CORPORATION SERVICE COMPANY®

Fraud and Electronic Document Recording

By: Paul Hodnefield
Associate General Counsel
CSC

WHITE PAPER

Prepared by:

Corporation Service Company®
800-927-9800
www.cscglobal.com

Fraud and Electronic Document Recording

The introduction of any new technology tends to be accompanied by some apprehension. That is certainly the case with electronic recording of real estate instruments. A lot is riding on the integrity of electronically recorded records, so stakeholders naturally question both the reliability of electronic real estate recording and whether there is increased potential for fraud. Fortunately, these concerns are largely misplaced. As this article will explain, electronically recorded real estate records are no more susceptible to fraud than paper records and in some respects offer much better protection.

Electronically recorded real estate records are no more susceptible to fraud than paper records and in some respects offer much better protection.

Real estate recording fraud

Fraudulent recording schemes take many different forms, but all tend to begin in the same manner. Generally, the perpetrator will look for vacant properties and then file a forged or fraudulent deed. The deed will purport to transfer title into the name of a stolen identity, a fictitious person or an entity controlled by the perpetrator. The deed then serves as the basis for further fraudulent activity.

A common practice is for the perpetrator to obtain a mortgage on the real estate based on the fraudulent deed. If the county recording office has large processing backlog, the perpetrator may be able to repeat the process several times before the recorded mortgages appear of record.

There are many other options for the enterprising criminal after the recording of a forged or fraudulent deed. For example, in one brazen scheme a man recorded false quit-claim deeds on vacant properties. He then drilled out the locks on the buildings and installed his own. Finally, he rented out the properties to unsuspecting tenants. The perpetrator managed to steal about $3.5 million using this method before law enforcement shut him down.

Fraudulent deed recording schemes require the perpetrator to overcome the party signature and notary requirements. The signatures on a fraudulent deed are normally obtained by forgery, deceit or duress. The notary requirement can be more difficult to circumvent. The perpetrator must either use a less-than-diligent notary or provide false identification. In some cases, a corrupt notary may even participate as a willing accomplice.

An entirely different type of fraud, known as “robo-signing,” has also been in the news for the past few years. This practice, discussed in more detail below, came to light during the foreclosure crisis. Unlike other types of recording fraud, robo-signing is conducted by the lender, not an unrelated third party.

Recording fraud is not new. It has been a concern as long as there has been a recording requirement. In response, the law has developed mechanisms to prevent fraud. The formalities of the party signature requirements and notarial acts, for example, provide some protection. Nevertheless, recording fraud remains a problem.

Many of the existing legal protections against fraudulent recording have one thing in common. They assume that recording involves a paper instrument. In

addition to the existing protections, new measures are needed for the electronic recording. And they are already in place.

To place electronic recording fraud prevention measures in context, it is important to define what the term "electronic recording" really means.[1] There are many different variations that would fall within the term. It can mean anything from the electronic submission of a scanned or "digitized" image of the executed paper real estate document to the submission of pure data for a document that never existed in a tangible format.

A number of different laws apply to eRecording. The federal E-SIGN Act[2] recognizes the validity of electronic signatures and notarial acts. The state Uniform Electronic Transactions Act ("UETA") likewise gives effect to electronic signatures and notarial acts. However, many states omitted real estate transactions from the scope of UETA. Consequently, the Uniform Real Property Electronic Recording Act ("URPERA") has also been enacted by a number of states to govern electronic recording of real estate documents.

Electronic recording fraud prevention

State laws often limit a recording office's ability to refuse potentially fraudulent instruments. The role of a recording office is to make sure that the instrument meets the statutory requirements for recording. If the instrument satisfies the recording requirements, then the recording office generally must record it. The recording office does not and really cannot verify the information set forth in an instrument.

Existing legal safeguards to prevent recording fraud generally address the execution of instruments. The formalities required for signatures and notarial acts are intended to ensure that the conveyance was voluntary, knowing, and made by the person entitled to execute the instrument. The real issue is how these procedural safeguards function in an electronic recording environment.

