November 2013

Electronic Signature & Electronic Delivery of Insurance Documentation – Advisory Report

The Centre of Study of Insurance Operations commissioned the law firm Fasken Martineau DuMoulin LLP to produce the attached advisory report in order to provide CSIO members with a broader understanding of the legal requirements necessary to design and implement an effective and compliant electronic signature and delivery process. The report scope also includes provisions regarding "best practices" guidelines for brokers and insurers to consider when designing and implementing an e-signature delivery and archival process.

CSIO believes this report will serve as a foundational document to our members as they investigate how to best leverage the benefits of eSignature technology, enhancing workflow efficiencies and delivering an improved customer experience.

The report contains:

- Summary of the legal requirements applicable to the use of electronic signatures, electronic records and electronic delivery in the P&C insurance business across Canada
- Summary of the legal requirements necessary to design and implement an effective and compliant electronic signature and delivery process
- Identification of "Best Practices" guidelines to consider when implementing an electronic signature solution
- Glossary of common term definitions with respect to electronic signatures

Important Note: This report is advisory in nature only and is not providing legal or other professional advice. If you require legal advice, you should consult with a qualified lawyer.

FASKEN MARTINEAU
www.fasken.com

CSIO

ELECTRONIC SIGNATURE AND ELECTRONIC DELIVERY OF INSURANCE DOCUMENTATION

By Daniel Fabiano, Fasken Martineau DuMoulin LLP[1]

1. Introduction

Although the legal barriers to electronic documents and electronic signatures have been largely eliminated, the insurance sector has continued to rely on the traditional paper and manual signature approach to executing contracts. This traditional approach is increasingly at odds with consumer expectations, as other members of the financial services sector move to support electronic documents and electronic signatures. Consumers are coming to expect that all of their financial transactions can and should be facilitated through electronic processes.

The Internet facilitates a steady stream of online contracts, often through the use of a credit card, simple online disclosure statements, and the click of an "I Agree" button. These contracts use electronic signatures, and rely on electronic delivery of key information (including a copy of the underlying contract). Although an insurance contract carries greater risk than a consumer goods transaction, other financial institutions permit and engage in relatively risky loan and securities transactions using secure electronic signature and document technology. Insurance brokers and carriers can take advantage of the many obvious advantages of an electronic documents process, and in doing so keep pace with consumer expectations. As part of any transition to electronic documents and electronic signatures, insurance brokers and carriers must understand the legal requirements.

In Canada, insurance is governed at both the federal and provincial level. Similarly, the use of electronic documents and electronic signatures is governed by both federal and provincial legislation. Also, some insurance laws have been amended to include specific references to electronic documents. Because of this "patchwork" of laws, this paper is intended to provide general comments and a high-level overview of the Canadian legal landscape as it relates to the use of electronic documents and electronic signatures in the property and casualty insurance sector.

While we have sought input from legal counsel across Canada, this paper is not legal or other professional advice. If you require legal advice, you should consult with a qualified lawyer. At the end of this paper is a list of lawyers/law firms who were consulted as part of this project and who can be retained to provide definitive advice applicable to your circumstances.

---

[1] Daniel Fabiano is a partner in the Toronto office of the international business law and litigation firm Fasken Martineau DuMoulin LLP.

2. Terminology

The definitions for several terms used in connection with this paper may vary. To avoid confusion, we have set out a basic glossary of key terms as an attachment to this paper. Also attached is a listing of the relevant statutes at federal and provincial levels which were consulted for this paper.

3. Legal Requirements

(a) Exclusions

Broadly speaking, electronic commerce legislation is of general application. This means that it applies to commercial activities unless those activities are expressly excluded, or are subject to other legal provisions that prohibit or regulate the use of electronic information or electronic documents.

Generally, electronic commerce legislation does not apply to: [2]

- wills and codicils;
- trusts created by wills or codicils;
- powers of attorney for financial affairs or personal care;
- documents that create or transfer interests in land and require registration to be effective against third parties; or
- negotiable instruments.

