will be considered part of the contents of the SOA. Proposed Section 201.17(e)(15) sets forth the purpose and scope of the new authentication and signature protocol. The regulation addresses the criteria under which the Office will consider electronic records and electronic signatures to be trustworthy, reliable, and generally equivalent to handwritten signatures executed on paper. The regulation applies to SOA records and related documents[20] in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in Section 201.17. Where electronic signatures meet the other requirements of Sections 201.17(d) and (e), the Office will consider the electronic signatures to be equivalent to full handwritten signatures,

[20] "Related documents" would include attachments related to the SOA submission and documents submitted in response to a request from the Licensing Division

initials, and other general signings required by Copyright Office regulations. Electronic records that meet the requirements of this regulation may be used in lieu of paper records unless paper records are specifically required.

2. Definitions

Proposed Section 201.17(e)(15)(i) would codify terms and definitions pertinent to electronic document authentication and electronic signatures on SOAs. The Office has created six new definitions:

(A) "Authentication" is a cryptographic or other secure electronic technique that allows the Copyright Office to authenticate the identity of an individual who signs and certifies a Statement of Account or related documents and to determine that the Statement or related documents were not altered, changed, or modified during their transmission to the Copyright Office.

An "electronic signature" is a signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

A "handwritten signature" is the scripted name or legal mark of an individual handwritten by that individual on a document or other writing and executed or adopted with the present intention to authenticate the signed document or other writing.

A "password," is confidential authentication information composed of a string of characters.

The term "token" refers to an item necessary for user identification when used for the authentication of a signature.

3. Signature Parameters

Proposed Section 201.17(e)(15)(iv) sets forth the functional requirements for tying the signer with the electronically filed SOAs. The Office proposes that electronically signed electronic records shall contain information that clearly indicates the following: (1) the printed name of the signer; (2) the date and time the signature was executed; and (3) the title of the signee.

The proposed regulation also specifies that each electronic signature is unique to one individual and shall not be reused by, or reassigned to, anyone else within the cable system.

4. Authentication Protocols

Proposed Section 201.17(e)(15)(v) establishes authentication components and controls for a Level 3 authentication protocol. Level 3 authentication requires at least a two factor authentication process and is based on proof of possession of a cryptographic key. Typically, a key may be used only during a limited time period, *i.e.*, up to 30 minutes. Each SOA must contain the signature of the appropriate certifying official. In some instances, one person will be responsible for signing multiple cable SOAs. The proposed system will allow a signing official to use a single electronic signature that automatically applies multiple signature time stamps to a batch of SOAs submitted by the multiple system operator ("MSO") during a single session, as explained below. In this way, a series of SOA submissions and electronic signings are made with one "signing" executed and initiated by the individual during one continuous period of controlled system access while the key remains valid. If the key's validity expires before all of the multiple SOAs are electronically signed with time stamps, a new key may be requested to complete the certification and signing process. Section (e)(15)(iii) provides that if the signing individual executes one or more electronic signings that are not performed during a single, continuous

period of controlled system access, the signer must reinitiate the authentication process to proceed with the signing.

5. Batch Submissions

Proposed Section 201.17(e)(15)(vi) addresses the submission of multiple SOAs by the same cable operator in one group or "batch" filing. The Office proposes that eLi be configured to enable a cable operator to choose to file multiple SOAs with a single "submit" key. The single electronic signature by the appropriate individual would be automatically applied to all SOAs in the batch with a separate recognizable electronic signature stamp and time stamp for each individual SOA comprising the batch. The proposed rule specifically states that batch or bulk filings of electronically filed Statements of Account would be permitted so long as the cable operator complies with paragraphs (3) and (4) of the regulation.

D. Other Rule Revisions

The shift from a paper filing system to an electronic filing system necessitates an examination of existing rules to see what needs to be changed to facilitate the transition. The Office has identified the following regulations as being in need of updating. There may be other rules that may be affected by the switch to electronic filing, but it is difficult to predict all conceivable changes at this time.

1. Accounting periods and deposits

Section 201.17(c)(2) establishes rules regarding accounting periods and the depositing of royalties under the cable statutory license. This rule needs to be updated to reflect the advent of electronic filing. The rule contains a reference SOAs being "physically received," which implies that a hard copy version of SOAs must be submitted to the Office. An update is necessary to remove the term "physically" from the regulation, to reduce any confusion.

