

REGISTERED E-MAIL[®] AND THE LAW

ABSTRACT

This memorandum discusses RPost[®] Registered E-mail[®] technology and its relevance to the legal status of e-mail communications. Despite recent legislation guaranteeing electronic messages the same legal status as paper documents, email messages can be legally worthless if their receipt or content is disputed. RPost[®] Registered E-mail[®] technology offers a solution to this problem by providing proof of content and delivery.

RPOST[®] TECHNOLOGY

The RPost[®] Registered E-mail[®] system provides the sender of an e-mail message with an electronic Registered Receipt[™] e-mail that documents the message's delivery. The receipt includes a "digital fingerprint" of the message that can be used to prove the exact content of the original message and its attachments. The Registered Receipt[™] e-mail itself is a digitally sealed, counterfeit-proof document whose contents can be authenticated by e-mailing it to an RPost[®] address.

The system works with any e-mail program. No special software is required to receive Registered E-mail[®] message and neither the sender nor the receiver need any special hardware. A small change to the corporate mail server or a light desktop software plug-in allows anyone or selected people in the company to send Registered E-mail[®] messages. The sender can opt to send Registered E-mail[®] messages from their regular e-mail programs.

Registered E-mail[®] can provide proof of delivery to any Internet address. Unlike other systems that attempt to confirm delivery, Registered E-mail[®] messages do not require the recipient to take any action to acknowledge receipt.

THE LAW¹

In the United States, the enforceability of electronic transactions is governed by the Electronic Signatures in

Global and National Commerce Act ("**E-SIGN**"),² a federal law enacted in 2000 that largely preempts inconsistent state law,³ and the Uniform Electronic Transactions Act ("**UETA**"),³ a uniform state law that was finalized by the National Conference of Commissioners on Uniform State Laws ("NCCUSL") in 1999 and has now been adopted by 40 states. In the European Union, the enforceability of electronic transactions is governed by the Electronic Signatures Directive adopted in 1999,⁴ and the Electronic Commerce Directive adopted in 2000.⁴

The force of these statutes is to remove barriers to the use of electronic transactions and to stipulate that electronic records and electronic signatures cannot be denied legal effectiveness solely on the ground that they are in electronic form.

Thus, **E-SIGN** states that, notwithstanding any other rule of law, "a signature, contract, or other record relating to [a] transaction . . . may not be denied legal effect, validity, or enforceability solely because it is in electronic form."⁵

Likewise, **UETA** provides that "a record or signature may not be denied legal effect or enforceability solely because it is in electronic form."⁶ **UETA** goes further, affirmatively stating that "if a law requires a record to be in writing, an electronic record satisfies the law", and "if a law requires a signature, an electronic signature satisfies the law."⁷

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 . . .".⁸

² Electronic Signatures in Global and National Commerce Act (hereinafter "**E-SIGN**"), S. 761, P.L. 106-229, 15 U.S.C. 7001 *et. seq.*, effective October 1, 2000.

³ Uniform Electronic Transactions Act (hereinafter "**UETA**"), approved by the National Conference of Commissioners on Uniform State Laws (NCCUSL) on July 23, 1999. A copy of **UETA** is available at www.law.upenn.edu/bll/ulc/fnact99/1990s/UETA99.htm.

⁴ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (hereinafter "Electronic Commerce Directive"); available at www.europa.eu.int/ISPO/ecommerce/legal/documents/2000_31ec/2000_31ec_en.pdf.

⁵ **E-SIGN**, 15 U.S.C. § 7001(a).

⁶ **UETA** § 7(a).

⁷ **UETA** §§ 7(c) and 7(d).

⁸ Electronic Signature Directive, Article 5

¹ For a more comprehensive discussion of the legal issues readers should see "The Legal Requirements for Creating Secure And Enforceable Electronic Transactions" by Thomas J. Smedinghoff. Available at <http://www.bmck.com/ecommerce/article-electronic-transactions2.doc>.

