LOCKE LORD BISSELL & LIDDELL LLP

# CONFIDENTIAL MEMORANDUM

**Date:** October 20, 2007

**To:** Zafar Khan, Chief Executive Officer

**From:** Jon Neiditz, Pat Hatfield, Jay Safer and Amanda Witt

**Subject:** Legal Review of RPost Registered E-mail® service in context of Electronic Law relative to Authentication / Admissibility Requirements.

---

This Memorandum is written in response to your request that we provide our analysis of the authentication and admissibility of the texts of e-mails and the content of their attachments, as well as of evidence of their sending and legal receipt and the time of sending and receipt, using RPost's Registered E-mail® service, in court proceedings in the United States. Given rapid developments in the law relating to the treatment of electronic documents, the admissibility of a particular document should always be examined against the latest precedents and other authorities in the governing jurisdiction in which admission is sought. That said, our review indicates that RPost's Registered E-mail® service has been carefully constructed in light of the evolving law, including applicable U.S. legal treatment of electronic message transmissions, information security and the admissibility of electronic evidence. Based on the description of the RPost Registered E-mail® service set forth in the Statement of Facts below, the use of that Service can contribute significantly to the admissibility of the elements in question.

The ease of replication and modification of electronically stored information ("ESI") and the openness and decentralization of networks, systems and the Internet pose challenges for establishing and maintaining custodianship of electronic documents. Thus organizations may have difficulty finding a credible custodian with firsthand knowledge of the process followed to create, execute, preserve, send and receive ESI, or to generate or recreate that ESI when it is to be proffered as evidence. By the same token, organizations face a significant challenge in rendering ESI secure against tampering immediately and continuously after the relevant event, such as creation or receipt. Typically, organizations have attempted to achieve such security through layers of protections, such as firewalls, passwords and other peripheral and access controls. However, as systems, databases, peripherals, access devices, and technology in general evolve, and as companies or blocks of documents are sold, merged, converted, migrated or updated, these layers of controls often lose their effectiveness and increase in cost with the addition of new controls.

ESI also presents opportunities for authentication in ways that paper documents do not. For example, ESI can be created with its own internal controls, as in the cases of digital rights management and certain kinds of encryption. Unlike the peripheral controls described in the previous paragraph, these internal controls are not as dependent on the information systems that contain them, so their maintenance over time is less prone to failure and increasing expense. In addition, and more importantly, the criticality of protecting ESI against the very substantial risk (in relation to secured paper documents) of tampering is diminished by the ability to detect tampering instantaneously through the use of devices such as "hash" algorithms, as long as one trusted original

or hash value can be maintained securely.[1] RPost's Registered E-mail® service takes advantage of these opportunities for data-level controls and tamper detection.

As used herein, "UETA" means the Uniform Electronic Transactions Act, as published by the National Conference of Commissioners on Uniform State Laws, and "ESIGN" means the Electronic Signatures In Global and National Commerce Act, 15 U.S.C §70001 et. seq.

## I. STATEMENT OF FACTS

### A. High-Level Summary of RPost Registered E-mail® Technology

RPost® technology creates an encrypted record of information including the following:

1. that a message was sent;
2. that the message was received by the recipient's server;
3. precisely when the message was sent to and received by to the recipient's server; and
4. that the message and its attachments had a specific, replicable content.

In this memorandum, we rely upon the facts provided to us, that are summarized in this Statement of Facts. We also implemented and used the core RPost® product described in this Statement of Facts, but did not oversee an independent technical evaluation of the product.

RPost® uses Public Key Infrastructure ("PKI") digital signature technology and RPost® Digital Seal™ technology, which is also based upon PKI cryptography, to verify content of data contained in the e-mail delivered to the recipient. The RPost® Digital Seal™ technology computes a digital digest of the message, encrypts it together with an identification of the sender and incorporates it into an HTML file that is attached to the e-mail message. This file, which can be read by most e-mail clients and all web browsers, identifies the sender of the message and allows any recipient who questions the authenticity of the record to verify the contents of the file by forwarding the message by e-mail to the RPost® system. When the message is submitted to the RPost® system, the Digital Seal™ is decrypted and hashes are compared to determine integrity of content. Provided that neither the Digital Seal data file nor the other attachments of the e-mail have been altered, the RPost® system returns a message that identifies the original sender and original official time of transmission, and attaches a reconstructed copy of the original message and attachments. Where alteration has occurred, the returned Authentication Receipt™ will so indicate.

Two types of evidence provided by RPost's Registered E-mail® service that are particularly significant legally are evidence of receipt and of the content of the e-mail delivered. Evidence of receipt is achieved under UETA as described below 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 Protocol (SMTP) that governs all Internet e-mail

[1] A "hash" function is a one-way function that accepts a digital string of characters and computes a fixed-length output value based on the entire string. The hash computation is a unique function of its input in the sense that changing any character of the input changes the hash, but it possesses no inverse - the input cannot be constructed knowing the hash output except by trial and error.

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 and acknowledge when the mail has been successfully received. RPost® creates a record of the recipient mail server's declaration of accepting the mail, or "sign off." For each delivered message, a transcript of the dialogue is included in each Registered Receipt™ in addition to other information, comprising an audit trail of the message's delivery. Since all Internet mail is delivered via SMTP, RPost® is able to record delivery in this fashion to any Internet destination. Proof of the content sent is achieved, without RPost® storing the content in question, through the use of cryptography meeting industry standards. RPost®'s technology may be more fully described as follows:

The RPost Registered E-mail® system creates a record of the delivery of electronic messages by providing the means for the sender to transmit messages through a server controlled by RPost®. The server, acting as a mail transport agent, receives a message from a sender to be sent to a recipient or recipients. For each intended recipient of the message: the server adds to the message, in formats recognized by various e-mail client programs, message headers eliciting delivery notifications from recipient's e-mail clients, where the e-mail address in the headers to which the notification is requested to be sent is an e-mail address controlled by RPost® and not the return address of the Sender of the message. The e-mail address embeds identifiers that uniquely identify the message and the particular recipient of the message.

The server determines the MX (Mail Exchange) server for the recipient's e-mail address and connects to the server employing widely-used protocols. Using these protocols, the server attempts to deliver the message to the recipient's Mail Exchange server and in doing so records, following recognized protocols, the dialogue between the two servers including that portion in which the receiving server accepts or refuses delivery of the message for the recipient.

Having attempted to deliver the message to each of its intended recipients and waited for a period sufficient to collect various forms of failure and delivery notifications from recipient mail servers, mail clients, and Internet protocols, the RPost® system prepares a report which indicates the delivery status of the message for each recipient.[2] A copy of this report is sent to the sender as the Registered Receipt™ e-mail. The record that contains all notifications and transaction records relevant to the delivery of the message is attached to the Registered Receipt™ as is the data that is a representation of the Sender's original message as it was received by the server. All attachments to the Registered Receipt™ are packaged with Digital Seal technology and/or encrypted and digitally signed by RPost®. This method of cryptographic integrity protection allows anyone in possession of the Registered Receipt™ to verify the authenticity of the data it contains by sending a copy of the Registered Receipt™ to an e-mail address controlled by the agent where cryptographic methods are used to determine if information in the Registered Receipt™ has been altered. If the cryptographic method used to authenticate the Registered Receipt™ determines that the information in the Registered Receipt™ has not been altered, then RPost reconstructs an authenticated copy of the Sender's original message -- including attachments -- as it was received by the server along with an

[2] RPost® marketing materials describe this process usefully as follows: "Just as a courier or postman may gather objective evidence of delivery by recording the dialog with the recipient's agent (i.e. mail room or assistant), the Registered E-mail® service gathers objective evidence of delivery by recording the dialog with the recipient's e-mail agent (i.e. mail server of record) and interprets this information for the sender using proprietary algorithms."

authenticated delivery analysis, authenticated official times of sending and receipt, and all authenticated notifications and transaction records relevant to the delivery of the message. This authenticated information and analysis is returned by RPost® to the sender (or to the party requesting authentication by having submitted the Registered Receipt™ e-mail to RPost®) in the form of an Authentication Receipt™ e-mail.

