E - SERIES

BBL | BOOKBINDER BUSINESS LAW

STROKES ON A COMPUTER

ELECTRONIC SIGNATURES

Published 23rd August, 2023

In the last episode of our E-series, we discussed the formation of electronic contracts. If you missed that episode, click here to access it.

In this episode we delve into electronic signatures. Get this: an agreement does not have to be in writing for it to be binding. But, often if the agreement is in writing, it is signed by the parties to evince that they are bound by its terms.

How do you sign electronically?

- There are many ways to effect an e-signature:
- An image of your manuscript signature;
- A mouse squiggle on a screen;
- Names typed in an e-mail;
- A hand-signature created on a tablet using a finger or stylus;
- Unique biometrics-based identifiers, e.g. a fingerprint, voice print, or a retinal scan;
- Clicking the 'I Agree' checkbox.

Why is a document signed anyway?

The function of a signature is to:

- identify the signatory,
- to associate a person with the contents of a document,
- to approve the contents of the document; and
- to witness another person's signature

An electronic signature is afforded functional equivalence to its manuscript counterpart under the Electronic Communications & Transactions Act ("the ECTA").

What makes an e-signature valid under the ECTA?

The mischief that the ECTA seeks to address with respect to electronic signatures is assurance of online security. Among other things, it ensures that the contents signed for by the signatory are not altered after signature, thereby preserving integrity. In paper-based transactions or contracts, prevention of alteration of contents after signature is usually achieved by either ruling through or initialling a page.

If you are using advanced e-signatures (aka digital signatures), you may know that if you have e-signed and someone tampers with the document, the electronic signature suddenly disappears. This is a function of some widely available programs nowadays.

This is because the signature creation data, within the context in which it is used, must be linked to the signatory and to no other person. It must have been under the control of the signatory at the time of signing; and any alterations made after signing must be detectable. The authentication method is one that is usually employed in digital signatures (usually referred to as advanced electronic signatures). The ECTA therefore requires authentication of advanced electronic signatures. This would be in the form of a certificate, which is defined in the ECTA as an electronic attestation that links signature verification data to a person and confirms the identity of the person.

Many of us do not use advanced e-signatures and this is where some of the online securities lie – someone can get a hold of your email address and send instructions to a Bank to pay out all your savings; someone can take the image of a manuscript signature that is stored in your desktop and append it to some agreement.

Catch us next week as we deal with navigating the fraudulent use of your e-signature. We help you navigate e-challenges through our years of experience in contract law and our understanding of the changing business landscape.

For more information, contact Olebile Muzila on olebile@bookbinderlaw.co.bw.