THE LIMITS OF CONVENTIONAL E-MAIL

These pieces of legislation 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 contracts⁹; that documents can be legally served by e-mail¹⁰ and that medical prescriptions can be submitted by e-mail.¹¹

But e-mail still has its limitations as a vehicle for legally binding communications. Thus, in the case of *Rio vs. Rio* the 9th circuit court of appeals ruled that Rule 4(f)(3) of the Federal Rules of Civil Procedure permits a variety of methods for process of service, and that e-mail was appropriate. But the justices noted that e-mail service is not without problems and limitations, if it can't be ensured that the e-mail was received (via a confirmation notice) or the content cannot be verified.¹²

Indeed, every case in which the status of e-mail communications have been upheld by the courts has been one in which there has been *no dispute* among the parties about the delivery, timing or content of the messages.

For legal purposes United States Postal Service (USPS) mail is presumed to have been delivered if sent. That this is so is testament to general confidence in the reliability of the U.S. Postal Service. But, the **E-SIGN** bill notwithstanding, this confidence is unlikely to be extended to e-mail any time soon.

E-mail is often not delivered. Indeed, an estimated two to ten percent of all Internet e-mail communications fail for some reason or other and senders are often not aware of failures.¹³

⁹ Nikoletta Banushi, "Can E-Mail Seal A Sales Deal?" Boston Globe, (March 16, 2002)

¹⁰ American Bar Association website (March 29, 2002)

¹¹ Arent Fox, Attorneys at Law case files, (February 19, 1998); Available from World Wide Web @ http://www.arentfox.com/quickGuide/businessLines/telemed/e-health_telemed/e-health_lawsRegs/caselaw/walqvwisc.html

¹² American Bar Association website (March 29, 2002); available from the World Wide Web @ <http://www.abanet.org/journal/ereport/m29email.html>

¹³ Wall Street Journal: On Friday, the Wall Street Journal reports that executives at Warner Music alerted employees that 2% of the e-mail in their AOL Time Warner system was being lost... it goes on to quote their memo as saying "if you are expecting critical e-mail, you may want to follow up with the sender." The article also mentions that the AOL e-mail issue has led more people to send via Fed Ex for delivery confirmation. [Matthew Rose and Martin Peers, "AOL's Latest Internal Woe: 'You've Got Mail' - 'Oops, No You Don't", Wall Street Journal, (March 2002)] The largest ISP in Quebec reports losing 10,000 e-mails and their spokesperson's response was that "they might lose some

In recent years these numbers have been getting worse not better as a result of the proliferation of "spam filters" added to systems to block junk email. None of these systems is perfect and when they fail they can block the delivery of important communications.

Most e-mail programs allow users to "request a receipt" for outbound messages. But, as a matter of internet regulation,¹⁴ neither recipient mail servers nor mail clients can be forced to generate a receipt and, in fact, only about 25% of mail clients are configured to return receipts if connected. In any case, the receipts received by such methods are simple text e-mails that can be readily counterfeited and easily disputed.

Even when messages are delivered and receipt is acknowledged it remains possible to dispute their contents. Anyone with the capacity to receive an e-mail is in a position to effortlessly and undetectably alter its contents, a situation which has no analogy in the world of hardcopy mail.

There do exist systems of digital signature that allow messages to be rendered tamper proof. But it is not often noticed that these systems, while they must be undertaken (and paid for) by the *sender*, protect only the *recipient*. That is, they provide the recipient with means for proving that a received message had a certain content, but they do not provide the sender with the means of proving that a message with a certain content was sent.

For this reason, users who must be certain of delivery, or who are statutorily bound to deliver messages and to prove that they have delivered them, are likely to be reluctant to trust ordinary e-mail.

RPost[®] technology offers to remedy this situation. RPost[®] technology provides a method by which the senders of e-mail can have proof:

- that a message was sent
- that the message was delivered
- precisely when the message was delivered to each recipient
- that the message had a specific content.