After the Registered Receipt™ e-mail is returned to the original Sender by RPost®, RPost® does not retain the original e-mail message and does not retain any representation or hashes of the original message, or transmission information of the original e-mail, obviating the possibility of unauthorized access to the e-mail via RPost® servers. RPost® keeps only the cryptographic keys as described below.

The Registered Receipt™ e-mail and the Authentication Receipt™ e-mail 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 received by each of its destination servers. The RPost® time is continuously set via Global Positioning Satellite (GPS) timing controlled by the National Institute of Standards and Technology (NIST) Atomic Clock in Boulder, Colorado, also known as NIST-F1, a cesium fountain atomic clock that serves as the United States' primary time and frequency standard. As of the summer of 2005, it was so accurate that it will neither gain nor lose one second in more than 60 million years.[3]

All of the data in the RPost® Registered Receipt™ and Authentication Receipt™ are protected by RSA/PKI signatures and encryption using a recognized protocol.[4] Although RPost®'s cryptographic certificates are purchased from the Verisign Corporation, this is not a requirement as the RSA/PKI signatures and encryption protocols are widely recognized. The hash algorithm used in this software is SHA-1 (Secure Hash Algorithm). This was developed by NIST and the U.S. National Security Agency and produces a 160-bit hash value.[5]

---

[3] The clock replaces NIST-7, a cesium beam atomic clock used from 1993 to 1999. NIST-F1 is approximately 10 times more accurate than NIST-7.

[4] Although RPost® encryption uses Microsoft CryptoAPI 2.0 NIST FIPS-141-1 validated instances of the SHA-1 and 3DES (triple DES) algorithms, use of this particular cryptography package is not a requirement for the operation of the RPost system.

[5] SHA-1 is the industry standard used in government communications and is ISO compliant. Papers circulated by three Chinese cryptanalysts in 1985 showed a weakness in the algorithm that cannot yet be exploited. Hash algorithms have two properties:

1) The input of the hash function cannot be derived from the resulting hash.
2) No two different inputs will result in the same hash (known as a collision).

Breaking a hash function means showing that either - or both - of those properties are not true. By brute force one collision will be found in 2^80 hashes of random messages. The Chinese cryptanalysts found that they could find a collision in 2^69 calculations. Hence this is a weakness in the SHA-1 algorithm. This is a theoretical weakness that cannot be currently exploited in a practical way. When the industry settles on the new hashing standard, those seeking the highest level of security should look to early adopters. In addition, in the RPost system, all renderings of SHA-1 values are over-encrypted with 3-DES encryption, meaning that even a wholesale compromise of the SHA-1 algorithm would not substantially affect the security of receipts.

## B. Pertinent Aspects of the E-mail Environment

The following aspects of the Internet e-mail environment are relevant to the utility of RPost® in achieving the admissibility of e-mail under the Federal Rules of Evidence, now and/or in the future:

1. A research firm estimates that around 3% of non-bulk, business-to-business[6] Internet e-mail goes undelivered to its intended recipient. The main reasons the firm identifies for non-delivery are legitimate messages wrongly identified as spam -- "false positives" due in part to increasingly aggressive use of spam filters -- and e-mail sent to mistyped addresses and those that no longer exist.[7] Other commonly known, more specific reasons include the wide variety of computer servers and systems at both ends of the correspondence and between them, lost data packets, and functions of e-mail programs that automatically fill in recently used addresses.[8]
2. Most e-mail programs allow users to "request a receipt" for outbound messages. But many e-mail systems are configured not to return any "delivery status notifications" or "bounce notices," so as to limit e-mail spammers' ability to distinguish valid e-mail addresses when others on the same system result in bounce notices.[9] In any case, the receipts received by such methods are simple text e-mails that can be readily counterfeited and easily disputed. 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 paper mail.
3. 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, again a situation with no analogy in the world of paper mail.
4. A recipient or sender of an email may change the time of its "receipt" or "sending," respectively (and the creator of any other computer-generated document may change the time of its creation or modification), by simply changing the time on the clock in his or her computer, server or other system. Thus, a falsified email and its attachments can appear to have been "sent" or "received" at the precise time the real email and attachments were sent or received, and the genuine email and attachments may contain no indicia of authenticity -- either in data or metadata -- to distinguish them from the falsified email and attachments. Paper mail, on the other hand, includes a postmark or other indication of sending and/or

---

[6] "Business-to-business Internet e-mail" is mail sent from one corporate e-mail system to another via the Internet, not including mail to consumers, nor mail that remains inside an organization's private system. "Non-bulk" means that this statistic ignores legitimate bulk mail, such as opt-in direct marketing and newsletters, as well as spam e-mails.

[7] Communication from Richi Jennings, Lead Analyst, E-mail Security practice, Ferris Research. to Zafar Khan, CEO, RPost on August 3, 2007.

[8] Intranet e-mail, by contrast, occurs within a controlled environment, so the issues of who sent what, and when, are less scrutinized. In recent years the percentage of e-mails received has been getting lower as a result of the proliferation of "spam filters" added to systems to block junk e-mail, and their aggressive use. None of these systems is perfect, and when they fail they can block the delivery of important communications.

[9] An even more serious problem can develop for a company that permits bounce notices, when as an indirect result its own e-mail system is automatically blacklisted by spam filters because its system has returned a large number of bounce notices to fake sender addresses.

receipt issued by a neutral third-party carrier, rather than a system under the control of one of the parties to a dispute.

### C. Assumptions

This review assumes only the facts stated above and:

1. that an RPost Registered E-mail® message pertaining to the recipient's business is sent to an e-mail address that has been typed accurately and is the sole e-mail address that the recipient or his or her agent on his or her business card, V-Card, business website or business advertising, or in a business directory or similar listing (the "Address"); and
2. that the recipient has not indicated to the sender -- or provided reasonable notice that the sender is reasonably likely to have received or found -- that he or she will not or cannot accept business correspondence of the type in question at the Address.

## II. ISSUES AND CONCLUSIONS

### A. Registered E-mail Receipt is a Statement of Fact of the E-mail Transaction

1. Does UETA apply to a Registered E-mail® message?

   *Generally, UETA applies when the recipient has held her or himself out as doing the sort of business to which the e-mail pertains at the e-mail address used, and has not indicated to the sender not to send business correspondence of the type in question to that address.*

2. When an e-mail is sent using RPost's Registered E-mail® service, when is such e-mail deemed "sent" under UETA?

   *Assuming that UETA applies and that the e-mail was properly addressed in accordance with UETA, the e-mail is deemed "sent" under UETA once it leaves the server of its agent, RPost®.*

3. When an e-mail is sent using RPost's Registered E-mail® service, when is such e-mail deemed "received" under UETA?

   *An e-mail is deemed received under UETA when the recipient's server associated with the designated e-mail address receives the e-mail from the sender. Because the protocol for sending all Internet e-mail confirms the actual recipient's address, not just the server address, RPost's Registered E-mail® service provides a record of delivery in accordance with UETA by recording the recipient's server's receipt thereof. This analysis may extend to the server of an agent of the recipient, such as an e-mail security or anti-spam filtering server if the recipient has the ability to retrieve the message or has control of the management settings of that filter.*

4. Could RPost's Registered E-mail® service effectively establish evidence of the content of an e-mail (both the body and the attachments) under applicable law?

