OneSpan
Be bold. Be secure.

ELECTRONIC SIGNATURES IN CANADIAN LAW

Stikeman Elliott

WHITE PAPER

TABLE OF CONTENTS

About the Authors

Written by Chris Lofft, Research Lawyer, Stikeman Elliott LLP, and Michael Laurie, Vice President, Product Strategy, OneSpan, OneSpan Sign co-founder and 25 year veteran of e-signatures.

This paper is a collaboration between Stikeman Elliott LLP and OneSpan. In part one, Stikeman provides an overview on the legal validity of electronic signatures in Canada. Part two has been prepared by OneSpan, and summarizes best practices recommendations for legal compliance when implementing e-signatures.

This whitepaper is not intended as legal advice or legal interpretation of Canadian laws or regulation.

PART 1

(I) Introduction

This paper briefly summarizes the applicable law in relation to the use of electronic signatures in Canada, with particular reference to the use of electronic signatures in the financial services sector. The legal validity of an electronic signature may be governed by provincial or federal law. Generally speaking, for most signatures (including those on contracts) it is provincial law that will be applied to determine whether an electronic signature can be used in place of a handwritten signature. Where a signing requirement is imposed by a federal enactment, then the legal validity of an electronic signature would be a matter of federal law.

(II) Contract Law Is Provincial

It should be noted that in Canadian law the formal and essential validity of a contract is generally determined by reference to the proper law of the contract, whether electronic or otherwise. Contract law in Canada is a matter of provincial law. Thus, the legal effect of an electronic signature on a contract – stated to be governed by the law of a province – would be determined by the law of that province, even where, for example, the contract is between two federally regulated entities (FREs). Canadian federal law has limited application to the threshold question of whether a contract is enforceable.[2]

(III) Signatures Generally

A signature has been defined as "[a] person's name or mark written by that person or at the person's direction" and in commercial law as "[a]ny name, mark, or writing used with the intention of authenticating a document".[3] The common law takes a flexible approach to the validity and legal effect of signatures; the method of signature of a document generally does not have to meet any specific standard of reliability.[4] In *ING Insurance v. Jetty*, a unanimous panel of the Ontario Divisional Court found that a statutory signing requirement, in that case under the Insurance Act (Ontario), could be satisfied by a typed signature:

> It is unreasonable to suppose that … [the purpose of the signing requirement] will be achieved or furthered by a requirement that the insurer sign in a particular way, namely by "putting pen to paper." The common law allows for a signature to be handwritten, stamped or typed, providing that the affixing of the signature conforms with the intent of the legislation. In this case, the intent of the legislation will not be affected or undermined if the signature of the insurer is typed, rather than hand-written.[5]

Accordingly, it is the intent behind the mark that has been affixed to a document as a "signature", rather than the form of the signature itself, that matters. Canadian courts have upheld the validity of online contracts that do not include a traditional signature.[6] A signature can be used to accomplish a number of legal objectives, but it has been said that the "primary function … is to give evidence that the signatory

(an individual or another legal entity) approves and adopts the content of the signed document".[7] Where a statute or regulation requires that a document be signed, so long as the purpose of the signing requirement is not frustrated by the manner of signature, then courts are unlikely to invalidate an act because of some perceived defect in the signature. Indeed, there is very little case law on the validity of the form of signatures.

(IV) Electronic Signatures in Provincial Law

Substantially uniform electronic commerce and electronic signature laws have been enacted across Canada. All the provinces and territories have stand-alone electronic commerce statutes of general application based on model laws promulgated by the U.N.[8] and the Uniform Law Conference of Canada ("ULCC").[9] For example, in Ontario the Electronic Commerce Act, 2000[10] (the "ECA") addresses the use of electronic documents in commercial transactions.[11]

Electronic documents are now recognized as being functionally equivalent to traditional paper-based documents for most purposes, subject to certain requirements with respect to authenticity and integrity. While there are some variations, the provincial e-commerce statutes generally stipulate that signatures, documents, and originals are not invalid or unenforceable by reason only of being in electronic form. Essentially, such e-commerce legislation does not create new law but makes the law "media neutral" and equally applicable to paper and electronic signatures and documents.

The ECA provides that "a legal requirement that a document be signed is satisfied by an electronic signature".[12] The term "electronic signature" is defined in the ECA and in most other e-commerce and related legislation to mean "electronic information that a person creates or adopts in order to sign a document and that is in, attached to, or associated with the document".[13] The authors of *Black's Law Dictionary* indicate that "[t]ypes of electronic signatures include a typed name at the end of an email, a digital image of a handwritten signature, and the click of an 'I accept' button on an e-commerce site".[14] It is clear from these sources that an electronic signature does not have to look like a handwritten signature, although it can (for example, a digitized representation of a handwritten signature).

