eSignature platforms to stay effective.

Aug. 19, 2020

Two decades ago, Congress enacted the ESIGN Act which recognized electronic

software, including in PDF readers, for a fully compliant electronic signature there are several factors that need to be considered when choosing a platform.

When determining whether or not an electronic signature is legitimate, ask six questions:

- Do I know who signed the document? (Signer Authentication)

- Do I know they intended to? (Affirmative Act)

- Has there been proper disclosure and consent? (Compliance)

- Has the document been altered in any way? (Document Authentication)

- Is the document electronically accessible to all signers? (Access)

- Can I prove all of this? (Evidence)

Your electronic signature method needs to meet all of these standards to give your signatures the most authenticity and transparency. **Signer authentication** allows you to verify signers through multiple identifiers, including IP address. When a signature request is sent, a consent form is sent in addition to the documents, to confirm it is an **affirmative act** and **compliant**.

The most secure forms of electronic signature and utilizes several safety measures to ensure **authenticity** including digital hashing, encryption, and public key infrastructure. This makes it impossible for a signed document to be unknowingly altered.

Continuous **access** to the signed document can be provided to all parties involved through a portal, or digital copies can automatically be provided.

Can You Prove It?

Furthermore, this audit trail document needs to be saved in a form which prevents it from being edited or deleted, whether it's stored in the same system or with a third-party. In a "write once, read many" format, this makes your electronic signatures compliant to most major standards including the ones enforced by the SEC and FINRA.

Going the Extra Mile With Compliance

Many compliance standards and regulatory bodies require multi-factor authentication methods for electronic signatures, including the IRS. Not only that, but authentication methods that are accepted as indisputable are needed.

Knowledge-Based Authentication (KBA) utilizes information from a third-party to generate a set of questions based on the recipient's personal identifying information that they must answer before fulfilling the eSignature request. Answers about the recipient are pulled from public information databases. For example, it will require the recipient to identify an address where they previously lived. This means the signer must willingly share personal information with the sender of the signature to generate the questions.

One Time Passcode (OTP) generates a random code that the recipient receives via text message that they must input before fulfilling the eSignature request. A code will be sent once the recipient's phone which they use to sign the document.

Summary

eSignature platforms are proven to be efficient and compliant methods for getting your business's essential documents signed. However, the rules of digital documents and signatures are different and require steps to ensure their legitimacy. It's important to know your industry's specific compliance requirements for eSignatures.

Many industries that handle finances and client private information require more

how document management software helps businesses reinvent their manual processes and spur growth.

Accounting • Auditing • Benefits • Technology