   *Yes, the encryption and tamper-detectability of RPost's Registered E-mail® service generally preserve the contents of emails and their attachments to a sufficient extent to satisfy process requirements inferred under UETA or ESIGN and evidence law and to establish evidence of content.*

5. What is the value of RPost®'s use of an objective, independent time source?

*Currently, RPost's link to a trusted and objective time source will provide essential and credible evidence in disputes in which the time an email what sent or received is material to the case, such as disputes concerning the coincidence or proximity of that time to events material to a case, or in the context of time-sensitive bid disputes. As the response of evidence law to the potential for tampering with computer-generated evidence becomes more refined, leading standard-setters such as X9 suggest that the use of an objective and independent time source is likely to become fundamental to the authentication of emails the admissibility of which is disputed, due to the characteristic of computer-generated documents described in Section I.B.4., above. Finally, as a data-level, intrinsic control, a trusted time stamp makes the authentication of an email and its attachments both easier and less expensive over time than layers of context-based incremental controls for reasons described below.*

6. What value to admissibility is offered by RPost®'s verification/reconstruction of the authentic original (E-mail and Attachments)?

*Authenticity is at the core of admissibility of evidence, and particularly so for computer-generated documents not subject to hearsay-related challenges. An authenticated document is deemed to have satisfied the preliminary threshold for trustworthiness. The ability to verify the content of originals significantly increases the likelihood of admissibility of a disputed document, and a process that has been accepted by courts will also speed that process.*

7. Can RPost's Registered E-mail® service serve as the functional equivalent of paper mail, to be used in lieu of certified mail, registered mail, return receipt mail, private express mail services, fax logs and similar types of paper mail services and confirmations of receipt and content?

*Yes, under UETA and ESIGN, a signature, contract or other record relating to a transaction cannot be denied legal effect solely because it is in electronic form, unless an applicable law other than UETA specifically permits such denial. In the absence of such a specific prohibition, UETA and ESIGN permit the use of electronic signatures and electronic notices as functional equivalents to "wet ink" signatures, certified mail, registered mail, return receipt mail, facsimiles and similar types of notices that are traditionally delivered in paper, and the features of RPost's Registered E-mail® service have generally been designed to serve as equivalents to the functions of the various types of paper-based communications that are generally absent in e-mail.*

## B. Registered Receipt™ Is Evidence Of The Transaction That Is Admissible In Court

1. Based on current statutes and case law, are the facts of the e-mail transaction as described in Points 1-7 of Section A admissible?

*The facts of the e-mail transaction captured and secured by RPost® are well-designed to build an effective case for authentication and admissibility, perhaps first in support of effective testimony and thereafter as a basis for self-authentication.*

2. Can RPost®'s Authentication Receipt™ provide the true electronic original?

*Yes, given the wide use and acceptance of RPost's cryptography, the Authentication Receipt™ can establish the "original" document through demonstration of RPost®'s processes and information safeguards, including both its use of Public Key Infrastructure and of hash values to detect any tampering during verification of the Registered Receipt™.*

3. Does the typed signature in a Registered E-mail® message serve as a verifiable electronic signature of the body of the e-mail and attachments (associated content) based on ESIGN , UETA and case law?

   Y*es. Under existing case law, ESIGN and UETA afford a typed signature transmitted electronically and properly authenticated the same weight as a wet ink signature.*

4. Does RPost® verify the authentic transaction meta-data and provide a delivery audit trail?

   *Yes. RPost® transmits the fact of receipt by the recipient server along with time stamp as well as embedded meta-data to the sender, providing a complete step-by-step audit trail of each transmission.*

5. Does the RPost® product create an admissible e-mail record?

   *There are multiple ways in which to admit e-mail into evidence, a number of which RPost® supports. Beyond admissibility, RPost® may offer substantial support for the "weight" of the proffered e-mail evidence.*

## III. LEGAL ANALYSIS

### A. Registered E-mail Receipt is a Statement of Fact of the E-mail Transaction

#### 1. Applicability of UETA

UETA was designed "to facilitate electronic transactions consistent with other applicable law"[10] by simplifying, clarifying and modernizing "the law governing commerce and governmental transactions through the use of electronic means."[11] We must first determine when UETA applies.[12]

First, the following areas of law are excluded from the scope of UETA: laws governing wills, codicils and testamentary trusts; the Uniform Commercial Code other than Sections 1-107 and 1-206, Article 2, and Article 2A; the Uniform Computer Information Transactions Act; and other areas of law that are specified by a particular state's law.[13]

---

[10] UETA Section 6(1). All references herein to UETA shall be deemed references to the model UETA and its commentary published by the National Conference of Commissioners on Uniform State Laws in 1999.

[11] Commentary No. 1(c) to UETA Section 6(1).

[12] UETA or a variant of UETA has been enacted in forty-six (46) states, excluding only Georgia, Illinois, New York and Washington. References to UETA that follow thus do not address the laws of those four (4) states.

[13] UETA Section 3. This section excludes certain transactions subject to the Uniform Commercial Code ("UCC"). The exclusion of UCITA is of very limited importance due to the adoption of UCITA by only a few states. The UCC is a model law adopted in all 50 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands that provides default rules for certain sales and other commercial transactions involving personal (i.e. moveable) property (not real property). Some of the most important sections of the UCC are NOT excluded from UETA: the very important articles on the Sales and Leasing of Goods (Articles 2 and 2a), as well as the sections on waivers or renunciations of rights or claims arising from alleged breaches (1-107) and certain writings necessary to satisfy the statute of frauds (1-206). The sections of the UCC excluded from UETA are particularly significant in financial services and include some other types of commercial transactions: Negotiable Instruments (including banknotes and drafts (commercial paper)); Bank Deposits (including check collection); Funds Transfers (between institutions); Letters of Credit; Bulk Transfers and Bulk Sales (including auctions and liquidations of assets); Warehouse Receipts, Bills of Lading and Other Documents of

Next, pursuant to Section 5(b) of UETA, UETA only applies to " transactions between parties each of which has agreed to conduct transactions by electronic means." Specifically, the "context and surrounding circumstances, including the parties' conduct[,]" must be examined when determining if "the parties agree[d] to conduct a transaction by electronic means."[14] "Transaction" is defined under UETA to mean "an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs."[15] The commentary to UETA suggests that such definition may be construed broadly to include individuals who would qualify as "consumers" under other applicable law.[16]

Because UETA is meant to be a "voluntary" act, it is necessary to establish "some form of acquiescence or intent on the part of a person to conduct transactions electronically … before the Act can be invoked."[17] Whether the parties have agreed to conduct the transaction by electronic means is a fact-specific inquiry. An explicit agreement provides certainty in establishing the parties' intent, but is not required since requiring a written agreement to conduct a transaction by electronic means would likely be "an unreasonable barrier to electronic commerce, at odds with the fundamental purpose of" UETA.[18] Fortunately, the commentary to UETA offers the following helpful examples to assist in determining whether the parties have likely acquiesced in such a manner that UETA would be deemed to apply:

> Joe gives out his business card with his business e-mail address. It may be reasonable, under the circumstances, for a recipient of the card to infer that Joe has agreed to communicate electronically for business purposes. However, in the absence of additional facts, it would not necessarily be reasonable to infer Joe's agreement to communicate electronically for purposes outside the scope of the business indicated by use of the business card.
>
> Sally may have several e-mail addresses-home, main office, office of a non-profit organization on whose board Sally sits. In each case, it may be reasonable to infer that Sally is willing to communicate electronically with respect to business related to the business/purpose associated with the respective e-mail addresses. However, depending on the circumstances, it may not be reasonable to communicate with Sally for purposes other than those related to the purpose for which she maintained a particular e-mail account.
>
> If Automaker, Inc. were to issue a recall of automobiles via its Internet website, it would not be able to rely on this Act to validate that notice in the case of a person who never logged on to the website, or indeed, had no ability to do so,

---

Title (including storage and bailment of goods); Investment Securities (including assets in addition to securities); and Secured Transactions (transactions secured by a security interest).

[14] UETA Section 5(b).

[15] UETA Section 2(16).

