Client Alert

Akin Gump
STRAUSS HAUER & FELD LLP

COVID 19 - The Use of E-Signatures in the UAE

April 2, 2020

As governments implement stricter measures to contain the spread of COVID-19, enforceability concerns regarding electronically signed documents are gaining additional relevance. These concerns are especially present in jurisdictions such as the United Arab Emirates (U.A.E.), where the use of e-signatures is not yet the norm.

The E-Commerce Law

Federal Law No. 1 of 2006 of the U.A.E. (the "E-Commerce Law") enshrines the principle that e-signatures are a legitimate means of authenticating documents. The E-Commerce Law applies to documents governed by the "onshore" laws of the U.A.E. and may not apply in certain free zones that have passed their own e-signature rules. For example, under the rules of the Dubai International Financial Centre (DIFC) e-signatures are governed by the DIFC Electronic Transactions Law of 2017, which outlines requirements that are wholly separate from the E-Commerce Law.

The E-Commerce Law recognizes both "ordinary" and "protected" e-signatures. In basic terms, a "protected" signature is presumed to be authentic, whereas an "ordinary" signature requires the party seeking enforcement to demonstrate that it has a "reasonable" basis for relying on the e-signature's authenticity:

- The question of whether reliance on an "ordinary" e-signature was reasonable often arises where parties use methods containing limited technical authenticity assurances. Reliance on documents signed in this way must be "reasonable," taking into account the surrounding factors. Those factors include the steps taken to determine authenticity at the time of signature, any technical security protections that are inherent in the e-signing method (including whether any authenticity certificates were issued) and other similar factors. If a dispute arises regarding the authenticity of an "ordinary" e-signature, the onus is on the party seeking enforcement to demonstrate that it had a "reasonable" basis to assume authenticity.
- An e-signature is "protected" if it is possible to verify with a high level of certainty that the e-signature is attributable to one specific person and that it was made under that person's full control. This determination is based on several considerations, including whether the e-signature required multifactor authentication and whether the technology reliably links the e-signature to the document on which it appears. While the E-Commerce Law does not prescribe specific technical criteria that will achieve "protected" status, this status is probably best secured by using an

Contact Information

If you have any questions concerning this alert, please contact:

Wael Jabsheh
Partner
wjabsheh@akingump.com
Abu Dhabi
+1 971 2.406.8525

Dinmukhamed T. Eshanov
Senior Counsel
dteshanov@akingump.com
Abu Dhabi
+1 971 2.406.8519

advanced e-signing platform such as DocuSign or other equivalent e-signing platforms. These well-tested platforms generate a digital trail that records who signed the document, their email and IP addresses and the steps taken to authenticate the signatory. These records link the signatory with the signature and underlying document in a way that makes tampering much more difficult. If a signature is "protected" under the E-Commerce Law, a party's reliance on it is presumed to be reasonable and the onus falls on the other party to disprove the signature's authenticity.

Prohibited Transactions

The E-Commerce Law prohibits the use of e-signatures for some transactions. These include:

a. Transactions relating to marriage, divorce and wills.

b. Deeds of title to immovable property.

c. Negotiable instruments.

d. Transactions involving the sale, purchase, certain leases and other dispositions of immovable property and the registration of other rights relating to immovable property.

e. Any document legally required to be attested before a notary public.

Practical Considerations

When e-signing documents under U.A.E. law, parties should keep in mind the following:

- First, not all commercially available e-signature platforms are the same. E-signature platforms authenticate signatures in different ways. Parties should use the most secure authentication methods available and they should use e-signature platforms that are well known and widely used.
- Second, given that the use of e-signatures is not as prevalent in the U.A.E., it is prudent to ensure that signing authority delegations grant express authority to sign by electronic means so that the opportunity to challenge the signatory's authority is limited.
- Third, parties should be cognizant of how the laws of other jurisdictions may be relevant to the underlying transaction. For example, if the e-signed document effects the purchase of an asset located overseas, will the transaction be recognized and enforceable in the country where the asset is located? Or could the sale and purchase be invalidated as a result? These considerations implicate conflicts of laws principles and issues of jurisdiction that are sometimes difficult to resolve, but they should be an important part of any decision regarding the use of e-signature for a particular transaction.

Finally, regardless of a party's location or the jurisdiction governing its contracts, any party that is widely adopting digital execution should ensure that it has taken appropriate action to guard against cyber-crime and online fraud. Parties should train their employees to protect their execution credentials and should institute written policies on the management and use of those credentials for all employees to follow.

akingump.com