Further, RPost[®] technology provides this proof in a form that satisfies the requirements of the governing laws.

again - we're not sure." There is no current way to know whether a subscriber's e-mail has been lost. [Canada Gazette, March 2002]

¹⁴ RFC 1891

PROOF OF DELIVERY

UETA provides that an electronic record is considered received by the intended recipient when it enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records of the type sent and from which the recipient is able to retrieve the electronic record, and is in a form capable of being processed by that system.¹⁵

In the case of e-mail, this provision means that an electronic message is delivered once delivered to the e mail server authorized¹⁶ to receive mail for the recipient's address. This might be a corporate mail server or the server of the Internet Service Provider that manages the individual's (POP) mail account.

It is important to note that an e-mail message is considered received even if no individual is aware of its receipt. That is, as with first class mail or indeed, USPS registered mail, once the message is delivered it makes no difference whether or not the addressee actually opens it.

To understand this provision it may help to compare United States Postal Service registered hardcopy mail. USPS registered mail must be signed for upon delivery. But USPS registration does not guarantee delivery to the *person* to whom the mail is addressed. What the Postal Service guarantees is delivery to the addressee or the addressee's "authorized agent". That is, an agent authorized to receive mail on behalf of the person to whom the mail is addressed. Thus, a mailroom clerk, a secretary, a wife, a parent; indeed, almost anyone answering the postman's knock at a recipient's address, can sign for a registered message. In effect, UTEA treats the operator of the recipient's mail server as the authorized agent for the receipt of mail.

UETA's criterion for delivery has been adopted in the electronic service of bankruptcy notices. US Courts Federal Bankruptcy Rule 9036 allows bankruptcy notifications to be sent by email only provided that the sender can obtain "electronic confirmation that the transmission has been received."¹⁷ The U.S. Courts Bankruptcy Notification Center treats this condition as satisfied provided that the recipient's mail server is

configured to send some form of acknowledgement of receipt.¹⁸

If delivery to mail server is delivery, proof of delivery must prove delivery to the recipient's mail server. What counts as such proof?

It is sometimes possible, with conventional e-mail technology, to elicit some form of acknowledgment of receipt from a receiving mail server or mail client. But these techniques work only some of the time, and, when they do, the best they can supply the sender with is a plain text e-mail acknowledgment that is easily forged or altered.

RPost's[®] patent pending technology proves delivery by recording the transactions between the RPost[®] server and the recipient's mail server as each message is delivered. These transactions are a dialog conducted in the Simple Mail Transport Protocol¹⁹ (SMTP) that governs all Internet e-mail communications. This English language protocol requires the recipient mail server to:

- identify itself
- declare itself prepared to accept mail on behalf of a named recipient
- acknowledge when the mail has been successfully received.

By recording the SMTP dialog, the RPost[®] system can document the recipient mail server's declaration of accepting the mail, or "sign off." For each delivered message, a transcript of the dialog is included in each RPost[®] Registered Receipt[™] e-mail receipt in addition to other information comprising an audit trail of the message's delivery. Since all Internet mail is delivered via SMTP, the RPost[®] system can provide proof of delivery to any Internet destination.

PROOF OF SENDING

Proving that a message has been sent is different from proving that it has been delivered. Sending a message may satisfy statutory or contractual requirements even if the message is, in fact undeliverable. Indeed, proof that a message has been sent and delivery attempted may be all the more important if it cannot, in fact, be delivered.

The presence of a message in the "sent" folder of an e-mail program cannot constitute proof of sending. Most mail programs allow messages to be transferred to the sent folder without being transmitted and for messages to be freely edited within the "sent" folder.

¹⁸ cf.

http://www.ebnuscourts.com/phase2/Phase2_emailpage.htm

¹⁹ The Simple Mail Transfer Protocol is defined in RFC 821 available at <http://www.faqs.org/rfcs/rfc821.html>.