[16] Commentary No. 12 to UETA Section 2(16).

[17] Prefaratory Note to UETA, Part A of Commentary (Scope of the Act and Procedural Approach).

[18] Commentary No. 3 to UETA Section 5.

> notwithstanding a clause in a paper purchase contract by which the buyer agreed to receive such notices in such a manner.
>
> Buyer executes a standard form contract in which an agreement to receive all notices electronically is set forth on page 3 in the midst of other fine print. Buyer has never communicated with Seller electronically, and has not provided any other information in the contract to suggest a willingness to deal electronically. Not only is it unlikely that any but the most formalistic of agreements may be found, but nothing in this Act prevents courts from policing such form contracts under common law doctrines relating to contract formation, unconscionability and the like.[19]

A recent decision construing Missouri's version of UETA "concluded that a fact finder will probably infer from the objective evidence that the parties agreed to negotiate and eventually reach the terms of an agreement via electronic mail based on their ongoing e-mail negotiations during all of 2003 and the beginning of 2004."[20] Furthermore, the parties' continued performance provided evidence of the parties' intent to conduct transactions and reach an agreement by electronic means.[21]

Similarly, a party who agrees to conduct a transaction by electronic means can also refuse to conduct other transactions by electronic means.[22] This right to refuse under Section 5(c) of UETA may not be waived by agreement and applies even if such party has conducted such transactions electronically in the past.[23]

2. **Evidence of Sending of E-mail.**

If UETA applies to the transaction, an e-mail is deemed "sent" under UETA pursuant to Section 15(a), which states the following:

> Unless otherwise agreed between the sender and the recipient, an electronic record is sent when it:
>
> (1) is addressed properly or otherwise directed properly to an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record;
>
> (2) is in a form capable of being processed by that system; and

---

[19] Commentary Nos. 4 and 5 to UETA Section 5.

[20] *International Casings Group, Inc. v. Premium Standard Farms, Inc.*, 358 F. Supp. 2d 863, 875 (W.D. Mo. 2005).

[21] *Id.*

[22] UETA Section 5(c).

[23] Commentary No. 6 to UETA Section 5.

(3) enters an information processing system outside the control of the sender or of a person that sent the electronic record on behalf of the sender or enters a region of the information processing system designated or used by the recipient which is under the control of the recipient.

For purposes of UETA, an "electronic record" is defined to mean "a record created, generated, sent, communicated, received, or stored by electronic means."[24] Part 1 of Section 15(a) requires the sender to use the correct e-mail address or other "specific information which will direct the record to the intended recipient."[25] The timing of when the e-mail is sent is determined by when the e-mail leaves the control of the sender such that the e-mail has left the sender's server.[26] If, however, the sender and the recipient share the same server or system (such as when both use the same server of a university or company), time of delivery shall be deemed as when the recipient gains control over the e-mail.[27] Accordingly, in such a situation, the e-mail would be deemed "sent" under UETA when the e-mail arrives at the recipient's server associated with the recipient's specified e-mail address or other "information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record."[28]

Applying UETA to RPost® and assuming that the e-mail was properly addressed in accordance with Section 15(a)(1) of UETA, the e-mail will be deemed "sent" under UETA once it leaves the server of the sender's agent, RPost®. In fact, as stated in the Statement of Facts above, the e-mail may leave the RPost server several times. RPost® records two times: when the e-mail arrives at the RPost® server and when it arrives at the recipient server. Using RPost®, the sender can establish that the e-mail was effectively "sent" between those two times. The more critical time element, defining legal delivery, however, is the time of receipt by the recipient's server, described in the next section.

3. **Evidence of Receipt of E-mail.**

Assuming UETA applies to the transaction and it is sent in accordance with Section II(A)(1) above, an e-mail is deemed "received" under UETA pursuant to Sections 15(b) and (e), which state the following:

> 15 (b) Unless otherwise agreed between a sender and the recipient, an electronic record is received when:
>
> (1) it enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record; and

---

[24] UETA Section 2(7).

[25] Commentary No. 2 to UETA Section 15.

[26] *Id.*

[27] *Id.*

[28] UETA Section 15(a).

(2) it is in a form capable of being processed by that system.

(e) An electronic record is received under subsection (b) even if no individual is aware of its receipt.

Similar to when the e-mail is sent, the recipient is deemed to have "received" the e-mail, regardless of whether the recipient is aware of its receipt or retrieves the e-mail, when it enters the recipient's "information processing system" or server, provided that the recipient has designated that system for use, uses it and can access the system.[29] By designating where e-mails are to be sent or directed, the recipient retains control of the place of receipt.[30] This provision of UETA permits a recipient to designate that personal e-mails are to be sent to a home e-mail address and business matters are to be sent to a business e-mail address. If a sender directs a business e-mail to the recipient's home e-mail address, such e-mail may not be deemed received if the recipient has designated his or her "business address as the sole address for business purposes."[31] If the recipient has actual knowledge of the e-mail by reviewing it from home, the recipient's presumed receipt of the e-mail is determined under the otherwise applicable substantive law.

Presumably, under Section 15(b)(1), if spam filters or other devices block the recipient's ability to retrieve the e-mail or place such e-mail automatically in "quarantine" or in a junk folder, such e-mail will not be deemed received by the recipient under UETA unless the recipient is "able" to retrieve the e-mail from such filters or repositories. Whether a recipient with no direct access to or notice of e-mails stopped by his or her company's or ISP's spam filter or other protective system is "able" to retrieve them has not been construed by U.S. courts. In theory this recipient has the ability to retrieve e-mails, at a minimum through requesting them from her corporate or ISP system administrator, but as a practical matter that ability may be limited in diverse, fact-specific ways. The proliferation of spam and the frequency of "false positives" in increasingly aggressive spam filters has maintained demand for end-user access to e-mails stopped by those filters, however, and an end-user with such access appears able to retrieve the e-mails, increasing the likelihood that delivery would be found under UETA against such a user, and the utility of RPost® Registered Receipts™ confirming arrival at the recipient's server. Neither opening, review nor knowledge that the e-mail arrived is required to establish delivery under UETA.

On the other hand, if the e-mail is automatically rejected by the recipient's server, it may not be deemed received under UETA on the argument that it has not entered the recipient's information processing system, and in any event the recipient could not retrieve the e-mail as required by Section 15(b)(1) of UETA. Under UETA Section 15(f), the sender's receipt of an electronic acknowledgment from a server or other information processing system in accordance with Section 15(b) of UETA establishes that the e-mail or electronic record was received by the recipient, but as noted above, this device is often disabled by corporations and ISPs. In that respect, RPost®'s automatic inquiries to the recipient server concerning whether an e-mail was received may be useful in establishing absence of receipt.

---

[29] Commentary No. 3 to UETA Section 15.

[30] *Id.*

[31] *Id.*

By recording the SMTP dialog (as explained in Attachment A hereto), RPost's Registered E-mail® service documents the recipient's mail server's declaration of the e-mail being accepted. Because all Internet e-mail is delivered by SMTP, RPost's Registered E-mail® service provides proof of delivery in accordance with UETA by recording the recipient's server's receipt thereof. RPost's Registered E-mail® service can also provide additional proof that the recipient opened the e-mail and, when it detects that the email has been opened, sends an acknowledgment to the sender to that effect.

4. **Proof of Content of E-mail.**

Although many e-mail programs permit senders to use a "request a receipt" or "request acknowledgment" from the recipient for outbound messages, UETA states in Section 15(f) that receipt of an electronic acknowledgment from a server or other information processing system in accordance with UETA establishes that the e-mail or electronic record "was received, but, by itself, does not establish that the content sent corresponds to the content received." Furthermore, such acknowledgment does not provide evidence of whether the e-mail was read or opened by the recipient.