Generally speaking, it is necessary to obtain a person's consent to use, provide, or accept information in electronic form, which consent "may be inferred from conduct if there are reasonable grounds to believe that the consent is genuine and is relevant to the information or document".[15]

For the most part, the provincial e-commerce laws contemplate what can best be described as a generic electronic signature. The use of additional security measures may be appropriate where the risk of fraud or repudiation in connection with an electronic signature is considered to be high.

As laws of general application, provincial e-commerce laws apply to commercial contracts (including sophisticated financial contracts) and other commercial documents. They would also apply in respect of any signing requirements under provincial statutes, to interactions with consumers, and to consumer contracts.[16] However, the e-commerce acts for the most part do not apply to wills and codicils (including trusts thereby created), certain powers of attorney, conveyances of real property, or negotiable instruments.[17] For these classes of documents, handwritten signatures on paper documents may still be required.

Even before the advent of electronic signatures and e-commerce legislation, courts have been receptive and willing to adapt to technological advancements. In *Beatty v. First Exploration Fund 1987 and Co.*,[18] a judge of the British Columbia Supreme Court found that faxed versions of signed proxies were valid proxies for the purpose of the exercise of voting rights under a limited partnership agreement that required the proxies to be "signed" and "in writing". The court noted that "[t]he law has endeavoured to take cognizance of, and to be receptive to, technological advances in the means of communication".[19] After a review of cases concerning the legal effect of telegrams and other technological advancements, the court concluded that:

> The conduct of business has for many years been enhanced by technological improvements in communication. Those improvements should not be rejected automatically when attempts are made to apply them to matters involving the law. They should be considered and, unless there are compelling reasons for rejection, they should be encouraged, applied and approved.[20]

Thus, long before the adoption of e-commerce laws, the court in Beatty concluded that what was essentially a form of electronic signature (i.e., transmitted via fax) was a valid signature. Given the flexible approach to the legal effect of technological advancements advocated in Beatty and later cases, and the electronic signature provisions of the provincial e-commerce laws, it is unlikely that a court would take an overly technical view of electronic signature requirements for the purpose of most statutory and other signing requirements.

> an electronic signature can incorporate electronic audit trail information that can help establish the identity of the signer, the requisite intent, and the complete and unaltered nature of the document

The provincial e-commerce and general laws do not stipulate any specific means of proof of a signature. Proof, should it be required, would be established by all the surrounding circumstances, subject to the applicable rules of evidence.[21] In this regard, an electronic signature can incorporate electronic audit trail information that can help establish the identity of the signer, the requisite intent, and the complete and unaltered nature of the document.

(v) Electronic Signatures in Federal Law

There are electronic document and electronic signature provisions in the federal statutes governing FREs that are financial institutions[22] and in the Canada Business Corporations Act.[23] These are generally based on the UNCITRAL model laws, with certain enhanced requirements as described below. "Electronic signature" is not defined in any of the FRE laws, but they incorporate the same concepts as the provincial e-commerce and PIPEDA definitions of "electronic signature", with the additional requirements that the signature resulting from the signer's use of a technology or process must permit proof that the signature is "unique to the person" and "can be used to identify the person".[24]

Accordingly, signing with the letter "x" would not likely satisfy these requirements, since that mark would not be unique to the person. However, a digital image or reproduction of the person's manuscript signature, or some other unique personal identifier, would be sufficient provided the technology or process used to affix the signature could also be used to identify the signatory.

Consistent with the notion of consent under provincial law for the use of electronic documents, where an FRE law requires a notice, document, or other information to be provided to a person, the sender must obtain the person's consent to receive such information in electronic form, and the addressee must designate an information system for its receipt.[25] Also similar to the provincial laws, the FRE laws do not stipulate any specific means of proof (other than for secure electronic signatures, where applicable). Proof would be established by all the surrounding circumstances, subject to the applicable rules of evidence.[26]

There is a legislative framework in the FRE laws and PIPEDA for a "secure electronic signature" for prescribed classes of documents.[27] It should be noted that the FRE law enhanced electronic signature requirements (whether generic or secure) apply only where an FRE law or regulation requires a signature.[28] Such requirements relate primarily to the internal workings of an FRE or its dealings with government, rather than to its dealings with third parties. As indicated above, in most instances it is provincial law that will govern the validity of an electronic signature.