¹⁵ **UETA** § 12(a); **E-SIGN**, 15 U.S.C. §7001(d)

¹⁶ Every internet email domain name has associated with it the internet name and addresses of an e-Mail eXchange Server (MX-server). The MX server is the official "Mail Transport Agent" for addresses in the domain. The name of the MX server(s) for every domain name is broadcast, daily, throughout the internet

¹⁷ Cf. <http://www.gamb.uscourts.gov/fedr/bank5e7l.htm> (2003)

UETA provides that a message is considered to have been sent when it “enters an information processing system outside the control of the sender”.²⁰ Whether the message can be further considered “sent to a particular recipient” is a matter of whether the sender knows, or has good reason to believe, that the address used is that of the recipient.²¹

If a recipient submits a particular email address to the sender in the course of business, and the sender and receiver maintain a business relationship, the sender has “good reason to believe” that this is the current address of the intended recipient. If the sender can document a delivery failure to such an address, then sending a message with a documented delivery failure may satisfy statutory or contractual requirements even if the message is, in fact undeliverable.

By these standards, a message would count as sent if it were transmitted to the sender’s Internet Service Provider (ISP) for relay on to its subsequent destination. Note, though that in the normal course of events, the sender does not have proof of such transmission. In the case of corporate users, where organizations typically control their own mail server, messages could not be said to have passed to systems “outside the control of the sender” if they are not delivered to their destinations. In such an environment no message can count as sent *unless* it is delivered.

Under the provisions of **UETA**, RPost® receipts constitute proof of sending even if the receipts report a failure of delivery. The receipts record the arrival of a message at the RPost® System, which is outside the control of the sender or recipient.

TIME STAMPING

When a message was sent and when it was delivered can be crucial and the precise measurement of these times can be critical. Thus, in matter of *Bowmen Inc.*²² the U.S. Comptroller General’s office held that a faxed document had not be submitted in time because the transmission was not completed (even though it had begun) before the deadline.

UETA provides that:

- the time at which a message is sent is the time at which it enters an information processing system not in control of the sender.

²⁰ **UETA** § 15(3).

²¹ **UETA** § 15(a)(1) and 15(a)(2)

²² *Bomen Inc.*, Comp Gen B-234652, May 17, 1989, 3 CGEN (CCH) ¶ 103, 198 (1989) (23 page fax started, but not completed, before the deadline).

- the time at which a message is delivered is the time at which it enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic messages.

Note that, for the purposes of proving time of delivery or sending, the time stamps displayed on e-mails indicating time of sending or receipt are valueless since they are entirely dependant on the clocks of the sender’s and recipient’s desktop computers and hence are highly inaccurate and easily manipulated.

RPost® Registered Receipt™ e-mails record both the time at which a message is received by the RPost® system from the sender and the time at which the message was delivered to each of its destination servers.

The RPost® system time is continuously set via Global Positioning Satellite (GPS) timing controlled by the National Institute of Technology Standards Atomic Clock in Boulder, Colorado. The system is accurate to one second in twenty million years.

RECORD RETENTION REQUIREMENTS

The **E-SIGN** act encourages electronic record storage by providing that any statute, regulation, or other rule of law that requires the retention of contracts or other records relating to transactions in or affecting interstate or foreign commerce may, with certain exceptions, be complied with by storing the documents electronically. However, the Electronic Signatures Act requires that the electronically stored documents must *accurately* reflect the information in the contracts or transactional records and be *accessible*²³ to all persons entitled to review them under statute, regulation, or rule of law in a form that is capable of being accurately reproduced for later reference.²⁴

RPost® Registered Receipt™ e-mail provides, not only an efficient and secure method for recording delivery and transmission data, but also a reliable and accessible method of storing and managing mailed documents.

An RPost® Registered Receipt™ e-mail is more than a claim that a message was delivered. Each receipt contains an audit trail of evidence and records collected from the recipient’s mail server, mail system and email client program. Receipts contain:

²³ **UETA** § 12(a); **E-SIGN**, 15 U.S.C. §7001(d). **E-SIGN** requires that the stored electronic record remains accessible to all persons who are entitled to access by statute, regulation, or rule of law, for the period required by such statute, regulation, or rule of law, in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.