In some respects the electronic recording process itself offers more protection against fraud than a paper instrument. Access to electronic recording systems is generally controlled through agreements between the recording office and third parties with a vested interest in the integrity of eRecording systems, such as portal software providers and service companies.

Recording fraud only works if the perpetrator thinks he or she can get away with it. That is inherently difficult with eRecording.

Recording fraud only works if the perpetrator thinks he or she can get away with it. That is inherently difficult with eRecording. The use of eRecording normally requires the submitter to enter into agreements with private companies and set up an electronic payment system. This arrangement leaves a set of electronic footprints traceable back to the submitter. Moreover, the persons and entities that would go through the set-up process for eRecording are nearly always legitimate enterprises that have a very low risk of potential fraud.

In practice, recording fraud nearly always involves paper instruments. That is not to suggest that fraud cannot be conducted through eRecording. It can. However, as explained below, the risk is no greater than with the recording of paper instruments.

Forgery of electronic signatures

The risk of fraud by a forged electronic signature and the applicable legal protections depend on the method employed for eRecording. An "electronic

[1] The term is also commonly referred to as simply "eRecording."
[2] 15 U.S.C. § 7001 (2013), et. seq.

signature" is 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.[3] That definition can include a scanned image of a paper document that the parties and notary executed with pen and ink, but is broad enough to include purely electronic or "digital" signatures.

The same statutory and procedural protections against forged signatures on a paper instrument apply equally to a scanned record submitted electronically. Forgery still requires the perpetrator to either deceive or conspire with the notary who verifies the signor's identity. Thus, the electronic recording of a scanned instrument presents no greater risk of fraud by forgery than does paper recording.

Forgery, however, becomes more difficult with purely electronic real-estate-related instruments. In that case, the parties and the notary apply digital electronic signatures. Those signatures never existed as pen and ink in tangible form.

The laws that give effect to electronic signatures do not change other legal requirements.[4] They only make electronic records effective to satisfy the existing requirements. Thus, the same protections against forgery apply to both wet ink signatures and digital signatures.

In fact, digital electronic signatures often provide an added layer of protection. Those involved in the transaction can limit access to documents. Furthermore, access requires login credentials. The electronic document typically contains metadata that provide details about who accessed it, applied a signature, when and from where. Consequently, there is a very distinct audit trail that ties the signature to a unique individual.[5] The last thing the perpetrator of criminal fraud wants to do is leave a clear trail for law enforcement to follow.

Finally, the signed electronic document is locked down so any attempt to tamper with the signature becomes evident. As a result, forgery of electronic signatures in the real estate recording process has been all but non-existent.[6]

Deceit, duress and electronic signatures

One cannot determine from any document, paper or electronic, whether a signature was made under duress or obtained by deceit. It is impossible to completely prevent this type of fraud. However, the formalities of the signature process for real estate instruments help prevent execution of the instruments under these circumstances. Prevention of fraud by duress or deceit depends on the role of the notary to observe the parties' demeanor and circumstances.

The notary continues to play this important role in the eRecording process. The substantive notary laws generally still apply to a notarial act performed electronically.[7] A notary public that performs his or her duties in compliance with the applicable law ensures that instruments recorded electronically are no more at risk of being executed with signatures obtained by deceit or duress than are paper instruments.

Fraud and notarial acts

As noted earlier, the ability of a perpetrator to fraudulently record real estate

[3] *See, e.g.,* 15 U.S.C. § 7006(5) (2013). Related laws adopt the same definition. *See*, Tex. Prop. Code § 15.002(4) (2013) (URPERA).

[4] The basic principle is that if a document would be recordable in paper format, an electronic document with the same content and meeting the requirements of the act is also recordable. *See* URPERA § 3 cmt. (a).