Insurance laws impose additional exclusions on the scope of electronic commerce as it relates to insurance.[3] Although the legislation varies across Canada, certain notices, declarations and similar documents are not permitted to be effected by electronic means or electronic notice or documentation – notably:

- a notice of cancellation of a contract of insurance (including for non-payment of premium);
- certain alterations to an insurance policy by the insurer (e.g., an alteration by an insurer following a loss payable to a person other than the insured[4]);

---

[2] The electronic commerce legislation in Manitoba, New Brunswick and Quebec does not specifically exclude wills or codicils, trusts created by wills or codicils or powers of attorney.

[3] The insurance legislation of some provinces (including Alberta, British Columbia and Manitoba (amendments pending Royal Assent)) and the federal government has been amended to make specific reference to electronic commerce legislation and to provide a more integrated approach to the use of electronic documents in the insurance sector.

[4] This is a requirement of s. 126(1) of the *Insurance Act* (New Brunswick) regarding fire insurance policies. See also Statutory Condition 15 (Notice) of the same statute.

- an appointment of a trustee for a beneficiary, or an alteration or revocation of the appointment by a declaration; or

- a nomination of a third party as having the rights and interests of the insured (third party policy) on the death of the insured.

In addition, there is a concern that a designation of beneficiaries may be found to be a "testamentary disposition" – and may be held to be invalid if it is not "in writing" as required by provincial succession laws. In British Columbia, this uncertainty has been addressed by amendments to the *Insurance Act* (British Columbia), which permits the electronic designation of beneficiaries. The insurance legislation of other jurisdictions, as applied to property and casualty insurance, does not specifically contemplate electronic designations of beneficiaries[5] – although case law appears to be evolving towards greater recognition of electronic signatures.[6]

(b) Consent to Electronic Process

Electronic commerce legislation does not oblige anyone to use electronic means to conduct business. Indeed, those laws provide that no one can be compelled to use, provide or accept information or a document in an electronic form – consent is required. Obviously that consent can be express (e.g., a written or verbal statement consenting to the use of electronic processes). It can also be implied from a person's conduct. To be effective, implied consent requires that there be reasonable grounds to believe that the consent is genuine and relevant to the information or document.

When using electronic means to enter into contracts and deliver documents and information, it is important to ensure that consent, whether express or implied, is clear – and that the consent is for both entering into an electronic contract as well as ongoing delivery of information by electronic means.[7]

---

[5] The *Fair Practices Regulation* under the *Insurance Act* (Alberta) permits beneficiary designations by electronic means; however, the provision only applies to life insurance or accident and sickness insurance.

[6] In Re Buckmeyer Estate, 2008, SKQB 141 (CanLII), an executor applied for probate to determine the validity of an existing will and to obtain an order as to whether a subsequent e-mail validly altered a beneficiary designation. The court held that an e-mail signature was an effective signature under the province's electronic commerce legislation, and could qualify as a declaration as defined under s.133(e) of *The Saskatchewan Insurance Act*. That section does not specify an "in writing" requirement, and defines a "declaration" as an instrument signed by the insured:

> (i) with respect to which an endorsement is made on the policy; or
>
> (ii) that identifies the contract; or
>
> (iii) that describes the insurance or insurance fund or a part thereof;
>
> in which he designates, or alters or revokes the designation of, his personal representative or a beneficiary as one to whom or for whose benefit insurance money is to be payable.

See also, in the non-insurance context regarding recognition of New Brunswick's e-legislation, *Girourard* v. *Druet*, 2012 NBCA 40.

[7] Though beyond the scope of this paper, it is noted that the federal government has proposed Canada's Anti-Spam Legislation (CASL) which could come into force in 2014. CASL is proposed to govern all "commercial electronic messages" by requiring the consent of the recipient (express or in certain circumstances implied) and prescribing certain forms of communication for compliance.

(c) In Writing Requirement

Like other types of financial institutions, insurance companies are subject to many requirements that information be set out "in writing". Under electronic commerce legislation (and bolstered by amendments to the insurance legislation in some jurisdictions), information or a document that is in an electronic form can satisfy a legal requirement that it be "in writing" – provided that the electronic form is accessible for subsequent reference.

