



Does E-mail Have the Same Evidentiary Foundation as Paper-and-Post Mail?

*RPost was invited to speak to the **Computer Law Committee of the IP Section of the California State Bar and Southwestern University School of Law on August 8**. The topic was about e-mail having the same evidentiary foundation as paper-and-post mail, some of the legal risks of standard e-mail, misconceptions of various e-mail security solutions in the market, and the evidentiary value of RPost Registered Receipt™ e-mail. A copy of the presentation made by Zafar Khan, CEO of RPost, is available at www.rpost.com/ipsection. This report on that session, prepared by **Thomas Palamides, Canadian Consulate General**, Los Angeles, was released to business and government executives on August 10, 2005.*

*Thomas Palamides, Trade Commissioner, Canadian Consulate General, 550 S. Hope Street, 9th Floor, Los Angeles, CA 90071
(Thomas.Palamides@international.gc.ca)*

INTRODUCTION

It was supposedly an open-and-shut case. The plaintiff presented six printed e-mail messages that were sent to the defendant over the course of several weeks. The e-mails detailed fully a story of breach of contract. The defendant affirmed receipt of e-mail message numbers one, two and six, but not the others. The judge ruled that all the e-mails were inadmissible. What went wrong?

A monumental shift has begun within our transactional-focused contract-based electronic society. E-mail correspondence on the Internet is very complex due to the wide variety of computer servers and systems. Therefore, it is NOT safe to assume that a recipient receives an e-mail when a sender sends a standard text message. Intranet e-mail, however, occurs within a controlled environment, so the issues of who sent what, and when, are less scrutinized. Should an e-mail communication end up in court, for any reason, its "evidentiary value" may be questioned unless precautions are taken.

Learn why agencies such as the US Congress' Government Accountability Office, Attorneys and Law firms nationwide, AT&T, Sprint, Qwest have taken steps to ensure validity of Internet e-mail correspondence.

REPORT

The Electronic Signatures in Global and National Commerce Act (ESIGN), a Federal Law enacted by the US Congress in 2000, and the Uniform Electronic Transaction Act (UETA) which stems from a United

Nations conference was first enacted in 1999 and has ratified, in various versions, by all fifty US States, define, "that a record or signature may not be denied legal effect or enforceability solely because it is in electronic form."

UETA goes further, affirmatively stating that "if a law requires a record to be in writing, an electronic record satisfies the law," and both statutes make reference that "if a law requires a signature, an electronic signature satisfies the law." Therefore, the ESIGN and UETA guarantee e-mail messages the same legal weight and value, in a court of law, as paper records.

Further, the courts have recently ruled that proposals tendered by e-mail can have the same force as written contracts [Plymouth Superior Court, Shattuck v. Klotzbach]; and that documents can be legally served by e-mail [9th Circuit court of Appeals, Rio Properties Inc. v. Rio International Interlink.]

Consistent with ESIGN and UETA, one should be aware of the fact that both provide that a contract, or a signature relating to a commercial transaction, may not be invalidated solely because it is in electronic form.

THE FALSEHOODS OF STANDARD E-MAIL

Because of the ease with which a text message can be modified (i.e. often with only two clicks of the mouse), a standard e-mail that is sent or received, archived electronically, or stored in printed form, has limited "evidentiary value" in a court of law. The usefulness of such documenting is very misleading. With e-mail, the burden of proof is currently on the sender. It has to be proven that it was sent. Moreover, it has to be proven that it was received. There is a misconception by the public that if one looks in the "Sent Folder" that the e-mail was actually delivered to the recipient.

There is also a "Time Stamp" that appears on a standard e-mail in the receiver's message window. The accuracy of this time, however, depends on the user's computer time setting, and has little "evidentiary value" in a court of law. Discussed later in this report is the fact that the recipient's authorized mail server does provide a level of time accuracy, which provides an increased level of message traceability.

So what do the courts deem "delivered" in reference to e-mail?