[5] *See, e.g.,* Nebr. Rev. Stat. § 86-611(4)(c), which governs electronic signatures. The statute requires the Secretary of State to adopt rules that provide a degree of security reasonably related to the risks and consequences of fraud or misuse for the type of electronic communication which, *at a minimum, shall require the maintenance of an audit trail of the assignment or approval and the use of the unique access code or unique electronic identifier*. (Emphasis added).

[6] Forgery may not be difficult when electronic signatures are used for other purposes, such as clicking on a website to place an order, but these concerns generally do not apply to electronic recording. For a more detailed discussion see Brian Livingston, *Beware: E-signatures can be easily forged*, CNET, http://news.cnet.com/Beware-E-signatures-can-be-easily-forged/2010-1071_3-281338.html (last visited Nov. 21, 2013)

[7] *See, e.g.,* UETA. § 11 cmt. ("This section permits a notary public and other authorized officers to act electronically… However, this section does not eliminate any other requirement of notarial laws.").

instruments depends on the notary public. A perpetrator must find a notary that willingly goes along with the fraud or is less than diligent in confirming identity. Otherwise, the perpetrator must use false identification. No one can prevent a notary from conspiring with the fraudster or force the notary to be diligent. That applies equally to paper and electronic recording. Criminal penalties[8] and civil liability, however, do act as a deterrent.

On the other hand, a diligent notary public can prevent fraud if they take care to verify the identity of the parties and circumstances. The notary can refuse to perform a notarial act if it appears a person is not signing of their own free will.[9] The signor must personally appear before the notary to sign or acknowledge the signature, giving the notary an opportunity to see the demeanor of the parties. If anything is amiss, the notary may not perform the notarial act.

Robo-signing and electronic recording

Another eRecording concern for county recorders and other stakeholders is the practice of "robo-signing." The term suggests an electronic process run amok, such as with a computer churning out electronically signed documents by the thousands without human intent or oversight.

The reality is quite different. The term "robo-signing" has nothing to do with computers or even an electronically automated process. It was coined to describe the practice where a bank employee signs a high volume of foreclosure documents and court pleadings, attesting to the accuracy of the information without verifying the actual facts and circumstances. The employee engaged in this repetitious and monotonous process is thought to be performing robotically, hence the term "robo-signing." As a result of fraudulent robo-signing practices, some borrowers faced improper or unnecessary foreclosure proceedings.

While robo-signing can be performed electronically, it has nearly always been a pen-and-ink practice. No technology can verify that a document signor actually conducted the necessary investigation that enables the party to attest. Consequently, the risk of robo-signing is no greater with electronic signatures or eRecording than it is with the recording of paper documents.

Conclusion

Concerns about fraud in the eRecording process are understandable. Fortunately, all of the protections against fraudulent recording of paper records apply equally to eRecording. In fact, electronically recorded instruments are less susceptible to fraud because of the audit trail and the commercial nature of the parties involved. In the end, fraud in the recording process cannot be eliminated, but the risk is substantially lower for instruments recorded electronically.

The author is a frequent speaker/writer on UCC, lien and real property service issues. Please feel free to contact him with questions or comments at phodnefi@cscinfo.com, or 800-927-9801, ext. 62375.

In the end, fraud in the recording process cannot be eliminated, but the risk is substantially lower for instruments recorded electronically.

[8] *See, e.g.*, Cal Gov Code § 8214.2(a) ("A notary public who knowingly and willfully with intent to defraud performs any notarial act in relation to a deed of trust on real property consisting of a single-family residence containing not more than four dwelling units, with knowledge that the deed of trust contains any false statements or is forged, in whole or in part, is guilty of a felony").

[9] *See, e.g.*, Mich. Comp. Laws § 55.285(8) (2013) ("A notary public may refuse to perform a notarial act."). *See also*, Model Notary Act of 2010 §5-2 ("A notary shall perform a notarial act only if the principal: (4) appears to be acting of his or her own free will").

CORPORATION SERVICE COMPANY®

www.cscglobal.com | www.cscglobal.co.uk | www.cscglobal.de | www.cscglobal.fr