2. Forms

Section 201.17(d)(1) explains where the public may obtain a physical copy of the Statement of Account form. This reference has been in the Office's regulations since 1978, but is irrelevant in an e-filing environment. During the transition to all-electronic filing, the Office proposes to retain this portion of the regulation to accommodate any remitters who may need to use the current SOA forms rather than immediately file on the new online filing system. The SOA forms are currently available either at www.copyright.gov or by contacting the Licensing Division at: Library of Congress, U. S. Copyright Office, Licensing Division, 101 Independence Avenue, SE, Washington, DC 20557-6400. The Office proposes amending the regulation to reflect this different procedure for obtaining hard copy SOA forms, and anticipates that such forms will ultimately be phased out.

3. Handwritten signatures

Section 201.17(e)(14) sets forth the handwritten signature requirements for cable systems filing hard copy Statements of Account. The Office understands, as explained above, that even after the transition to an e-filing system, there will for some time remain certain instances in which cable operators will need to file physical versions of the SOA forms. For example, paper filings may still be necessary where cable operators must back-file SOAs for accounting periods that ended before eLi becomes operational (*i.e.*, covering an accounting period such as January 1-June 30, 2011). The Office anticipates that there will be very few instances in which this mode of filing will still be warranted. Nevertheless, the Office proposes to maintain the current handwritten signature requirements, but modify Section 201.17(e)(14) to include a reference to the new electronic signature requirements.

4. Copies of Statements of Account

Current Section 201.17(l) requires cable operators to file an original and one copy of a Statement of Account with the Licensing Division. The Office proposes to retain this requirement to address those limited instances where paper filings are still necessary. However, the Office plans to amend this rule to clarify that when a licensee files a SOA via eLi, only one electronic form need be filed with the Licensing Division because digital copies can easily be made if the situation so warrants. This will reduce unnecessary filings and work burdens.

5. Signatures and certifications related to corrections, supplemental payments, and requests for refunds

Current Section 217.17(m) outlines the procedures to be followed by a cable operator who seeks to correct a SOA, submit a supplemental royalty fee payment for deposit, or request a refund of royalty fees already paid. Section 217.17(m)(3)(iii)(B) outlines the procedure to be followed where the operator's calculation of the royalty fee payable for a particular accounting period was incorrect, and the amount deposited in the Copyright Office for that period was either too high or too low. The regulation requires the cable operator to submit an affidavit or statement that indicates that the corrected information is signed and certified as made in good faith under penalty of perjury. The affidavit or statement must describe the reasons why the royalty fee was improperly calculated and include a detailed analysis of the proper royalty calculations. The Licensing Division has accepted under this provision amended SOAs that have been signed and certified by the appropriate party in Space O of the statement, because the certification language in Space O is the equivalent of a sworn affidavit or statement in accordance with Section 1746 of title 28 of the United States Code.

The Office posits that it would be appropriate to retain this provision for requests to correct the royalty calculations made in SOAs that were not filed and signed electronically, so long as such statements are still accepted by the Office. However, the Office proposes to amend

the regulation to codify the Division's current practice of accepting the filing of a signed and certified amended SOA in lieu of the sworn affidavit or statement required by the regulation, so long as the amended statement (with any pertinent attachments), describes the reasons why the royalty fee was improperly calculated and includes a detailed analysis of the proper royalty calculations.

The Office has also determined that for SOAs that were originally filed and signed under the eLi system, the electronic signature verification process will satisfy the signature and certification requirements set out in the current Section 201.17(m)(3)(iii). As with paper submissions, the Office would require that electronic amended Statements of Account include, either on the amended statement itself or in an attached document, an explanation of why the royalty fee was improperly calculated and a detailed analysis of the proper royalty calculations.

IV. CONCLUSION

The Office hereby seeks comment from the public on issues raised in this Notice related to the authentication of electronically filed Statements of Accounts, the establishment of proposed rules for electronic signatures, and the concomitant rule changes necessary to implement the new proposed regulations. If an interested party identifies any additional pertinent issues related to the authentication of electronic signatures on SOA forms that have been filed on eLi, the Office encourages the party to bring those matters to its attention.

List of Subjects in 37 CFR Part 201

Copyright.

Proposed Regulation

For the reasons set forth in the preamble, the Copyright Office proposes to amend part 201 of title 37 of the Code of Federal Regulations as follows:

PART 201–GENERAL PROVISIONS

1. The authority citation for part 201 continues to read as follows:

Authority: 17 U.S.C. 702.

2. Amend §201.17 by:

a. Revising the first sentence of paragraph (c)(2), the last sentence of (d)(1), paragraphs (e)(14) introductory text and (e)(14)(iii)(A) and (B);

b. Adding paragraph (e)(15); and

c. Revising paragraphs (l) and (m)(3)(iii)(B).