The electronic evidence created by RPost's Registered E-mail® service and the RPost® Digital Seal® technology may not be excluded solely because it is in electronic form pursuant to Section 13 of UETA. Therefore, UETA would not prohibit the admission of such evidence, but it does not provide guidance on the authenticity of the contents of such e-mail.

The Registered Receipt™ e-mail includes an encrypted copy of Sender's original message and all attachments as they were received by the recipient's server. Anyone in possession of that Registered Receipt™ is able to verify the authenticity of the data it contains by sending a copy to an e-mail address controlled by RPost® where RPost®'s cryptographic methods are used to determine if information in the Registered Receipt™ has been altered, employing hash algorithms and RSA/PKI signatures. As noted at the outset of this memorandum, the use tamper detection methods, such as hash algorithms, is particularly well suited to electronic evidence, and the use of hash values has been accepted by many courts. [32]

If the cryptographic method used to authenticate the Registered Receipt™ determines that the information in the Registered Receipt™ has not been altered, then RPost®'s agent reconstructs an authenticated copy of the Sender's original message -- including attachments -- as it was received by the server along with an authenticated delivery analysis, authenticated official times of sending and receipt, and all authenticated notifications and transaction records relevant to the delivery of the message. This authenticated information and analysis is returned by RPost® to the Sender (or to the party requesting authentication by having submitted the Registered Receipt™ to the agent) in the

[32] RPost®'s method of comparison of the purported message to the decrypted originals via hash values have been accepted by many courts. See, generally: *Sanders v. State*, 191 S.W.3d 272,278 (Tx. App. 2006); *United States v. Heiser*, 2006 WL 1149254 p.9 (M.D. Pa. April 228, 2006); *United States v. Hibble*, 2006 WL 2620349 pp.7,8 (D.Az. September 11, 2006); *United States v. Cartier*, 2007 WL 319648 pp.1,2 (D.N.D. January 30, 2007); *O'Bar v. Lowe's Home Centers, Inc.*, 2007 WL 1299180 p.5 (W.D.N.C. May 2, 2007); *Krause v. State*, 2007 WL 2004940 pp.2,3 ( Tx. App. July 12, 2007).

form of an Authentication Receipt™ e-mail. This approach provides a credible foundation for the admission of the contents of the e-mail, as discussed more fully below.

5. **Legal Time the E-mail is Sent and Received.**

The use of an accurate clock is not critical to proving sending or delivery under UETA. Its importance to e-evidence derives from the ultimate importance of verified time to authentication. As noted above, in the absence of an objectively accurate time stamp, a recipient or sender of an email may change the time of its "receipt" or "sending," respectively, by simply changing the time on the clock in his or her computer or system. Thus, a falsified email and its attachments can appear to have been "sent" or "received" at the precise time the real email and attachments were sent or received, and in the absence of a time stamp from an accurate clock independent of the system of the perpetrator of the fraud, the genuine email and attachments may contain no indicia of authenticity -- either in data or metadata -- to distinguish them from the falsified email and attachments.[33]l Therefore, the application of a time stamp from an accurate, independent clock is likely to prove important in a dispute concerning the authenticity of an email, and is likely to be favored by courts as the potential for tampering with ESI becomes better recognized and/or as tribunals look for ways of obviating authentication disputes. Moreover, as a data-level rather than peripheral control tied to a source of accurate time (the NIST-F1) that is very likely to continue to be incrementally improved and very unlikely to disappear, the time stamp associated with RPost's Registered E-mail® service is likely to provide a reliable and cost-effective control over time. Prior, less accurate versions of the NIST-F1 have been used in admitting evidence, for example, regarding aircraft collisions.[34]

In addition to its likely usefulness in authenticating a proffered email where the time of the email is not itself relevant, as discussed in the previous paragraph, an accurate, independent time stamp has more specific uses where the time of the email is relevant. For example, the coincidence or nearness of the time of record creation or sending to the facts and circumstances of the case may be material, as is often the case with the disclosure of inventions. One noteworthy area of time-critical email events is time-sensitive bid submissions and contracting. Failure to send or receive a proposal within the specified time can preclude the recipient's obligation to consider the proposal and leave the proposer with only limited recourse against a common carrier.[35] In this context, the value of electronic proof of time of delivery is evident under U.S. federal government contracting regulations: By submitting a federal contracting proposal electronically so that it is received no later than 5:00 p.m. one working day prior to a proposal due date, a bidder is excused if the hard copy bid

---

[33] As noted above, in this respect paper mail is easier to authenticate than email without an objectively-valid time stamp, because it includes a postmark or other indication of sending and/or receipt issued by a neutral third-party carrier, rather than a system under the control of one of the parties to a dispute.

[34] E.g., *In re Greenwood Air Crash*, 924 F. Supp. 1518, 1527 (S.D.Ind.,1995).

[35] Failure to timely submit a bid leaves can leave the bidder with only limited recourse against a recipient. See, e.g., *Husman v. Purolator Courier*, 832 F.2d 459, 461 (8th Cir.1987), and *Todd Heller, Inc. v. United Parcel Service*, Inc., 754 A.2d 689 (Pa.Sup.,2000).

is received late.[36] Other legal instances in which accurate time may have evidentiary importance include fact situations in which the order of events are critical and time-sensitive notice obligations.

### 6. Verifies/Reconstructs Authentic Original (e-mail and attachment)

Authentication is a subset of relevancy—evidence which is not authentic cannot be relevant.[37] Therefore, issues of authenticity are essentially questions of conditional relevancy involving a factual determination by the jury and admissibility.[38] Because determining if scanned documents are authentic is a matter of conditional relevancy, a court must engage in a two-step process.[39] First, before admission of the evidence, the court must determine if there is a sufficient foundation for a jury to reasonably find that the proffered evidence is authentic.[40] Second, the jury resolves the question of whether the evidence is what the proponent claims.[41]

As noted above, the Registered Receipt™ e-mail includes not only metadata relating to the email transaction, but an encrypted copy of Sender's original message and all attachments as they were received by the recipient's server. Anyone in possession of that Registered Receipt™ is able to verify the authenticity of the data it contains by sending a copy of it to an e-mail address controlled by RPost® where RPost®'s cryptographic methods are used to determine if information in the Registered Receipt™ has been altered, employing hash algorithms and RSA/PKI signatures. As noted at the outset of this memorandum, the use tamper detection methods, such as hash algorithms, is particularly well suited to electronic evidence, and the use of hash values has been accepted by many courts. [42]

If the cryptographic method used to authenticate the Registered Receipt™ determines that the information in the Registered Receipt™ has not been altered, then RPost®'s agent reconstructs an authenticated copy of the Sender's original message as it was received by the server along with an authenticated delivery analysis, authenticated official times of sending and receipt, and all authenticated notifications and transaction records relevant to the delivery of the message. This authenticated information and analysis is returned by RPost® by the party requesting authentication

---

[36] 48 C.F.R. 14.304 (b)(1)(i).

[37] *Lorraine v. Markel Am. Ins. Co.*, No. PWG-06-1893, 2007 WL 1300739, 11 (D. Md. May 4, 2007.

[38] *Id.*, at 11-12.

[39] *Id.*, at 12.

[40] *Id.*

[41] *Id.*

[42] RPost®'s method of comparison of the purported message to the decrypted originals via hash values have been accepted by many courts. See, generally: *Sanders v. State*, 191 S.W.3d 272,278 (Tx. App. 2006); *United States v. Heiser*, 2006 WL 1149254 p.9 (M.D. Pa. April 228, 2006); *United States v. Hibble*, 2006 WL 2620349 pp.7,8 (D.Az. September 11, 2006); *United States v. Cartier*, 2007 WL 319648 pp.1,2 (D.N.D. January 30, 2007); *O'Bar v. Lowe's Home Centers, Inc.*, 2007 WL 1299180 p.5 (W.D.N.C. May 2, 2007); *Krause v. State*, 2007 WL 2004940 pp.2,3 ( Tx. App. July 12, 2007).

by having submitted the Registered Receipt™ to the agent in the form of an Authentication Receipt™ e-mail.

