DREW & NAPIER

DREWTECH SERIES

CHAPTER 6

Signing without signing

— Contactless contracts

16 July 2020

LEGAL UPDATE

In this Update

With face-to-face meetings falling out of favour because of restrictions on physical interaction, the venerable practice of signing documents in wet ink has started to give way to electronic means of signing documents. However, such technological methods, while useful, come with technical and legal risks.

This article discusses the different varieties of electronic signatures, and their various benefits and limitations.

WET-INK, ELECTRONIC AND DIGITAL SIGNATURES

Not all signatures prepared on an electronic device are alike. They can broadly be separated into two categories, “electronic signatures” and “digital signatures”.

The difference between the two is not just cosmetic. From a technological standpoint, these are very different, requiring different levels of technology to implement. From a legal standpoint, secure electronic signatures are also able to benefit from certain presumptions about authenticity and authorship.

A. Electronic signatures

When asked what an electronic signature is, most people would point to an image of a traditional wet-ink signature inserted above the signature line in a document, where one would otherwise sign by hand. However, this is not the only form of an electronic signature recognised by the law in Singapore.

Broadly speaking, the term “electronic signature” can be used to describe any process that indicates acceptance of an agreement or confirmation of the contents of the document.

Under the Electronic Transactions Act (“**ETA**”), a requirement for a signature can be satisfied through electronic means where:

(a) a method is used to identify the signatory and to indicate the signatory’s intention in respect of the information contained in the electronic record; and

(b) this method is as reliable as appropriate for the purpose for which the electronic record was generated or communicated, in light of all the circumstances, including any relevant agreement; or proven in fact to have fulfilled the function above, by itself or together with further evidence.

This sets a fairly low bar for an electronic signature, since a method used to identify a signatory and indicate her intention can potentially include something as straightforward as an email from an email address belonging to the signatory. By sending the email from her account, the sender indicates her intention to convey the information contained in the email, and the email address identifies her as the sender of such content. Of course, as factors such as the value of the transaction go up, any method used must be considered to see if it is “as reliable as appropriate” given the matters at stake. Given that email addresses can be as frivolous as one wishes, it would be prudent to consider if one would accept an otherwise

unsigned email from a "*fraudster1974@gmail.com*" as being a sufficient identifier for the counterparty to a multi-million dollar sale of property.

B. Digital signatures

Digital signatures are quite different. Using methods such as asymmetric cryptography, hashing functions, and certification from global authorities, these "signatures" are tied to a document and serve as an assurance as to the authenticity of the contents of the document. These can give the recipient of the document a high level of assurance that the document is indeed from the person or entity which it purports to be sent from, and that the contents of the message or document have not been altered or modified.

However, what this method gains in security, it loses in ease of usage. While an electronic signature can be easily added with rudimentary word processing programs, creating and verifying a secure electronic signature requires specialised software. Fortunately, many document processing solutions now have these programs integrated into their functionality.

C. Secure electronic signatures

The ETA recognises a secure electronic signature as a security procedure, either a digital signature or one that is commercially reasonable and agreed to by the parties involved, that can be verified as being:

(a) unique to the person using it;

(b) capable of identifying such a person;

(c) created in a manner or using a means under the sole control of the person using it; and

(d) linked to the electronic record to which it related in such a manner that if the record was changed, the electronic signature would be invalidated.

If these conditions are met (which is eminently achievable with application of a modern digital signature solution), and the parties involved have agreed to the use of such a solution, presumptions arise that the signature is indeed that of the person to whom it correlates, and that it was affixed by that person with the intention of signing or approving the electronic record. Put simply, it becomes much more difficult for a person whose signature is on the document to claim that it was forged or otherwise falsified.

APPLICABILITY OF ELECTRONIC SIGNATURES

As a general rule, electronic signatures are given the same treatment as wet-ink signatures, meaning that an electronic signature will suffice as a replacement for a wet-ink signature. However, the ETA specifically excludes the following matters:

(a) The creation or execution of a will.

(b) Negotiable instruments, documents of title, bills of exchange, promissory notes, consignment notes, bills of lading, warehouse receipts, or any transferable document or instrument that entitles the bearer or beneficiary to claim the delivery of goods or the payment of a sum of money.