While the US Postal Service deems First Class mail delivered if sent, this is not true of electronic mail. UETA stipulates that electronic messages can be judged "delivered" only if they can be shown to have arrived at the recipient's mail system. There are four e-mail confirmations messages, which mirror First Class postal delivery. They are: Opened (Recipient signed); Mailbox (assistant or colleague signed and put it on your desk); Mail Server (mail room acknowledged delivery by signing)

and Failure (no one signed for it). The four aforementioned analogous levels of delivery have been confirmed by case law under the UETA.

GRAY AREAS OF E-MAIL “DELIVERY”

Estimates of two-percent of Internet e-mails never reach their intended destination. This may be due to reasons such as lost data packets, a mistyped e-mail address, or an aggressive use of Spam filters on a recipient’s system. Just because a sender does not receive a “bounce” reply notice, does NOT mean that the e-mail was delivered. The reason for this is that many e-mail services are set such that a no “delivery status notifications” or “bounce” notice occurs so as limit an e-mail spammers’ ability to capture a valid e-mail address.

TRACKING SYSTEMS

There are today certain services that provide a notice of “opening” of an e-mail message some of the time. Simple Web-tracking (i.e. Web bugs) provide a low level of confirmation, but are limited. Typical software provides a text, or HTML, web receipt that cannot be easily authenticated. It also does not list the contents associated with the e-mail. Therefore, the challenge becomes to capture the dialog from the sender, associate it with the precise content and times of transmission, and interpret the server dialog so as to present a timely and easy-to-understand text for the sender.

Even though it is very difficult to intercept standard e-mail in transit, some look at using encrypted e-mail for additional privacy. However, encrypted e-mail is generally cumbersome and requires passing passwords or keys back and forth, which could also be intercepted if such is the concern. Further, with encrypted line connections, the e-mail is in plain text inside the sender or recipient’s organization leaving it vulnerable to manipulation.

Standard digital signatures require the purchase, installation, and management of a digital code (certificate) that is associated with a password, system, or smartcard. To be enforceable under US law, however, an electronic signature must possess THREE elements: A sound, symbol or process; attached to or logically associated with an electronic record, and; made with the intent to sign the electronic record. Hence, an electronic signature can be simple – a typed name, properly associated with an e-mail and with explicit intent is the simplest form of electronic signature. The challenge then is to provide this method “evidentiary value” such that it would conform to existing law.

REGISTERED E-MAIL (RPOST):

Software developed by RPost brings a new level of understanding to the issue. The sophisticated software provides legally valid proof of time and content sent and received, for any Internet address, without storing information or requiring compliant action by the receiver, and able to reconstruct the original e-mail. An e-mail message is generated and returned to the sender that provides evidence of the entire e-mail transaction, which is admissible in court. The RPost software actually aggregates the transmission information from the sender’s and receiver’s mail servers, interprets it, and produces an easy to read report. The information that is provided is returned to the sender within one business day and contains: proof of sending and receipt; proof of official time sent and received; proof of content (including attachments; re-constructs original content, delivery, and times).

WHAT’S IT MEAN TO CANADA?

The Ontario Provincial government is currently evaluating RPost to validate e-mail communications. Expect other Canadian government agencies to evaluate the technology as well.

CONCLUSION

More than twenty years ago Andrew S. Grove, Former Chairman of Intel Corporation, and one of the business world’s best visionary from the later part of the last century, wrote a slim book on the revolutionary change which e-mail brought to corporate America. E-mail improved delivery of information within an organization, and provided a means by which external communication could be carried out effectively throughout the value supply chain. This was a major process shift in productivity. With “evidentiary value” being added to e-mail, one may expect to see yet another step in the evolutionary process of productive business. Practicable goals are more rapid deal closure, sign-offs as required by by-laws, contracts, statutes, assurances, business confidence, and peace of mind.