This Registered Receipt™ is secured by PKI technology of which RPost® is the only key holder. If at a time in the future, Sender needs verification of receipt of his e-mail as well as its content, RPost® is able to provide such as the sole holder of the keys. RPost® at that time can determine that the message has not been tampered with or if it has, it can affirm that fact as well.

As described in more detail in Part B below, RPost® may need to introduce testimony concerning its information safeguards and generally accepted cryptographic methods. Because we conclude in Part B below that the safeguards and methods described in the Statement of Facts above generally meet court-accepted standards, and assuming that RPost® technology keeps pace with changes in those standards, we believe that the decrypted and reconstructed message and attachments from the Registered Receipt™ will be accepted in court as an authentic original.

### 7. Functional Equivalent of Electronic Signatures and Notices

A core principle of UETA is that "the medium in which a record, signature, or contract is created, presented or retained does not affect its legal significance."[43] Specifically, pursuant to Section 7 of UETA, a "record or signature may not be denied legal effect or enforceability solely because it is in electronic form." Under UETA, if a law requires a record to be in writing, an electronic record satisfies that law.[44] Therefore, if a sender needs to deliver a document to a third party, the sender may rely on a document delivered electronically (unless such reliance or delivery is specifically prohibited by an applicable law other than UETA as described in the following paragraph).

UETA also recognizes that otherwise applicable law may impose additional requirements that must still be satisfied even if the record is sent electronically. Under Section 8 of UETA, if the "parties have agreed to conduct a transaction by electronic means and a law requires a person to provide, send, or deliver information in writing to another person, the requirement is satisfied if the information is provided, sent, or delivered, as the case may be, in an electronic record capable of retention by the recipient at the time of receipt." An electronic record is not capable of retention by the recipient if the sender or its information processing system prevents or inhibits the recipient's ability to store or print the electronic record.[45] Accordingly, if a notice or record is sent electronically, a law requiring the delivery of that information in writing will only be satisfied if the recipient can print or store such electronic record.

Furthermore, if another law other than UETA requires a record to be posted or displayed in a certain manner, to be sent, communicated or transmitted by a specific method or to contain

---

[43] Commentary No. 1 to UETA Section 7.

[44] UETA Section 7(c).

[45] UETA Section 8(a).

information formatted in a certain manner, the electronic record must satisfy those requirements by being in the requisite format or sent in the designated manner.[46] For example, if a document must contain 20-point bold type, the electronic record must also contain such type. In this regard, RPost®'s use of HTML to preserve original formats and its use of common formats in its Registered Receipt™ and Authentication Receipt™ can be helpful in meeting the requirements of such laws other than UETA. If the law requires that the notice be delivered by overnight carrier, the notice must be delivered in such manner.[47]

Parties to a transaction governed by UETA may not as a rule vary the requirements of Section 8 of UETA by agreement, but may agree to electronic delivery if a requirement of law other than UETA requires the sender to "send, communicate, or transmit a record by [first-class mail, postage prepaid][regular United States mail],"[48] if such law permits such an agreement.

Therefore, under UETA, electronic signatures and electronic notices can serve as functional equivalents to "wet ink" signatures, certified mail, registered mail, facsimiles and similar types of notices that are traditionally delivered in paper unless an applicable law other than UETA prohibits such use.

Except as noted otherwise, the analysis under ESIGN (the federal statute) and of UETA, which all but four (4) states have adopted, are essentially the same. To the extent that states that have adopted electronic signature laws inconsistent with UETA (or no electronic signature laws), such state laws are preempted by ESIGN's broad preemption provisions.[49] For those states that have enacted a version of UETA, that state's enactment will govern, except as otherwise noted in ESIGN. As discussed in detail below, one of the most significant areas where ESIGN continues to apply even in those states that have enacted a pristine version of UETA is in the area of consumer disclosures. It is ESIGN that requires special steps to be taken to provide certain consumer disclosures exclusively via electronic means.

ESIGN similarly recognizes that an electronic signature can be as legally effective as a signature applied in wet ink on paper. ESIGN does not give electronic signatures a special status in the law. Rather, ESIGN states that a signature may not be denied legal effect *solely* because it is in electronic form. The foundational provision of ESIGN acknowledging electronic signatures provides:

> (a) In General.--Notwithstanding any statute, regulation, or other rule of law (other than this title and title II), with respect to any transaction in or affecting interstate or foreign commerce-

---

[46] UETA Section 8(b).

[47]Note, however, that in some but not all such circumstances and depending on the wording of that statute, an organization may be able to avail itself of the functional equivalence analysis discussed below in complying with that statute.

[48] UETA Section 8(d).

[49] ESIGN Section 102(a).

> (1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
>
> (2) 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.[50]

ESIGN, like UETA,[51] gives equal recognition to electronic signatures and electronic records, with the few exceptions mentioned below. The general permissibility of use of electronic signatures and records is, however, limited by ESIGN Section 103, which does not permit the use of electronic notices in the following circumstances:

(a) any notice of cancellation or termination of utility services (including heat, water and power);

(b) notice of default, acceleration, repossession, forfeiture, or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual;

(c) notice of the cancellation or termination of health insurance or benefits (excluding annuities);

(d) notice of recall of a product, or material failure of a product, that risks endangering health or safety; or

(e) any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

Furthermore, Section 101 of ESIGN, which permits the use of electronic records or signatures, will not apply to a contract or other record if its governed by law relating to the creation and execution of wills, codicils or testamentary trust, certain areas of family law and the Uniform Commercial Code other than Sections 1-107 and 1-206 and Articles 2 and 2A.[52]

ESIGN provides that Consumer Disclosures may be delivered exclusively electronically, provided, however, that the recipient of the Consumer Disclosure is first provided, and agrees, to the ESIGN Consent.[53] Whether a particular transaction requires a Consumer Disclosure, and how

---

[50] ESIGN Section 101(a).

[51] UETA Section 7(a).

[52] ESIGN Section 103(a).

[53] ESIGN §7001(c). As used herein, "Consumer Disclosures" means information relating to a transaction or transactions in or affecting interstate or foreign commerce, required by a statute, regulation, or rule of law (other than ESIGN) to be provided or made available to a consumer in writing, which triggers the obligation to provide the ESIGN Consent. "ESIGN Consent" means a disclosure required under ESIGN to be delivered to a recipient if such recipient is a consumer and the sender has an obligation to provide any Consumer Disclosures to such recipient, and such sender intends to deliver the required Consumer Disclosures exclusively through electronic means.

the ESIGN Consent is delivered in connection with the required Consumer Disclosure, are determined on a transaction-by-transaction basis.

ESIGN, but not UETA, prescribes special rules for the delivery through electronic means of a Consumer Disclosure required to be made in writing under another federal or state law in a transaction. An example of a Consumer Disclosure required in the context of the sale of a life insurance policy is a life insurance replacement notice that an insurance company or agent must deliver to a consumer before selling a new life insurance policy. ESIGN's Consumer Disclosure provision states that:

> If a statute, regulation, or other rule of law requires that information relating to a transaction or transactions in or affecting interstate or foreign commerce be provided or made available to a consumer ***in writing***, the use of an electronic record to provide or make available (whichever is required) such information satisfies the requirement that such information be in writing if--
>
> (A) the consumer has affirmatively consented to such use and has not withdrawn such consent;
>
> (B) the consumer, prior to consenting, is provided with a clear and conspicuous statement--
>
> (i) informing the consumer of (I) any right or option of the consumer to have the record provided or made available on paper or in non-electronic form, and (II) the right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and of any conditions, consequences (which may include termination of the parties' relationship), or fees in the event of such withdrawal;
>
> (ii) informing the consumer of whether the consent applies (I) only to the particular transaction which gave rise to the obligation to provide the record, or (II) to identified categories of records that may be provided or made available during the course of the parties' relationship;
>
> (iii) describing the procedures the consumer must use to withdraw consent as provided in clause (i) and to update information needed to contact the consumer electronically; and
>
> (iv) informing the consumer (I) how, after the consent, the consumer may, upon request, obtain a paper copy of an electronic record, and (II) whether any fee will be charged for such copy;
>
> (C) the consumer--
>
> (i) prior to consenting, is provided with a statement of the hardware and software requirements for access to and retention of the electronic records; and

> (ii) consents electronically, or confirms his or her consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent;[54] and
>
> (D) after the consent of a consumer in accordance with subparagraph (A), if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent, the person providing the electronic record--
>
> (i) provides the consumer with a statement of (I) the revised hardware and software requirements for access to and retention of the electronic records, and (II) the right to withdraw consent without the imposition of any fees for such withdrawal and without the imposition of any condition or consequence that was not disclosed under subparagraph (B)(i); and
>
> (ii) again complies with subparagraph (C).