Similarly, if there is a legal requirement to *provide* information or a document to another person "in writing", that requirement can be satisfied if the electronic information or document is capable of being retained and accessed by the recipient for subsequent reference.

In addition, the legislation of some provinces permits electronic information or documents to satisfy a legal requirement even if that requirement specifies a non-electronic form (e.g., where the legal requirement is specific to a paper document). Generally, this requires that the electronic document be organized in the same or substantially the same way as the non-electronic form, as well as capable of retention and access by the recipient for subsequent reference.

(d) Electronic Copy in Place of an Original Paper Document

In some circumstances, a legal requirement may be specific to an "original" document (e.g., where an original document must be provided to a person). Generally, electronic commerce legislation permits an electronic copy to be retained or provided in place of an original paper document. An electronic document can substitute for that original document, provided that:

- the electronic document is retained in the same format as the original paper document, or in a format that accurately represents the information contained in the original paper document;

- there exists a "reliable assurance" as to the "integrity" of the information contained in the electronic document from the time the document was first created; and

- the information in the electronic document will be accessible for subsequent reference by any person who is entitled to have access to the written document or who is authorized to require its production. Information or a document is <u>not</u> capable of being retained if the person providing electronic information or a document prevents or hinders its printing or storage by the recipient.

Also, where an electronic document is sent or received in lieu of an original paper document, information must be retained concerning the origin and destination, and the date and time when it was sent or received.

Clearly, "integrity" is critical to the retention of electronic documents in place of original paper documents. Assessing the "integrity" of the electronic document is largely a matter of considering whether the information in the document has remained complete and unaltered, apart from the introduction of any changes that arise in the normal course of communication, storage and display. Organizations must select an electronic medium to retain the document that is stable and that assures it will remain unaltered through its life cycle – from creation, in the

course of access, transmission and copying, during retention and until archiving or destruction. Any assessment of the integrity of an electronic document must assess the security measures applied to protect the document throughout its life cycle.

Integrity is also critical to the process of modifying an electronic document, whether the modification is made directly to the document or is documented separately, for example in an amending document. To ensure the integrity of any modification to an electronic document, the person having the authority to make the modification must record the name of the person having requested the modification, the time and reason for the modification, and the name of the person who made the modification. Any modification can form an integral part of the document even if it is recorded in a separate document.

(e) Electronic Forms

Organizations that use pre-programmed electronic forms to facilitate the creation of electronic documents must provide a means for users to correct errors in the document and to notify the organization of errors. A failure to do so could result in the document being unenforceable or the cancellation of the underlying transaction.

It is important to note that, in addition to the notion of consent discussed above, customers cannot be compelled to use specific forms in their dealings with their insurers, absent some legal requirement. In a recent decision of the Saskatchewan Court of Queen's Bench, the Court found that customers may change their beneficiary designations simply by submitting an e-mail message with the required information to satisfy s.133(e) of *The Saskatchewan Insurance Act*, and that an e-mail can contain a valid electronic signature.[8] It is not a requirement under that Act that the insured execute a specific form provided by the insurance company.

(f) Electronic Signature

Electronic signatures are generally permitted by Canadian electronic commerce laws. Canadian electronic commerce laws generally define an "electronic signature" as 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.[9]

Whether an electronic signature will meet a legal requirement for a signature on a document depends on the circumstances specific to that document – including any relevant agreement, the purpose for which the document is created, the time the electronic signature is made, and

---

[8] See Love v. Love, 2011 SKQB 176 (CanLII), and also Buckmeyer Estate, Re, 2008 SKQB 260 (CanLII).