REFERENCES TO E-TRANSACTION LAWS

The Uniform Electronic Transaction Act (“UETA”) and the Electronic Signatures in Global and National Commerce Act (“ESIGN”) define, in similar language, **“that a record or signature may not be denied legal effect or enforceability solely because it is in electronic form.”**¹ UETA goes further, affirmatively stating that **“if a law requires a record to be in writing, an electronic record satisfies the law,”** and both statutes state that **“if**

¹ UETA § 7(a).

a law requires a signature, an electronic signature satisfies the law.² These statutes guarantee e-mail messages the same legal weight and value as paper records. Indeed, courts have recently ruled that proposals tendered by e-mail can have the same force as written contracts,³ and that documents can be legally served by e-mail.⁴ To be enforceable under U.S. law, **E-SIGN** and **UETA** require that an electronic signature possess three elements:⁵ (1) A sound, symbol, or process, (2) attached to or logically associated with an electronic record, and (3) made with the intent to sign the electronic record.

In the case of *Shattuck v. Klotzbach*,⁶ the Plymouth Superior **Court determined that using e-mail, the two parties settled on the price of a house**; as the e-mail referred to the purchase and sale agreement that would be prepared. **All the e-mails exchanged by the two parties ended with the "typewritten" names of the senders.** The judge refused to dismiss the case because he believed that the parties' agreement to terms within an e-mail is in fact binding, even though there was no physical signature. The Court stated the following: **"Even though e-mail is in writing, most people still think of e-mail as an informal form of communicating. Now the Court is saying that it is a binding document."**

The relevance is that e-mail is binding without any special "digital signature" other than the author of the e-mail typing his or her name logically associated with the content of that e-mail.

While this decision and the enactment of UETA and E-SIGN are great news for those who wish to use electronic methods to conduct business, one must be able to prove delivery and authenticate the original content of the e-mail and attachments (i.e. original terms and conditions) in order to protect against a dispute over the terms of a contract sent via e-mail. **RPost Registered Receipt™ e-mails provide transaction parties with accountability, irrefutable proof of delivery and receipt, official time stamp and non-repudiation.**

Requirements for creation of electronic contracts are based on the Uniform Electronic Transactions Act (UETA), the E-Sign Act, among others.

A contract may be made in any manner sufficient to show agreement, including offer and acceptance, or conduct

that recognizes the existence of a contract.⁷ There are fundamental provisions in E-SIGN, UETA, and the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce that support the validity of electronic contracts.

E-SIGN provides that "a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation."⁸ Similarly, UETA provides that "a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation."⁹ Finally, the UNCITRAL Model Law on Electronic Commerce goes a bit further by providing both that "an offer and the acceptance of an offer may be expressed by means of data messages", and "where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose."¹⁰

An offer may be accepted "in any manner and by any medium reasonable in the circumstances."¹¹ Typical offline acceptances include written and oral communications, as well as acceptance by conduct. Their online counterparts include acceptance by e-mail or other form of electronic message, by electronic agent, and by conduct such as clicking on a button or downloading content.

Thus, if an offer is made by e-mail, one should be able to accept it by the same means.¹²

UETA provides that an electronic record is considered received only when it enters a computer system "that the recipient has designated or uses for the purpose of receiving electronic records of the type sent."¹³ Thus, if the parties have regularly corresponded in the past by e-mail, an e-mail acceptance sent to the offeror's e-mail address will presumably be effective.

UETA provides that the time at which an electronic record is considered to have been sent is the time that the record "enters an information processing system outside the control of the sender" (in the case where a message is sent from one computer system to another), or "enters a region of the information processing system designated or used by the recipient which is under the control of the

² UETA §§ 7(c) and 7(d). E-SIGN §101(a)

³ Nikoletta Banushi, "Can E-Mail Seal A Sales Deal?" Boston Globe, (March 16, 2002)

⁴ American Bar Association website (March 29, 2002)

⁵ **E-SIGN**, 15 U.S.C. § 7006(5) and **UETA** § 2(8) (definitions of "electronic signature").

⁶ Nikoletta Banushi, "Can E-Mail Seal A Sales Deal?" Boston Globe, (March 16, 2002)

⁷ UCC 2-204.

⁸ E-SIGN, § 101(a)(2).

⁹ UETA, § 7(b).

¹⁰ UNCITRAL Model Law on Electronic Commerce, Article 11(1).

