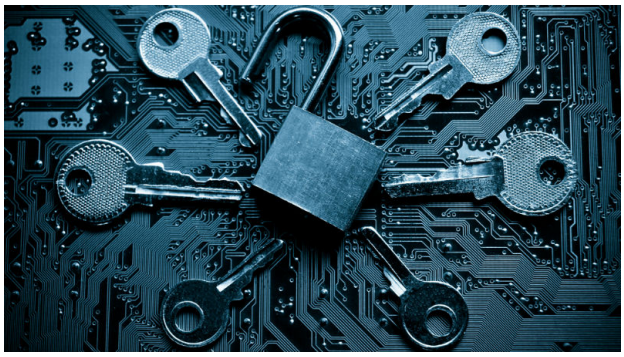
REALTY BIZ NEWS

SMS Authentication: A (Simple) Key for Proving Real Estate Document Legitimacy

AUGUST 30, 2016

In real estate, the deal is never over until the paperwork is signed. But what happens if someone finds something wrong with transaction documents months after you've received your commission? It can happen. A client could claim he never signed a specific clause in a contract, or a real estate authority could put a deal under investigation for fraud.



Documents in the real estate industry—whether captured with ink and paper or in electronic form—are serious matters, and the stakes behind every signature are incredibly high. For clients, it could be their life savings or their dream home. For agents, it's their business reputation and livelihood.

Today many of these real estate documents are signed electronically with e-signatures—and for good reason. E-signatures make signing documents quicker, easier and cheaper. But with digital documentation comes digital responsibility—especially when it comes to keeping tabs on who exactly has access to electronic real estate documents.

Advanced Authentication

Identity authentication for e-signatures exists in several different forms. The most basic type of authentication occurs when a signer logs into her email with a username and password, and then accesses a link to digitally sign a home contract. The technology assumes that since the signer was able to access the email account, she is, indeed, the person intended to sign that contract.

This is fine for many documents. But again, in real estate, there's a lot of financial weight that rests on each transaction—not to mention sensitive personal information that you wouldn't want in the hands of a hacker.

So when documents need to be signed remotely or by clients whom agents don't personally know—or when real estate professionals simply want to go the extra mile with digital security—"multi-factor authentication" provides that extra level of protection. Commonly used by internet giants including Amazon, Google and many others, multi-factor authentication requires at least two forms of identity authentication.

Multi-factor authentication can come in many forms, but the best types are those that combine something you know (a user name and password, a customer ID number, a security question) with something you have (a mobile phone, a hard token, a one-time passcode) or something you are (your fingerprint, your voice).

Some factors are easier to implement than others. For instance, giving each client a hard token to use each time a signature is required isn't usually practical. The token could be lost, and for agents with a large book of business, those tokens could be a pricey investment. Biometric authentication—when signers would use their fingerprints, their voice or something else that's innately a part of them to verify their identity—is still a nascent practice.

SMS Authentication

Short message service (SMS) authentication is one of the real estate industry's best methods to include in multi-factor authentication because it's common, safe and easy. In addition to the first step of authentication, such as requiring a user to sign into an email account, he must also supply the one-time, random passcode he received via a text message to a cell phone. Those two steps combined have to happen successfully before he can gain access to contracts or other documents that need to be signed.

With SMS authentication, you have two points of proof that a signer is who she says she is, making claims of fraud much more difficult. It wouldn't be easy for someone to suggest you had access to her email and her mobile phone when the document was signed. And since your clients are rarely without their mobile phone, it's as convenient as it is secure. It's also cost-effective since there's no hardware to purchase, software to download, or emerging technology to invest in.

This digital form of identity authentication is far easier to prove in court as well. When signature discrepancies occur on paper, you would likely need a handwriting analyst to study the details of style, pressure and spacing to determine if any possible fraud may have occurred. With SMS authentication, a digital audit trail will track and record what number the one-time code was sent to, when it was opened, etc. Further, it's the second layer of proof—not the first, not the only.

Real estate transactions are never low risk. As you move forward with digital adoption in your practice, especially when signers are remote or not personally known, remember to protect and defend your documents' signatures so that there is never any question as to who actually did the signing. You may never need that proof in court—but if you do—your commission, your reputation and your business will be the better for it.

About the authors:

John Harris is the Chief Technology Officer at SIGNiX, a Chattanooga-based digital signature solutions provider that makes signing documents online safe, secure, and legal for any business. SIGNiX offers the only independently verifiable, cloud-based digital signature solution, which combines workflow convenience with superior security. Learn more about what makes SIGNiX different at www.signix.com.

Lisa Mihelcich is the Chief Operating Officer at zipLogix™, a Fraser, Mich.-based technology company created by, owned by and working for real estate professionals to improve productivity and efficiency industry wide. Its software automates and simplifies the repetitive and complex steps of real estate transactions, and is used by more than 650,000 real estate professionals across the country. To learn more, visit www.ziplogix.com.