[9] In addition, when considering compliance with such legislation, a distinction could be drawn between (i) the sufficiency of an electronic signature to validate an insurance form, contract or application; and (ii) delivery of electronic notices to an insured to be relied upon by the insurer where such notices have traditionally occurred in person, by regular mail, or by registered mail. See for example, s. 112 and Statutory Condition 15 (Fire Insurance) of the New Brunswick *Insurance Act*; s. 29 of the Nova Scotia *Insurance Act*; ss. 3, 4, 23 of the Newfoundland and Labrador *Insurance Contracts Act*; and ss. 85, 86, 101, Statutory Conditions 5 & 15 (Fire Insurance), and Statutory Conditions 8 & 9 (Automobile Insurance) of the Prince Edward *Island Insurance Act* regarding traditional means of delivery of notices. While the case law is still evolving, it is expected that systems for the delivery of electronic notices will receive greater scrutiny, in terms of the form and substance of electronic notices.

whether the electronic signature is reliable, both in terms of identifying the person in terms of the association of the electronic signature with the relevant electronic document. In part, this is because the form of electronic signature can vary, from encrypted digital signatures to mere digitized signatures (electronic representation of a signature).

Some jurisdictions (including the federal insurance legislation) impose an evidentiary requirement concerning electronic signatures used in insurance documents. Those jurisdictions require that the technology or process used to process or create an electronic signature be able to prove that the signature created using the technology or process:

- is unique to the person signing that electronic document;
- is incorporated into, attached to or associated with that electronic document; and
- can identify the person using the technology or process to sign the document.[10]

Also, public bodies may specify additional requirements concerning the use of electronic signatures on documents submitted to those public bodies. For example, public bodies can specify information technology standards and other requirements around electronic signatures. These requirements only apply to submissions to public bodies, and would not generally apply to the exchange of documents between an insurer and insured.

It is worth noting that the legal landscape in Quebec regarding electronic signatures is less straight-forward and clear than other provinces; however, the relevant legislation and Quebec's Civil Code do permit electronic signatures in principle, and electronic signatures are widely used in Quebec.[11]

---

[10] *Insurance Companies Act* (Canada), s. 1044.

[11] The Quebec electronic commerce law requires any signature affixed to a document, in whatever medium, to meet the requirements of article 2827 of the Quebec Civil Code. It also provides that such a signature will be valid if the integrity of the document is ensured and the link between the signature and the document was established at the time of signing and has since been maintained. Section 2827 of the Quebec Civil Code provides that a "signature is the affixing by a person, to a writing, of his name or the distinctive mark which he regularly uses to signify his intention". This introduces the requirement that if a signature is not the "name" of a person, the distinctive mark used in place of the name must be used "regularly" to signify an intention to be bound. In *Re: Meunier*, 2005, QCCS 13171 (CanLII), the Quebec Superior Court confirmed the validity of a signature consisting of the name of the person in block letters (which was not the usual way in which the individual signed documents). In light of the case, the name of the person typed on a computer may constitute a signature. In *Roussel v. Desjardins Sécurité financière*, 2012, QCCQ3835 (CanLII) the Court concluded that a digitized version of the signature of a lawyer printed on a Court proceeding was a "signature" pursuant to section 2827 of the Quebec Civil Code. The comments of the Ministry of Justice on this provision of the Civil Code of Quebec mention the intention that a concept of a "distinctive mark" could encompass an electronic code that identifies a person; however, the electronic code must be used "regularly" to signify intention. In light of this, when a Court is determining whether, in the circumstances, the intention of an individual was to mark his or her consent to a legal document, the Court will assess the means used by the individual to "sign" a document. There may be a lesser probative value attributed to simply typing a person's name or initials as a signature.

(g) Formation of Electronic Contract

Electronic commerce legislation permits valid contracts to be formed (i.e., offer and acceptance) by electronic means, including by touching or clicking on an appropriate icon or other place on a computer screen, or by speaking.

As with the use of electronic signatures, the legal landscape in Quebec regarding the formation of electronic contracts for financial products is somewhat unclear due to certain comments of Quebec's Autorité des marches financiers (the "**AMF**"). In 2012, following a public consultation concerning the distribution of insurance products via the Internet, the AMF suggested that several provisions of Quebec's *Financial Product Distribution Act* impliedly forbids insurers and brokers from making insurance proposals and concluding contracts via the Internet.[12] We note, however, that the AMF has not engaged in any enforcement activities in line with this suggestion and that in making the foregoing suggestion, the AMF acknowledged that certain entities construe the Act more broadly, and in a manner that would permit such online activities. In practice, we note that several insurance companies are making proposals and concluding insurance contracts in Quebec via the Internet.