¹¹ UCC 2-206(1)(a).

¹² It is well established that an acceptance may properly be sent by the same means as the offer, unless the offer says otherwise. See Restatement (Second) of Contracts § 65.

¹³ UETA § 15(b)(1).

recipient” (in the case where a message is sent from one person to another on the same system, such as where both parties are on AOL). An electronic record will be considered to have been sent as of that time, provided that it is addressed properly to an information processing system that the recipient has designated or uses for the purpose of receiving electronic records and from which the recipient is able to retrieve the electronic record, and provided further that it is in a form capable of being processed by that system.^{14 15}

Further, The U.S. National Archives and Records Administration Modern Records Program¹⁶ has provided the following guidelines for electronic records:

For a record to remain reliable, authentic, with its integrity maintained, and useable for as long as the record is needed, it is necessary to preserve its content, context, and sometimes its structure. A trustworthy record preserves the actual content of the record itself and information about the record that relates to the context in which it was created and used. Specific contextual information will vary depending upon the business, legal, and regulatory requirements of the business activity (e.g., issuing land use permits on Federal lands). It also may be necessary to preserve the structure or arrangement of its parts. Failure to preserve the structure of the record will impair its structural integrity. That, in turn, may undermine the record’s reliability and authenticity.

Non-repudiation is one of the essential security services in computing environments, being mainly applied in message handling systems and electronic commerce. The non-repudiation services that are being used in e-commerce can also be used in ascertaining the reliability of electronically-signed records. Non-repudiation services provide irrefutable evidence that an action took place. The services protect one party to a transaction (e.g., electronically signing a record) against the denial of the other party that a particular event or action took place. The services also provide safeguards that protect all parties from a false claim that a record was tampered with or not sent or received.

Similarly, the European Union Electronic Signature Directive requires member states to “ensure that an electronic signature is not denied legal effectiveness solely on the grounds that it is in electronic form.”¹⁷

In the European Union, the enforceability of electronic transactions is governed by the Electronic Signatures Directive adopted in 1999, and the Electronic Commerce

Directive adopted in 2000. Internationally, model laws governing the enforceability of electronic transactions have also been developed by the United Nations Commission on International Trade Law (“UNCITRAL”) Working Group on Electronic Commerce, which completed work on its Model Law on Electronic Commerce in 1996, and finalized and approved its Model Law on Electronic Signatures in 2001. These model laws have served as the basis for legislation enacted in several countries.

The term “electronic signature” means “an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.”¹⁸ Under the European Union Electronic Signature Directive, “electronic signature” means “data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.”¹⁹

The term “transaction” is defined in the E-SIGN Act as “an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons, including any of the following types of conduct: (A) the sale, lease, exchange, licensing, or other disposition of (i) personal property, including goods and intangibles, (ii) services, and (iii) any combination thereof; and (B) the sale, lease, exchange, or other disposition of any interest in real property, or any combination thereof.”²⁰ UETA defines “transaction” as “an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.”²¹

Each of these legal definitions and statutes support the RPost Registered E-mail® service’s basis of enabling a legal electronic transaction. Each support the use of RPost® Registered E-mail® for electronic signature, service, delivery, time, non-repudiation and content authentication, for offers, counter-offers, and acceptance of offers in transactions.

This report is not legal advice, but is an analysis of the application of existing legal principles regarding e-commerce to business communications. If you have any questions as to how these principles apply to you or your transactions or business, you should consult qualified legal advice.

¹⁴ UETA § 15(3).

¹⁵ UETA § 15(a)(1) and 15(a)(2).

¹⁶ The National Archives and Records Administration, Policy and Communications Staff, Office of Records Services, Modern Records Program, Washington, D.C.

¹⁷ Electronic Signature Directive, Article 5(2)

¹⁸ E-SIGN, 15 U.S.C. § 7006 (5); UETA § 2(8).

¹⁹ Electronic Signatures Directive, 1999/93/EC (13 December 1999), Article 2(1).

²⁰ E-SIGN, 15 U.S.C. § 7006(13).

²¹ UETA § 2(16).