²⁴ **E-SIGN** 15 U.S.C. § 7001(d)(3); **UETA** § 12(d).

- Sender's name and e-mail address
- The names and email addresses of each intended recipient
- The time the message was received by the registration server
- The time the message was delivered to each recipient
- A unique network identifier for each message
- The delivery status of the message to each destination (e.g. "Delivered to Mailbox", "Opened")
- Details of the delivery of each message (typically: the name of the recipient server)
- Transcripts of server-to-server delivery transactions
- The digital fingerprint of the message
- The size of the message
- The subject of the message
- The file name and size of each attachment of the message together with their digital fingerprints
- Delivery Status Notification messages sent by receiving mail servers
- Opening receipts sent from recipient mail records
- Hyper Text Transport Protocol (HTTP) records recording opening of messages
- A copy of the original message together with all of its attachments

The records are all stored in compressed encrypted and tamper-detectable form within the receipt.

Anyone who wishes to authenticate the information contained in an RPost[®] Registered Receipt[™] e-mail can forward a copy by e-mail to the RPost[®] Registration Networks[™] at the address "verify@rpost.net". Provided that the receipt has not been tampered with, an authenticating message will be returned with a regenerated original e-mail attached. The record can be reproduced or printed like any other e-mail or attachment.

Because RPost[®] receipts are themselves, e-mail messages, they can be made readily accessible to any interested parties. At the same time, RPost's[®] methods of authentication and tamper proofing mean that any holder of an RPost[®] receipt can independently confirm precise content of the original message and its delivery history.

RECORD CONFIDENTIALITY

In many business contexts it is important that records be maintained confidentially and there are circumstances in which it may be required that records be permanently destroyed. In this connection it is important to note that once the sender of a Registered E-mail[®] message is sent a receipt (never more than a few hours after the message is sent) The RPost[®] system deletes all copies of the message and its attachments. The holder of the receipt is the only one who can authenticate the message's contents or delivery.

REPLY REGISTERED[™] AND ONLINE CONTRACTING

It is well established that an acceptance may properly be sent by the same means as the offer, unless the offer says otherwise.²⁵ E-SIGN and UETA extend this principle to offers and acceptances conveyed by electronic means. In this connection RPost's[®] "Reply Registered[™]" feature is of special interest.

This feature allows a recipient of a registered message to reply with a Registered E-mail[®] message even when that recipient does not subscribe to the RPost[®] service.²⁶ The receipt for this reply is copied to the replying party and the sender of the original message. Replies to registered replies are, in turn, sent registered and both parties are copied with a receipt. In this way, both parties to an e-mail negotiation can be provided with an authenticatable and non-repudiatable record of the history and content of an extended correspondence.

DIGITAL SEAL[™] AND ELECTRONIC SIGNATURE

The RPost[®] service makes available to its subscribers the option of *digitally sealing[™]* a Registered E-mail[™] message. Digital Sealing[™] is a method of electronic signature.

Electronic signatures, like handwritten signatures, can serve a variety of purposes.

- **Expression of Intent** – A signature evidences the signer's intent with respect to the document signed. A signature may, for example, signify an intent to be bound to the terms of a contract, the approval of a subordinate's request for funding of a project, authorization to a bank to transfer funds, confirmation that the signer has read and reviewed the contents of a memo, an indication that the signer was the author of a document, or merely that the contents of a document have been shown to the signer and that he or she has had an opportunity to review them.
- **Satisfaction of Legal Requirements** – A signature is often used to satisfy a law or regulation that requires the presence of a signature before the document will be considered legally effective.
- **Security** - Signatures often function as a security device. That is, signatures can be used (1) to authenticate a document (i.e., to identify the signer

²⁵ Restatement (Second) of Contracts § 65

²⁶ Typically, a user of the RPost service will direct a message to be sent registered by including a "(R)" at the beginning of the messages subject line. By writing "(R+)" the sender can send the message so that its reply will be registered.

and indicate that such person is the source of, or has approved, the document), and/or (2) to ensure the integrity of the document (i.e., to ensure that the document has not been altered since it was signed).