(h) Timing of Receipt of Electronic Contract or Document

Electronic information or an electronic document is not "provided" to a person if it is merely made available for access by the person – something more is required, for example, sending an electronic document to an e-mail address provided by the person for that purpose; or, displaying the electronic information to the person in the course of a transaction that is being conducted online.

For contracts, an electronic contract is formed as part of transmitting it to the counter-party (i.e., it is formed in the 'sending' of acceptance). The contract is formed when it enters an information system outside of the sender's control. If the sender and the recipient use the same system, the contract is formed when it becomes capable of being retrieved and processed by the recipient.

For other electronic documents (such as notices), an electronic document is generally considered to be "sent" in the same circumstances. Similarly, an electronic document is generally presumed to be "received" when it enters the recipient's information system and becomes capable of being retrieved and processed by the recipient.

If, however, the recipient has not designated a particular system for the purpose of receiving information or documents of the type that was sent, receipt is only presumed at the time that the recipient becomes aware of the information or document in its information system, and once it can be retrieved and processed by the recipient. Put another way, if the recipient did not specify e-mail as the means of receiving a particular electronic document, and the sender chose to deliver that document by e-mail, the sender would have to alert the recipient to the relevant e-mail message in some fashion – the e-mail message alone would not suffice.

---

[12] Sections 27, 28, 39 of the Act and sections 6, 10 and 12 of the *Regulations Respecting the Pursuit of Activities as a Representative* made pursuant to the Act.

Electronic information or an electronic document is deemed to be sent from the sender's place of business and received at the addressee's place of business.

4. Authentication, Repudiation and Evidence

(a) *Authentication*

One of the challenges presented by electronic transactions is ensuring that the person signing a document or otherwise giving directions is authorized to do so. When dealing with consumers in person, government-issued photograph and other identification can be used to validate the identity of the consumer (e.g., a driver's license). Online transactions are another matter, and alternate forms of authentication are critical to addressing issues of repudiation and fraud in the online environment. Options to validate authority or identity include (among many others): challenge question and answer (or "shared secrets", in which a person is required to provide certain information that another person is unlikely to know); redirection to a secure Website with a login and password; voice signature; video capture; and e-mail notification.

Generally, electronic commerce legislation and insurance legislation do not outline specific authentication measures for online transactions. When adapting an in-person authentication process to an online or electronic environment, organizations should:

- ensure that their authentication protocols adhere to the same legal standard imposed on the applicable activity – this may require organizations to revisit the legal requirements around verifying identity or authority for specific activities and consider how to adapt them appropriately; and

- consider which of the various authentication options and technologies is best suited to validating authority or identity, given the legal requirements and the likelihood of fraud arising out of that activity.

(b) *Repudiation*

Any electronic signature process must consider the risk that the counter-party to a transaction (e.g., the person completing the application for insurance) may repudiate the electronic record – even though it contains that person's electronic signature. Repudiation can be based on various grounds, including that the electronic record was altered after it was signed, or that the electronic signature was used without authorization.

In the end, repudiation is a challenge to the enforceability of a particular document. Repudiation is always a concern in any transaction and the risk of repudiation can be exacerbated in an online environment unless appropriate risk mitigation measures are employed. Such risk mitigation measures need to address following issues:

- Identity – the electronic signature is that of the person who is intended to sign the document;

- Intention – the person applied his or her signature with the intent to sign the document; and

- Integrity – the electronic signature is bound to the document so that any changes to the document can be detected.

One method of managing the risk of repudiation is the form of signature. When determining whether an individual signed a document, one generally relies on the individual's signature as evidence of his or her agreement to the document's contents. At one extreme, an original handwritten signature can be difficult to replicate. Even more difficult to replicate (and at the other technological extreme) is a digital signature (i.e., involving public / private key encryption). Between these two extremes are a range of electronic signature options which are more or less reliable, depending on the circumstances. It is important that a secure and reliable means of electronic signature is chosen for documents that present a higher risk of repudiation.