PART 2

Best Practices for Addressing E-Signature Legal Requirements

Clearly, the legal foundation exists for the use of e-signatures in Canadian commerce. The provincial and federal laws provide instruction on what an electronic signature needs to accomplish. The law, however, is intentionally technology neutral when it comes to e-commerce and e-business and as such, does not specify how a technology should meet those requirements. For organizations seeking best practices guidance when evaluating e-signature solutions, the following pages summarize the key requirements with recommendations for compliance, based on OneSpan's 25 years of experience working with leading law firms, financial services organizations, and government agencies in Canada and around the world.

Intent

Like its paper equivalent, an electronic signature is a legal concept. Its purpose is to establish a lasting, reliable record of intent. As stated in the legal overview, “it is the intent behind the mark that has been affixed to a document as a 'signature', rather than the form of the signature itself, that matters.” How a signer applies their e-signature in an online process is therefore very important. An e-signature solution should:

- Place conspicuous signature cues at the appropriate locations in the document. Signing cues should be placed directly on signature lines in the document so the placement of the signature relative to any disclosure text (often located just above a signature line) is maintained.
- Use deliberate language to make it clear that by clicking the “SIGN HERE” button, the customer is affixing their signature to the document. It is not advised to use “NEXT” navigation buttons to capture intent.
- Provide the opportunity to opt-out or confirm the intention to move forward in the transaction.

One approach to avoid is the use of a “general acknowledgement”. This is where a user clicks a button or check box once to sign several documents or several signatures in a document with a single e-signature. The e-signature will be associated to a general acknowledgement statement covering all signatures or documents being signed. This is especially not recommended for consumer transactions where disclosures, applications and contracts are subject to much greater scrutiny by the courts.

In addition to building all of these practices into the workflow, the e-signature solution should capture this in the audit trail as proof that a sound process was used to build the customer’s understanding of what they were agreeing to and signing.

> In the Federal PIPEDA, certain classes of documents are held to a higher standard, requiring electronic signatures with four characteristics:
>
> 1. The signature is uniquely linked to the signatory.
> 2. It is capable of identifying the signatory.
> 3. It is created using means that the signer can maintain under his or her sole control.
> 4. It is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Method of Signature Capture

Stikeman's legal overview confirms that, "...an electronic signature does not have to look like a handwritten signature, although it can." Both the act of clicking a button (known as the click-to-sign method) and drawing a signature on a signature capture pad or touchscreen tablet (known as a digitized hand-scripted signature) are equally valid. Unless hand-scripted signatures are required by regulations, in most processes the choice of signature capture method is based on usability, not legality.

Signer Authentication

The need to authenticate and identify a signer varies quite a bit in Canadian e-commerce laws. In the legal overview, an electronic signature is "electronic information that a person creates or adopts in order to sign a document and that is in, attached to or associated with the document". However, the laws are technology neutral and provide no guidance on how to accomplish this. In the Federal PIPEDA, certain classes of documents are held to a higher standard, requiring electronic signatures with four characteristics that should be found in any electronic signature solution:

1. The Signature Is Uniquely Linked to the Signatory

This typically means a system where all user credentials/identities are unique, including:

- Knowledge-based authentication through third-party databases or personal information. This is often used for new customers and users;
- Shared secret data like user ID/PIN, a link from an authenticated email or secret question challenge;
- One-time passcode devices, including using SMS on mobile phones;
- Uploading a photo of a driver's license as further proof of the signer's identity;
- Use of digital certificates on smartcards and mobile phones.

2. The Signature Is Capable of Identifying the Signatory

The above methods for credentials and identity are all associated to an identity which is captured as part of the authentication process and stored with the electronic signature.

3. The Signature Is Created Using Means That the Signer Can Maintain Under Their Sole Control

In each of the methods described above, the signatory has the means to maintain the electronic signature under their control.

4. The Signature Is Linked to the Data to Which It Relates so That Any Subsequent Changes to the Data Will Be Detectable

This characteristic is very important for the electronic signature and is described in the following section.

Some additional considerations for authentication also include:

- The ability to configure different authentication methods within the same transaction
- The flexibility to adapt one or more authentication methods to the risk profile of the organization and EACH process being automated.

> As a result, if any information in the document is changed in any manner, it will be detected and the electronic signature will be visibly invalidated.

