CORPORATE COUNSEL
An ALM Website
corpcounsel.com | June 12, 2019

Electronic Signatures: Legal & Practical Considerations for E-Signing on the Virtual Dotted Line

By Anthony J. Diana and David G. Krone

As technology pervades all aspects of business life, business leaders, customers, and employees increasingly expect to be able to execute signatures on agreements, documents and elsewhere with the same level of convenience and assurance as the rest of their IT-enabled business. In response, organizations are exploring solutions allowing individuals to sign these documents electronically, and without requiring signatories be physically present. These electronic signature ("e-signature") solutions provide substantial benefits not only in terms of convenience, but also security and record keeping. However, in assessing whether or how to employ e-signatures, particularly in higher risk transactions, organizations should be careful to manage the practical issues and potential legal complexities associated with e-signatures through careful assessment and a robust governance program.

Implemented correctly with appropriate controls, e-signatures can provide marked improvements in convenience and overall security when compared with traditional physical or "wet" signatures. The ability to instantaneously execute a contract facilitates efficiency and convenience for all interested parties. E-signature solutions also complement current efforts by many businesses to centrally integrate and manage their contracts into digital repositories. Furthermore, forensic security controls coupled with e-signatures provide authoritative and quick verification, reducing the opportunity for fraud or challenges to authenticity.

However, different e-signatures present varying levels of practical risk associated with demonstrating their authenticity and enforceability. Many different types of e-signatures may be considered enforceable under U.S. and foreign law, including the use of an e-signature service, but also typing one's name or initials, an email address or signature line or a scanned manuscript signature, to name a few. In assessing which e-signatures are permitted and in what contexts, an effective e-signature program takes into account the following practical issues: authentication, adoption, non-repudiation, and admissibility.

Authentication involves validating the identity of the individual that

signed the document, and organizations should have methodology in place to tie an e-signature to that individual. Authentication may be accomplished through one or more of the following: "something you know," such as a password unique to the signatory; "something you have," such as a one-time code sent by text message or email to the signatory's personal device; and "something you are," such as a fingerprint scan. A solution incorporating two or more factors is preferable, especially for high risk transactions.

Adoption involves an individual's specific consent that an e-signature operates as an original signature for the purpose of the record and requires the signatory to accept the specific e-signature used in the contract. This can be accomplished through a click-through agreement or a provision in the contract itself.

Non-repudiation involves ensuring that, in executing an e-signature, the signatory intended to agree to the specific terms of the contract or other document. For example, a typical non-repudiation protection requires the signatory to manually apply the e-signature he or she adopted to signature lines in the contract by clicking on designated signature fields.

Finally, admissibility involves the maintenance of documentation or other electronic evidence of the above authentication, documentation, and non-repudiation processes so that it may be presented in court. Admissibility requires that organizations maintain compliance documentation on the accuracy and immutability of its record-keeping system.

In additional to these practical risks, legal requirements for e-signatures may vary substantially depending on the transaction and applicable governing law. An effective e-signatures program must establish clear guidelines clarifying the impact of choice of law and choice of jurisdiction provisions in governing contracts. Generally, across U.S. federal and state law, baseline e-signature laws and requirements are generally consistent, and provide for their general enforceability. However, while the Uniform Commercial Code generally provides for the use of e-signatures in connection with funds transfers, letters of credit, and secured transactions (among others), it requires additional specific technical controls for investment securities, and does not provide for non-negotiable instruments. Non-U.S. countries also vary significantly in their approach to e-signatures, with some imposing additional technical requirements. In particular, European Union General Data Protection Regulation requirements may apply to e-signature transactions involving European individuals or entities, potentially requiring the e-signature solution to accommodate controls such as data protection, data subject rights or restrictions on cross-border transfers.

These legal and practical issues frequently overlap and may entail technical discussions with e-signature solution vendor and/or developers and coordination between internal stakeholders. Accordingly, an organization's e-signature governance program should take full account of its particular business and operational needs. As an initial matter, the program should carefully define the scope of activities where e-signatures may be permitted, including business lines, types of transactions, and jurisdictions. The program should further outline legal requirements observed in the various countries an organization conducts business in, as well as the necessary steps to ensure compliance with those requirements. It should define the approved technology and methodology for e-signatures in particular transactions. Finally, the program must establish controls to operate and manage e-signatures themselves, including policies, procedures, audit protocols, retention methods, and storage.

In sum, e-signatures provide substantial benefits for organizations looking to streamline and modernize their signatures process. Implemented correctly in accordance with a coordinated program, e-signatures may provide more effective and efficient mechanisms for enforceability than tradition physical signatures. However, e-signatures nevertheless also come with specific legal and practical risks that organizations should understand and anticipate appropriately through program controls.

Anthony J. Diana *is the co-chair of Reed Smith's IP, Tech & Data Group and focuses his practice on commercial litigation, internal and regulatory investigations, electronic discovery and information governance, and data privacy and security.*

David G. Krone *is an associate in Reed Smith's IP, Tech & Data Group and focuses his practice in cybersecurity, data privacy and information governance. He counsels clients on the legal, technical and managerial aspects of Records retention to reduce their enterprise information footprint.*