Another method of managing the risk of repudiation of electronic documents is to maintain an audit trail together with tamper-proofing measures. This helps to ensure that any changes to the electronic document are tracked and can be explained and validated, with unauthorized changes blocked so that they do not alter the document. In many ways, electronic documents can offer greater security and tamper-proofing than paper documents because of the ability to maintain information about changes and attempted changes to the document.

(c) *Electronic Evidence*

Organizations utilizing electronic contracts and other documents must have confidence that such records will be admissible in a dispute or legal proceeding. Prior to the enactment of electronic documents, federal and provincial evidence statutes and a number of rules of evidence (e.g. hearsay, authenticity and the best evidence rule) could present challenges when attempting to rely on electronic evidence in a legal proceeding. However, a number of evidence statutes have been amended to provide significant confidence and certainty regarding the admissibility of electronic documents.

Assessing the validity of a specific electronic document or signature can only be done in light of the specific factual context – just as with handwritten signatures. Admitting electronic records into evidence may require an individual with first-hand knowledge of the relevant technology and processes within the organization to provide an affidavit that attests to certain facts, such as:

- how the electronic document or signature system works and that it was functioning properly (or, if not operating properly, the operational issues did not affect the integrity of the document and there are no other reasonable grounds to doubt the integrity of the system);

- the facts supporting how the counter-party (e.g., the consumer) is the person who signed the electronic record;

- the audit trail of the electronic document; and

- how tamper-proofing measures show no alteration of the electronic document.

Electronic documents, electronic signatures and electronic records management systems need to be designed with evidentiary concerns in mind. For example, complying with certain published

standards regarding electronic records can result in positive benefits in the context of litigation. The *Canada Evidence Act* and provincial evidence acts provide that standards may be considered in determining the admissibility of electronic records. One notable standard, the Canadian General Standards Board's "Electronic Records as Documentary Evidence CAN/CGSB-72.34-2005" standard, is intended to provide a means by which organizations can establish: "(a) authenticity of a record, (b) integrity of the [records management system] that a record was recorded or stored in; and (c) that it is "a record made in the usual and ordinary course of business…". Complying with this standard will help ensure that electronic information is admissible in court.

5. Advisable Practices

The legal requirements discussed above give rise to a number of advisable practices for insurance brokers and carriers when designing and deploying an effective and compliant regime to use and handle electronic signatures and electronic documents.

i. When considering electronic signature and electronic document processes, involve relevant internal personnel, legal counsel and technology experts at the outset. The goal should be to design a process that is operationally suitable, legally compliant and technologically feasible – and without the need for wasteful or costly reversals or failures.

ii. Develop a corporate policy that is reviewed and updated regularly (at least once a year). Consider designating a senior officer or employee as responsible for implementing the policy and keeping on top of changes in the law (e.g. introduction of new electronic commerce and related legislation at federal or provincial levels). Use the policy to train new personnel who will be involved in the processing of electronic documents and to coordinate practices among different departments or groups (e.g. IT and legal).

iii. Consider which electronic signature methodologies are suitable for which processes. Likely, several electronic signature capabilities will be needed. Business processes should be assessed to consider both the legal requirements, as well as technological limitations. Likely, less risky transactions may merit a digitized signature or simple e-mail signature line; whereas, high risk transactions may require electronic certificates or secure log-in.

iv. Determine how electronic documents will be delivered. In doing so, consider privacy and confidentiality issues. For example, should information be sent within the body of an e-mail, or in a secure attachment, or should the e-mail contain a link to a password protected site through which the consumer can log-in to retrieve the information. The advantage of the latter is that it contributes to an audit trail.

v. E-mail inherently involves issues like spam filters or discontinued accounts. Consider how to handle undelivered e-mail (e.g., where the message "bounces back" due to some error or issue with the recipient's e-mail account). This may require a further review of how the law in your jurisdiction applies to notices of undelivered mail. Most jurisdictions permit organizations to resort to registered mail as a fall-back if other means of communication are unavailable.