Traditionally, under U.S. law, any symbol that is made with the intent to sign a document can qualify as a legally valid signature.

Both **E-SIGN** and **UETA** extend this basic approach to the concept of an electronic signature. To be enforceable under U.S. law, they require that an electronic signature possess three elements:²⁷

- A sound, symbol, or process,
- Attached to or logically associated with an electronic record, and
- Made with the intent to sign the electronic record.

Electronic signatures that meet these requirements are considered legally enforceable as substitutes for handwritten signatures for most transactions in the United States.²⁸

E-SIGN and **UETA** recognize that there are many different methods by which one can “sign” an electronic record. But the most commonly acknowledged forms of electronic signatures are so called “digital signatures” that employ asymmetric encryption technologies and rely on the Public Key Infrastructure (PKI). It will be useful then to compare RPost’s[®] patent pending method of digital sealing with PKI digital signatures.

DIGITAL SIGNATURES VS. DIGITAL SEALS™

To digitally sign a message using PKI, the sender must possess a private encryption key usually purchased from a vendor recognized as a PKI certificate authority and must have an e-mail client program capable of carrying out the signing process. In the signing process, the sender’s software computes a digital digest or “hash” of the contents of the message and encrypts this information, together with other information identifying the sender, using the sender’s private encryption key. The encrypted information is included as an attachment to the message. To “read” the signature the recipient’s mail program must be able to apply the senders’ public encryption key to decrypt the attachment, extract identifying information

²⁷ **E-SIGN**, 15 U.S.C. § 7006(5) and **UETA** § 2(8) (definitions of “electronic signature”).

²⁸ See **UETA** §§ 2(8) and 7(d) and **E-SIGN**, 15 U.S.C. § 7001(a) and 7006(5). The European Union Electronic Signature Directive also uses a similar definition of an electronic signature. Electronic Signature Directive, Article 2(1).

about the sender and compare the decrypted digital digest with a digital digest of the received message. In addition to asymmetric cryptographic algorithms, PKI systems typically employ a one-way hashing algorithm (most commonly SHA-1) and a symmetric encryption algorithm (most commonly the Data Encryption Standard (DES) or the enhanced 3DES).

There are several shortcomings with such a system:

- The system requires that the recipient possess software capable of performing the necessary cryptography. Some of the most commonly used mail clients, e.g. web based mail clients, lack this capacity. The method is not *universal* among e-mail clients.
- When a message is “digitally signed” in this manner *any* change to the body of the message, however innocent, will result in a failure to authenticate. For example, the changes typically introduced into a message by forwarding it from most e-mail clients will change the message’s digest and will result in a failure to authenticate. PKI digital signatures are, in this sense, not *robust*.
- Finally, when a message fails to authenticate because it has changed, it is for all practical purposes, impossible for the recipient to know which portion of the message has changed or to reconstruct the original message. The method is not *resilient*.

These shortcomings are fraught with legal consequence. The lack of universality raises issues about the force and value of a digitally signed document when served to a recipient who lacks the software or encryption keys required to authenticate it. The fact that digitally signed messages are not robust or resilient means that inconsequential and inadvertent changes to the text of a message could wholly and irreparably void the document’s signature.

The RPost[®] Digital Sealing™ service is done at the RPost[®] Registration Networks™. The user need have no special software on his or her desktop machine. Users are not required to possess any cryptographic keys. Having received an e-mail message from the sender over a secure connection, the RPost[®] server computes a digital digest of the message, encrypts it together with an identification of the sender and incorporates it into an HTML (digitalseal.htm) file that is attached to the message. This file, which can be read by most mail clients and all web browsers, identifies the sender of the message and invites any recipient who doubts its provenance or the authenticity of its contents to forward the message by e-mail to the RPost[®] Registration Networks (at address verify@rpost.net). When the message is submitted to the RPost[®] Registration Networks, the digital seal is decrypted. Provided that neither the seal nor the other attachments of the message have been tampered with,

The RPost[®] system returns a message that identifies the original sender and attaches a reconstructed copy of the original message.