The revisions and addition read as follows:

§201.17 Statements of Account covering compulsory licenses for secondary transmissions by cable systems

* * * * *

(c) * * *

(2) Upon receiving a Statement of Account and royalty fee, the Copyright Office will make an official record of the actual date when such statement and fee were received in the Copyright Office. * * *

* * * * *

(d) * * *

(1) * * * Copies of Statement of Account forms are available online at www.copyright.gov/forms or upon request to the Library of Congress, Copyright Office, Attn: 111 Licenses, 101 Independence Avenue, SE, Washington, DC 20559.

* * * * *

(e) * * *

(14) The handwritten or electronic signature of:

(iii) * * *

(A) The printed name of the person signing the Statement of Account;

(B) The date of signature, for handwritten signatures on statements that are not filed electronically, or, the electronically created date and time stamp for electronically filed and signed statements.

* * * * *

(15) For signatures on and certification of Statements of Account, each statement must include either a handwritten signature or an electronic signature of a person designated in paragraph (e)(14) of this section. Signing the Statement of Account signifies that the signer has examined the statement and certifies that all statements of fact contained therein are true, complete, and correct to the best of the signer's knowledge, information, and belief, and are made in good faith.

(i) For purposes of this section:

(A) *Authentication* is a cryptographic or other secure electronic technique that allows the Copyright Office to authenticate the identity of an individual who signs and certifies a Statement of Account or related documents and to determine that the statement or related documents were not altered, changed, or modified during their transmission to the Copyright Office.

(B) An *electronic signature* means a signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified. Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

(C) A *handwritten signature* is the scripted name or legal mark of an individual handwritten by that individual on a document or other writing that is executed or adopted with the present intention to authenticate the signed document or other writing. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(D) A *password* is confidential authentication information composed of a string of characters.

(E) A *token* is an item necessary for user identification when used for the authentication of a signature.

(ii) Each electronic signature shall require electronic authentication. Electronic authentication shall require use of both an identification code and a password to obtain a random generated key for access to the Statement of Account for the purpose of signing the statement.

(iii) When an individual executes one or more electronic signings not performed during a single, continuous period of controlled system access, each new electronic signing or signings shall require the signer to reinitiate the authentication process.

(iv) Electronically signed records shall include information that clearly indicates:

(A) The printed name of the signer;

(B) The date and time the signature was executed; and

(C) The title of the signer.

(v) Each Statement of Account must contain the signature of the appropriate certifying official. The verification of the electronic signature of that official must be accomplished by use of an authentication system determined by the Register of Copyrights. The electronic signature authentication process shall be based upon the signer/certifier's proof of possession of a

cryptographic key that would provide that person with access to the certification page of the document being electronically signed.

(vi) A cable official of a multiple system operator may, during a single period of controlled system access, use a single electronic signature to sign/certify multiple Statements of Account so long as the official complies with paragraphs (3) and (4) of this Section. Once such official electronically signs the certification page of the first in a series of related statements, the electronic licensing system will in the same signing session automatically apply multiple electronic signatures and time stamps to some or all of the statements in the batch. If the cryptographic key expires before all of the multiple statements are electronically signed and time stamped, to complete the batch certification and signing process the official must request a new key and begin a new period of controlled system access.

* * * * *

(l) *Copies of Statements of Account*. If a licensee files a Statement of Account electronically, the licensee shall file one electronic copy of the Statement of Account with the Licensing Division of the Copyright Office.

* * * * *

(m) * * *

(3) * * *

(iii) * * *

(B) In the case of a request filed under paragraph (m)(1)(ii) of this Section, where the royalty fee was miscalculated and the amount deposited in the Copyright Office was either too high or too low,

(*1*) If the original Statement of Account was not filed and signed electronically, the request must be accompanied by an affidavit under the official seal of any officer authorized to administer oaths within the United States, a statement in accordance with Section 1746 of title 28 of the United States, made and signed in accordance with paragraph (e)(14) of this Section. In the alternative, the cable operator may choose to file an amended Statement of Account signed and certified in Space O of the amended statement. The affidavit, statement, or amended Statement of Account shall describe the reasons why the royalty fee was improperly calculated and include a detailed analysis of the proper royalty calculations. If the filing official chooses to file an amended Statement of Account, this additional information may be included on the Statement of Account itself or may be set out in a written document attached to the Statement of Account.

(*2*) If the original Statement of Account was filed and signed electronically, the filing official of the cable system shall electronically sign and file in accordance with paragraph (e)(15) of this Section an amended Statement of Account. The amended statement shall include on the amended statement itself, or in an attached written document, an explanation of why the royalty fee was improperly calculated and a detailed analysis of the proper royalty calculations.

* * * * *

Dated: June 18, 2013

_____
Maria A. Pallante,
Register of Copyrights.

[BILLING CODE 1410-30]

[FR Doc. 2013-15016 Filed 06/25/2013 at 8:45 am; Publication Date: 06/26/2013]