vi. Obtain the consumer's consent to:

a. accept all notices and communications by electronic delivery;

b. use electronic signatures to sign documents where appropriate (e.g., where subject to appropriate means of authenticating the identity of the consumer)

Consider framing the consent broadly to encompass a variety of methods. Consider capturing a consumer's consent to sign a document using an electronic signature in a separate document. Ensure that consent requirements are updated to reflect new legislation or regulations.

vii. For audit trail purposes, consider how each electronic document can be tracked so that important audit trail information is recorded and associated with the record. For example, technological means can be employed so that the document is electronically stamped with the time and date through all steps in the process. In particular, ensure that the time of sending or of receipt of a document may be established – for example, by producing a transmission slip or an acknowledgement of receipt. This should log the date, hour, minute and second of sending or receipt and should indicate the source and destination of the document.

viii. Consider how to tamper-proof electronic documents. The security should be effective at the time that the electronic signature is applied to the document or, if not signed, upon its creation or receipt (at the latest). The content should be locked through encryption technology so that any unauthorized alterations are not possible or are identifiable as unauthorized.

ix. Ensure that the "original" electronic document is distinguished from any copies. Copies of "original" electronic documents should only be made with the approval of an appropriate control person.

x. If voice signatures will be used at any point, consult with legal counsel concerning how to document a voice signature.

xi. When obtaining an electronic signature, use a process that:

a. requires the signer to access and open the document before it can be signed – this helps to evidence that the signer had an opportunity to read and understand the document before signing it;

b. requires a specific affirmative action in order to effect the electronic signature;

c. clearly informs the signer of how to sign the document (e.g., clicking "I Agree" represents the signer authorizing the document and agreeing to its terms); and

d. records the date, time and signature and retains that information, along with the signed document, in a secure, tamper-proof manner.

6. Glossary

"**audit trail**" means a set of records that document a sequence of activities that affect a given transaction – including instances in which a document is accessed, modified, executed and transmitted. These records are to be secure from inappropriate modification or tampering and are essential in responding to challenges to an electronic signature or the integrity of an electronic document.

"**authentication**" means verifying that a person signing a document or otherwise giving directions is authorized to do so.

"**digital signature**" is a mathematical scheme (using public key and private key encryption) for demonstrating the authenticity of a digital message or document. A digital signature is a specific means of implementing an electronic signature, although not all electronic signatures are digital signatures. It is not a signature as much as it is a code.

"**digitized signature**" means an image of a handwritten signature taken from an electronic signature pad or paper scan. A digitized signature is not a digital signature, and is generally not seen as secure because it can be easily copied.

"**electronic document**" means a record created, sent, received or stored by electronic means.

"**electronic signature**" means 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.

"**repudiate**" means to challenge the enforceability of a document, whether because it was not duly executed, or because it was altered without the consent of the person against whom it is to be enforced.

"**tamper-proofing**" means the use of encryption technology to secure a document once an electronic signature is applied, and to secure the related audit trail. If a document is modified or tampered with, the technology would invalidate the document or otherwise flag the tampering.

7. **Law Firms and Lawyers Consulted**

Alberta / British Columbia	**Fasken Martineau DuMoulin LLP** *Kareen Zimmer*
Saskatchewan	**McDougall Gauley LLP** *Jacqueline Shaw* *Michael Wright*
Manitoba	**Taylor McCaffrey LLP** *Nicole D.S. Merrick* *Patrick Rykes*
Ontario / Federal	**Fasken Martineau DuMoulin LLP** *Daniel Fabiano* *Koker Christensen*
Quebec	**Fasken Martineau DuMoulin LLP** *Jean-Philippe Mikus*
New Brunswick **Newfoundland** **Nova Scotia** **Prince Edward Island**	**Stewart McKelvey** *Charles LeBlond* *Dan Boone* *Colin D. Piercey* *Daniela Bassan* *Nicole McKenna*