Document and Signature Integrity

As noted above, the electronic signature should also be linked to the data to which it relates in such a manner that any subsequent change of the data is detectable. This tamper-proofing is achieved using digital signature technology. The digital signature process creates a digital fingerprint of the document known as a hash, which can be used at a later point to verify the integrity of the electronic record. The hash is encrypted using PKI encryption based on the highest US government standards, to ensure its integrity. As a result, if any information in the document is changed in any manner, it will be detected and the electronic signature will be visibly invalidated.

Note that applying a single digital signature as a tamper-seal for an entire document is not a recommended practice. If a signer and a co-signer e-sign a record on two separate days, that history should be reflected in the audit trail and the integrity of the document should be independently verifiable for each e-signature. The best practice is to apply a digital signature to each e-signature in the document.

All electronic signature data and audit trails should be embedded directly within the document rather than stored separately in the cloud or a proprietary database. In addition to being more secure and easier to manage, there are two pragmatic reasons for this:

1. Document authenticity can be verified independently of the e-signature software. If the vendor goes out of business, the documents are not affected since there is no need to go online to the vendor's site to verify the integrity of the e-signed document.
2. The record can securely travel through any email, storage, or archiving system without being compromised or requiring additional programming. This enables organizations to manage e-signed records in a manner that meets their long-term record retention policies.

The electronic signature solution should therefore:

- Place an e-signature block at the location where the signature was applied
- Embed the e-signature audit trail directly in the document
- Link the audit trail to each signature
- Secure the document and each signature with a digital signature
- Include the date and time of EACH signature in the audit trail
- Provide the ability to verify the validity of the signed record offline, without going to a website
- Provide one-click signature and document verification
- Provide the ability to download a verifiable copy of the signed record with the audit trail

Electronic Delivery

Offer secure, web-based document download with email notification rather than sending documents containing personally identifiable information via unsecured email. This could compromise the customer's private data and violate privacy laws. This method of e-delivery enables the sender to track when the customer obtains a copy of the records and gather evidence of the fact that a record was in-fact delivered.

Another best practice for the delivery of electronic records involves bounce-backs. It sometimes happens that the email notification cannot be delivered to the recipient. In that case, it is prudent to ensure the sender receives an email or other electronic notice to that effect, and that there is a policy in place for alternative action.

> Contract and evidentiary rules apply to electronic records in the same way they do with paper. If ever a dispute over an electronically signed contract goes to court, judgment will be rendered based on the evidence admitted

Document Storage and Retention

Record retention, retrieval, and accessibility are key considerations since electronic documents and associated signatures, audit trails, and evidence must be accessible for the lifetime of the record (50+ years in some cases). The best practice is to save the e-signed documents as Adobe PDF files, an ISO standard and a reliable format for the long term. In addition to the ISO-32001 standard, which defines the overall PDF document format, there is also the PDF/A archival standard. This standard further defines which elements of a PDF document file should be present or excluded for long-term archival.

Note that recipients must always be able to access a copy of the executed documents. The organization originating the transaction may have an obligation to ensure that parties to the transaction have access to signed records.

Evidence

Contract and evidentiary rules apply to electronic records in the same way they do with paper. If ever a dispute over an electronically signed contract goes to court, judgment will be rendered based on the evidence admitted.

Essentially, it is the strength of the electronic evidence that determines exposure to legal and compliance risk. There are two types of electronic evidence: document evidence and process evidence. Together, they provide proof that the document was signed, that it has not been modified, and a demonstration of how the document was presented, reviewed, and signed. With that in mind, look for an e-signature solution that:

- Captures and stores the entire electronic process. An e-signature solution should capture evidence of the full signer experience (i.e., all web pages viewed by the signer, all actions taken by the signer, and other relevant on-screen information, as well as emails and text messages sent during the transaction, together with the time and date of each event, and the user information).
- Makes it easy to review all of the steps and screens that the consumer saw as they were going through the signing process (including the look of the documents as presented in the browser).
- Makes it possible to reliably reproduce the evidence at any point, even years later.

Conclusion

OneSpan understands the unique requirements of the Canadian market and has been automating customer-facing transactions for regulated organizations for more than 25 years. At OneSpan, our technology and expertise is based on insights gained through implementations at leading banks around the world, insurance carriers, healthcare providers, and government agencies – as well as evidentiary and admissibility best practices.

Works Cited

[1] Our review of the applicable laws herein is intended as a high-level overview and should not be construed as legal advice in relation to any particular factual situation. This paper is solely for the bene t of the adressee (eSignLive). It may not be quoted, in whole or in part, or otherwise referred to or used for any purpose other than as general information without the prior written consent of both eSignLive and Stikeman Elliott LLP.