The RPost[®] system is *universal* in the sense that it does not require the recipient to possess any specialized software or to possess any cryptographic keys to authenticate the message. Any recipient capable of sending or receiving Internet mail can authenticate a digitally sealed message.

Unlike digitally *signed* documents, digitally *sealed*[™] documents are *robust* insofar as they can be forwarded and reformatted without destroying their ability to be authenticated. Moreover, because the authentication of a digitally sealed message can, in many cases, reconstruct the original message even if the circulated copy has become corrupted, digitally sealed messages are *resilient*.

Digital Sealing[™] uses a subset of the same algorithms used by digital signature technology (specifically, 3DES and SHA-1). The cryptographic soundness of these algorithms is universally recognized.

IS ENCRYPTION NECESSARY?

While the RPost[®] system uses cryptographic techniques to protect its receipts and seals, the system does not encrypt the contents of registered messages themselves. Given widespread worries about Internet security it might be wondered whether confidential and sensitive information can be trusted to unencrypted e-mail.

The American Bar Association has recently addressed this and has issued a Formal Ethics Opinion stating, "A lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct (1998) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint. The same privacy accorded U.S. and commercial mail, land-line telephonic transmissions and facsimiles applies to Internet e-mail".²⁹

In any case, the RPost[®] system is compatible with additional methods of encryption that users may wish to adopt. Further, one should note that all e-mail systems at their most basic level requires each receiver to have a unique and private password and username to view e-mail.

RPOST[®] ENCRYPTION AND SECURITY

The hash algorithm used in this software is SHA-1 (Secure Hash Algorithm). This was developed by the U.S. National Security Agency and published by the National Institute of

Standards and Technology (NIST). NIST issued FIPS PUB 180-1 (Federal Information Processing Standard Publication) describing the SHA-1 standard. This specifies the SHA-1 standard for federal requirements and encourages the use in private and commercial applications. The standard was released with the approval of the Secretary of Commerce in 1995. SHA-1 is a standard algorithm used in government communications and is court tested and ISO compliant. The hash algorithm takes in one or more blocks of 512 bits and produces a 160-bit hash value.

The cryptography techniques used in this software are implemented using the Microsoft CAPICOM (version 2.0) libraries. The CAPICOM COM client provides services that enable application developers to add security based on cryptography to applications. CryptoAPI includes functionality for authentication using digital signatures, for enveloping messages, and for encrypting and decrypting data. RPost[®] encryption uses Microsoft CryptoAPI 2.0 NIST FIPS-141-1 validated instances of the SHA-1 and 3DES (triple DES) algorithms.

RPost's[®] physical and network facilities have been inspected and certified by the U.S. Government as meeting Federal Standards for the handling of critical and confidential messages.

U.S. Government inspectors, TRW Information Systems Security Officers, and PriceWaterhouseCoopers have certified that the RPost[®] Registration Networks[™] comply with industry best practices for network security, availability, and business procedures.

The United States General Services Administration (GSA) has approved the RPost[®] Registered E-mail[®] product and pricing and AT&T, Sprint, and Qwest's government divisions offer Registered E-mail[®] messages for acquisition through the GSA Information Technology Federal Service Supply Schedule 70.

AT&T certifies the availability of the Registered E-mail[®] service for AT&T customers.

The RPost[®] Registered E-mail[®] system has been formally accepted by the largest State Bar associations for attorney education credits, including the California, Texas, Virginia, Florida, and Tennessee State Bar Associations.

RPost[®] technology is patent pending. "RPost[®]", "Registered E-mail[®]", "(R)egistered E-mail[®]", "Registered Receipt[™]", "(R)[®]", "(R)egistered Receipt[™]", and "(R)eceipt" are among the trademarks owned by RPost[®]. Further information is available on the Internet at www.rpost.com or by e-mail at info@rpost.com.

²⁹ ABP Formal OP 99-413