***Consumer's Consent to Electronic Delivery- How.*** The recipient's affirmative consent to the Consumer Disclosure must exhibit the recipient's ability to access the Consumer Disclosures in the form they will be provided. For example, if the required disclosures (the replacement notice for example) were to be posted at a secure web site accessible only after the recipient is given a unique access code, ESIGN requires that the recipient be given that unique access code during the Consumer Disclosure process and then confirm that the unique access code in fact allowed the recipient to access the secure site where such required disclosures will be posted. If *how* the recipient consents to receive disclosures electronically does not demonstrate that the recipient actually accessed that secure web site, then the Consumer Disclosure is likely to be ineffective and therefore the basis for providing the required disclosures exclusively by electronic means fails. If the statutorily required Consumer Disclosures (such as the replacement notice) were to be provided by e-mail in an html format (to permit more graphics and various font sizes to emphasize provisions as may be required by the disclosure laws), then the Consumer Disclosure should be e-mailed to the recipient using an html formatted notice, in a manner that reasonably allows the sender to validate or the recipient to confirm receipt. Likewise, if the recipient is going to be provided the required disclosures only in a PDF format as attachments to an e-mail, the Consumer Disclosure would be required to prompt the recipient to confirm that he or she was able to receive, open and save the PDF documents.

***Failure to Comply with the ESIGN Consumer Disclosure Requirements.*** Failure to comply with the ESIGN Consumer Disclosure requirements does not render void or voidable the underlying transaction (the application for insurance or the insurance policy ultimately issued). ESIGN provides:

---

[54] Note that the technology discussed in this memorandum does not address this ESIGN requirement, but it is addressed in RPost's eContracting™ and Register Reply™ products, to be discussed in a subsequent memo.

> (3) Effect of failure to obtain electronic consent or confirmation of consent.--The legal effectiveness, validity, or enforceability of any contract executed by a consumer shall not be denied solely because of the failure to obtain electronic consent or confirmation of consent by that consumer in accordance with paragraph (1)(C)(ii).[55]

Failure to comply with the ESIGN Consumer Disclosure requirements could, however, subject the sender to regulatory sanctions for failing to provide the required disclosures (such as the replacement notice) in accordance with applicable law. There may also be civil remedies available to recipients if the disclosures are deemed to have not been given effectively.

We believe that the Consumer Disclosure requirements of ESIGN likely survive the reverse preemption by UETA of ESIGN in the forty-six (46) states in which UETA applies. We do not believe that RPost's Registered E-mail® service core delivery feature alone includes a process designed to conform to the consent to electronic delivery of the ESIGN Consumer Disclosure requirements, so we do not view the core Registered E-mail® service alone as sufficient to satisfy such requirements in the absence of additional process.[56] Of course, only a limited subset of documents sent as e-mails or their attachments are Consumer Disclosures subject to the ESIGN disclosure requirements above. Moreover, we understand that many of RPost®'s clients obtain consumer consent to the form of electronic delivery prior to using Registered E-mail® services to deliver disclosures under ESIGN.

Therefore, under ESIGN, electronic signatures and electronic notices can serve as functional equivalents to "wet ink" signatures, certified mail, registered mail, facsimiles and similar types of notices that are traditionally delivered in paper unless a law other than ESIGN prohibits such use or if otherwise excluded from the scope of ESIGN, and subject to the consumer disclosure requirement of ESIGN.

## B. Registered Receipt™ Is Evidence Of The Transaction That Is Admissible In Court

Questions of admissibility are governed by the Federal Rules of Evidence ("F.R.E.") or their state equivalents.[57] RPost's Registered E-mail® service assists in establishing the authenticity of ESI. "In order for ESI to be admissible, it also must be shown to be authentic…[T]he requirement] is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims…It also [e]nsures that evidence is trustworthy.".[58] Although many courts have

---

[55] ESIGN Section 101(c)(3).

[56] RPost's eContracting™ and Register Reply™ products, for example, addressed in a subsequent memorandum, could be used to provide comprehensive documentation of the consumer's agreement to access the disclosures in the form provided.

[57] Many states have adopted rules of evidence that track the Federal Rules of Evidence (FRE). For purposes of this discussion all cited cases are based on the FRE or state law that follows the FRE.

[58] *Lorraine v. Markel American Insurance Company*, 241 F.R.D. 534 , 541-542 (D.Md 2007).

chosen understandably and legitimately not to grapple with issues of the admissibility of electronic documents when not in dispute,[59] Judge Grimm's opinion in *Lorraine v. Markel American Insurance Company* and some other recent cases may indicate that this area will become increasingly challenging as the legal system faces more questions about electronic documents.[60] If so, authentication will need to be carefully considered. As Judge Grimm noted, "A party seeking to admit an exhibit need only make a prima facie showing that it is what he or she claims it to be. This is not a particularly high issue to overcome . . . Ironically, however, counsel often fail to meet even this minimal showing when attempting to introduce ESI, which underscores the need to pay careful attention to this requirement. Indeed, the ability to get evidence admitted because of a failure to authenticate almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation.[61]

Certain subparts of Sections 901 and 902 of the Federal Rules of Evidence, which address authentication, have been identified in District Court opinions as particularly suited to the ESI and especially e-mail: Sections 901 (b)(4) and (b)(9), and 902 (7) and (11). Rules 901 (b)(4) and (9) require witness testimony to authenticate proffered evidence, while 902 (7) and (11) allow for self-authentication.

The automation of many RPost® processes such as the production of the Registered Receipt™ is useful in achieving admissibility, in part given that computer-generated records do not contain hearsay (except insofar as they contain the assertions of a person and are offered to prove the truth of the matter asserted). For any documents that RPost® generates that are "untouched by human hands," authentication is the primary hurdle, since the proponent is relieved from the added requirement of making the computer generated information fall within an exception to the hearsay rule. "The admissibility of the computer tracing system record should be measured by the reliability of the system, itself, relative to its proper functioning and accuracy."[62] "Inaccurate or misleading data only materializes if the machine is not functioning properly."[63]

---

[59] Opposing parties often allege that computer records have been tampered with and thus lack authenticity. Such claims have been viewed as "almost wild-eyed speculation…without some evidence to support such a scenario…." *United States v. Whitaker*, 127 F.3d 595, 602 (7th Cir. 1997).