[2] Federal law can result in the non-enforcement of a contract (for example, under federal insolvency laws). Enforcement of a contract is a distinct issue from enforceability of a contract.

[3] Bryan A. Garner, ed., Black's Law Dictionary (9th ed. 2009), sub verbo "signature", online: Westlaw Canada.

[4] ING Insurance Co. of Canada v. Jetty, 2010 ONSC 1091 (Div. Ct.).

[5] Ibid. at para. 8; the case concerned an insurance settlement agreement that according to regulation was required to be signed by both insurer and insured.

[6] For example, clicking on an "I agree" icon: Rudder v. Microsoft Corp., [1999] OJ No 3778 (SCJ) at paras. 16-17 (per Winkler J. (as he then was)); Kanitz v. Rogers Cable Inc. (2002), 58 OR (3d) 299 (SCJ) at paras. 31-33.

[7] John Gregory, "A Book Review: Stephen Mason, Electronic Signatures in Law (3d Edition, Cambridge University Press, 2012)" (22 Aug 2013), www.slaw.ca (blog), available online: http://www.slaw. ca/2013/08/22/a-book-review-stephen-mason-electronic-signatures-in-law-3d-edition-cambridge-university-press-2012/. See also Druet v. Girouard, 2012 NBCA 40 at para. 28.

[8] The United Nations Commission on International Trade Law (UNCITRAL), UNCITRAL Model Law on Electronic Commerce (1996), and UNCITRAL Model Law on Electronic Signatures (2001), both available online at: http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce.html.

[9] ULCC, Uniform Electronic Commerce Act (1999) ("UECA"), available online at: http://www.ulcc.ca/en/. The UECA is itself based primarily on the U.N. model laws.

[10] SO 2000, c. 17.

[11] The ECA is substantially similar to the other provincial e-commerce Acts. The various (generally minor) differences between the provincial e-commerce Acts are beyond the scope of this short paper.

[12] ECA, s. 11(1).

[13] ECA, s. 1(1); see also Personal Information Protection and Electronic Documents Act, SC 2000, c. 5 ("PIPEDA"), s. 31.

[14] Black's, supra note 3, sub verbo "electronic signature". 15 ECA, s. 3.

[16] ULCC, Prof. Michael Deturbide, "Electronic Communications Convention - Impact on common law jurisdictions" (2008), available online at: http://www.ulcc.ca/en/uniform-acts-new-order/current-uniform- acts/680-uncitral-electronic-communications-convention/1621-convention-on-the-use-of-electronic- communications-in-international-contracts-impact-on-common-law-jurisdictions-2008.

[17] See for example, ECA, s. 31; note that some provinces have modi ed their e-commerce legislation to permit electronic signatures and electronic documents in connection with the creation or transfer of an interest in land.

[18] (1988), 25 BCLR (2d) 377 (SC). 19 Ibid. at para. 21.

[20] Ibid. at para. 29; see also Century 21 Canada Ltd. Partnership v. Rogers Communications Inc. 2011 BCSC 1196 at para. 65 ("While Beatty addressed the use of faxed documents, the observations of Hinds J. apply no less ... when applied to the technology of the Internet"). In Re Buckmeyer Estate, 2008 SKQB 141, a Saskatchewan court (without reference to Beatty) found that an email signature was a valid signature for the purpose of a bene ciary designation under provincial insurance law.

[21] Rules of evidence for electronic documents may be found in the Evidence Act (Ontario), and equivalents in most other provinces, which generally provide that electronic documents can have the same evidentiary value as other evidence.

[22] Insurance Companies Act, SC 1991, c. 47 ("ICA"); Bank Act, SC 1991, c. 46; Trust and Loan Companies Act, SC 1991, c. 45; Cooperative Credit Associations Act, SC 1991, c. 48 (collectively, "FRE Laws").

[23] RSC 1985, c. C-44.

[24] See for example, ICA, s. 1044.

[25] See for example, ICA, s. 1037(1).

[26] Rules of evidence for electronic documents similar to those found in the provincial evidence statutes may be found in the Canada Evidence Act, RSC 1985, c. C-5.

[27] See for example ICA, s. 1043 (statutory declarations and af davits). Secure electronic signatures contemplate more stringent technical and authentication requirements than generic electronic signatures; see the Secure Electronic Signature Regulations, SOR/2005-30, enacted under PIPEDA.

[28] ICA, ss. 1043, 1044.

CONTACT US
For more information:
info@OneSpan.com
OneSpan.com/Sign