(c) The creation, performance or enforcement of an indenture, declaration of trust or power of attorney, with the exception of implied, constructive and resulting trusts.

(d) Any contract for the sale or other disposition of immovable property, or any interest in such property.

(e) The conveyance of immovable property or the transfer of any interest in immovable property.

Despite the exclusions above, the courts have been permissive in allowing electronic signatures to take the place of wet-ink signatures in these excluded categories. While it would be prudent to execute such documents by hand in light of the exclusions, it appears that it is not necessarily fatal that parties have used electronic signatures in place of wet-ink signatures.

The Infocomm Media Development Authority has also released a public consultation paper on 27 June 2019, considering the removal of these excluded categories for business related transactions. While the final word on whether these changes will take effect is not out, this reflects a growing acceptance, even at the governmental level, of e-signatures.

RISKS AND RISK MANAGEMENT

The benefits of electronic signatures are clear – they save the effort of having to print out a document, sign it, scan it back into a computer, and send it off to the intended recipient. However, this convenience also brings with it associated risks.

The most obvious would be the ease of forgery of such signatures. In the case of an image of a wet-ink signature on a document, it is trivial for an unscrupulous actor to create a duplicate image of this signature and

append it onto as many documents as she wishes. This poses problems for both a potential sender as well as a recipient of a document purporting to be signed electronically. The sender is concerned that her signature will be forged for documents which she has no intention of signing. A recipient will fear that the purported sender of the document will later claim that she had never signed this document, and that it is either a cunning forgery made by the recipient or that it was intercepted in transmission and modified (or both).

Of course, as with all claims of forgery, these allegations must be backed up by compelling evidence. Nevertheless, parties considering using electronic signatures should ensure that good electronic trails or records of the document are kept. For instance, when receiving a document with an electronic signature via email, it would be prudent to retain a copy of the email as proof that the document was signed and sent by the counterparty. It is also critical that images of your signature are not unwittingly sent to third parties, for instance as part of an editable Microsoft Word document. Instead, send only PDF files with the signature already inserted, and where possible the signature should overlap with existing content on the page so that it is harder to extract a clean image of the signature.

However, these steps will only go so far to prevent a committed fraudster from forging or alleging forgery of the electronic signature. Self-deleting functions are now available on many messaging apps, and given enough perseverance, careful extraction of a clean image can be performed on even the most convoluted signatures. While electronic signatures cannot be avoided, especially given the realities of international commerce and events such as quarantines, parties should consider the risk profile of their transaction and the trustworthiness of the counterparty to the transaction. Attention should also be given to the use of secure electronic signatures, which are able to mitigate or even resolve these risks altogether, both from a technical as well as a legal standpoint.

CONCLUSION

KEYPOINT

Electronic signatures are no longer a technological novelty to be toyed with. Recent global events have demonstrated the need for tools which can bridge the physical distance between parties.

Electronic signatures and their ilk will form an essential part of this toolkit. Anyone dealing with documents of any sort would therefore be well advised to give careful thought to the implementation of electronic signatures into their workflow processes, while keeping a keen eye on

the legal implications, risks, and effectiveness of these electronic signatures.

UPDATES IN DREWTECH SERIES

1. Chapter 1: The Importance of an Exit Strategy in Technology Contracts <6 March 2019>
2. Chapter 2: Employees, Technology and A Legal Hangover – Bring Your Own Problems? <4 June 2019>
3. Chapter 3: I host, you post, I get sued? <24 September 2019>
4. Chapter 4: Diabolus ex machina <18 February 2020>
5. Chapter 5: Bringing hygiene online – the MAS notice on cyber hygiene <28 April 2020>
6. Chapter 6: Signing without signing – contactless contracts <16 July 2020>

For questions or comments, please contact:

Rakesh Kirpalani
Director, Dispute Resolution &
Information Technology
Chief Technology Officer
T: +65 6531 2521
E: rakesh.kirpalani@drewnapier.com

Timothy Oen
Associate, Dispute Resolution &
Information Technology
E: timothy.oen@drewnapier.com

Drew & Napier LLC

10 Collyer Quay
#10-01 Ocean Financial Centre
Singapore 049315

www.drewnapier.com

T : +65 6535 0733
T : +65 9726 0573 (After Hours)
E : mail@drewnapier.com

DREW & NAPIER

DREW & NAPIER