[60] See, e.g.: *In Re Vee Vinhnee*, 336 B.R. 437 (proponent failed properly to authenticate exhibits of electronically stored business records); *United States v. Jackson*, 208 F.3d 633, 638 (7th Cir. 2000) (proponent failed to authenticate exhibits taken from an organization's website); *St. Luke's Cataract and Laser Institute PA v. Sanderson*, 2006 WL 1320242, at *3-4 (M.D. Fla. May 12, 2006) (excluding exhibits because affidavits used to authenticate exhibits showing content of web pages were factually inaccurate and affiants lacked personal knowledge of facts); *Rambus v. Infineon Tech. A.G.*, 348 F. Supp. 2d 698 (E.D. Va. 2004) (proponent failed to authenticate computer generated business records); *Wady v. Provident Life and Accident Ins. Co. of Am.*, 216 F. Supp. 2d 1060 (C.D. Cal. 2002) (sustaining an objection to affidavit of witness offered to authenticate exhibit that contained documents taken from defendant's website because affiant lacked personal knowledge); *Indianapolis Minority Contractors Assoc. Inc. v. Wiley*, 1998 WL 1988826, at *7 (S.D. Ind. May 13, 1998) (proponent of computer records failed to show that they were from a system capable of producing reliable and accurate results, and therefore, failed to authenticate them)." *Lorraine*, p. 542.

[61] *Lorraine,* at 542.

[62] *State v. Meeks*, 867 S.W.2d 361, 376 (Tenn.Crim.App.1993).

[63] *State v. Armstead*, 432 So.2d 837, 840 (La. 1983) See also: *People v. Holowko*, 486 N.E.2d 877, 878-79 (Ill. 1985) (automated trap and trace records); *United States v. Duncan*, 30 M.J. 1284, 1287-89 (N-M.C.M.R. 1990) (computerized

1. F.R.E. 901

F.R.E. 901(b)(4) "is one of the most frequently used [rules] to authenticate e-mail and other electronic records. It permits exhibits to be authenticated or identified by '[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics.' "[64] This rule has been used to authenticate e-mail based on circumstantial evidence such as a defendant's work e-mail address, the sending and receipt of emails and testimony that showed the defendant was familiar with the e-mail's content.[65]

RPost®'s use of hash values in producing its Authentication Receipt™ will assist in obtaining admission of RPost's Registered E-mail® service receipts under F.R.E. 901(b)(4). Hash values have repeatedly been accepted to ensure the authenticity of electronic documents.[66] "In order for two hash values to match, the files being compared must be identical for every character and every line,"[67] and RPost®'s hash values also capture all transactional and embedded metadata. By comparing the hash value of the Registered Receipt™ e-mail to the proposed evidence, the Authentication Receipt™ will streamline the need for testimony under F.R.E. 901(b)(4). Judge Grimm's *Lorraine* opinion indicates that authentication of an exhibit based on its hash value is appropriate.[68]

The *Lorraine* opinion also supports the use of metadata in authenticating electronic documents under F.R.E.901(b)(4): "[b]ecause metadata shows the date, time and entity of the creator of an electronic record, as well as all changes made to it, metadata is a distinctive characteristic of all electronic evidence that can be used to authenticate it under Rule 901(b)(4)."[69] However, Judge Grimm also notes that "this method is not foolproof," because, quoting *Weinstein on Evidence:*

---

records of ATM transactions); 2 J. Strong, *McCormick on Evidence* § 294, at 286 (4th ed.1992); Richard O. Lempert & Stephen A. Saltzburg, *A Modern Approach to Evidence* 370 (2d ed. 1983). Cf. *United States v. Fernandez-Roque*, 703 F.2d 808, 812 n.2 (5th Cir. 1983) (rejecting hearsay objection to admission of automated telephone records because "the fact that these calls occurred is not a hearsay statement"). Accordingly, a properly authenticated computer-generated record is admissible. See Lempert & Saltzburg, at 370.

[64] *Lorraine,* p. 544.

[65] *United States v. Siddiqui*, 235 F.3d 1318,1322-23, (11th Cir. 2000); *United States v. Safavian*, 435 F. Supp.2d 36, 40 (D.D.C. 2006).

[66] See generally: *Sanders v. State*, 191 S.W.3d 272,278 (Tx. App. 2006); *United States v. Heiser*, 2006 WL 1149254 p.9 (M.D. Pa. April 28, 2006); *United States v. Hibble*, 2006 WL 2620349 pp7,8 (D.Az. September 11, 2006); *United States v. Cartier*, 2007 WL 319648 pp.1, 2 (D.N.D. January 30, 2007); *O'Bar v. Lowe's Home Centers, Inc.*, 2007 WL 1299180 .p5 (W.D.N.C. May 2, 2007); *Krause v. State*, 2007 WL 2004940 pp.2,3 ( Tx. App. July 12, 2007). [use official citations, if available]

[67] *L-3 Communications Westwood Corp. v. Robicharux*, 2007 WL 756528 (E.D.La., March 08, 2007).

[68] *Lorraine*, p. 547.

[69] *Id.* at 547, 548.

> [a]n unauthorized person may be able to obtain access to an unattended computer. Moreover, a document or database located on a networked-computer system can be viewed by persons on the network who may modify it. In addition, many network computer systems usually provide for a selected network administrators to override an individual password identification number to gain access when necessary.[70].

RPost®'s Registered Receipt™ e-mail and Authentication Receipt™ e-mails, however represent the "best possible case" for authentication of an e-mail under F.R.E. 901(b)(4) precisely in view of that uncertainty and of the possibility of tampering with the hash value of the original, because the Registered Receipt™ presents all metadata, as well as all content of the e-mail and attachments, in an automatically encrypted form to which RPost® alone possesses the decryption algorithm, and the Authentication Receipt™ compares the proffered e-mail to the decrypted original using hash values and other replicable cryptographic processes.

F.R.E. 901(b)(9) is frequently used as a litmus test for admissibility of computer-related information. It is "one method of authentication that is particularly useful in authenticating electronic evidence stored in or generated by computers. It authorizes authentication by '[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result'"[71] "[It] dictates that the inquiry into the basic foundational admissibility requires sufficient evidence to authenticate both the accuracy of the image *and* the reliability of the machine producing the image."[72]

Imwinkelried's *Evidentiary Foundations* prescribes an eleven-step process for admission of computer generated records under 901(b)(9)[73]. Two recent opinions indicate that counsel should be prepared to address all eleven steps in tendering computer-generated records.[74] Most of the

---

[70] *Id.* at 548, quoting Jack B. Weinstein & Margaret A. Berger, *Weinstein's Federal Evidence* § 900.01[4][a] (Joseph M. McLaughlin ed., Matthew Bender 2d ed. 1997).

[71] *Id.* p. 549.

[72] S*tate v. Swinton*, 268 Conn. 781,811: 847 A.2d 921, 941,42 (CT. 2004) applying the federal standard to a state case.

[73] Edward J. Imwinkelried, *Evidentiary Foundations*, 58-59 (LexisNexis 6th ed. 2005).

1. The business uses a computer.
2. The computer is reliable.
3. The business has developed a procedure for inserting data into the computer.
4. The procedure has built-in safeguards to ensure accuracy and identify errors.
5. The business keeps the computer in a good state of repair.
6. The witness had the computer readout certain data.
7. The witness used the proper procedures to obtain the readout.
8. The computer was in working order at the time the witness obtained the readout.
9. The witness recognizes the exhibit as the readout.
10. The witness explains how he or she recognizes the readout.
11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

[74] *Lorraine* p.558 n. 27, and *In re Vee Vinhnee*, 336 B.R.437 (BAP 9th 2005) (exhibit excluded as penalty for failing to satisfy these steps).

testimony proffered under these eleven steps is a simple recitation of facts. More challenging is step four, which requires proof that the "procedure has built-in safeguards to ensure accuracy and identify errors…regarding computer policy and system control procedures, including control of access to the database, control of access to the program, recording and logging changes, backup practices, and audit procedures to assure the continuing integrity of the records."[75] In satisfying this requirement or making arguments for admissibility under 901(b)(4), RPost® might have to provide expert technical testimony as to its functionality and safeguards.[76] Following initial court decisions recognizing those safeguards, parties may stipulate to the authenticity of RPost's Registered E-mail® service, in which case such testimony will not be required.

Under 901(b)(9), aspects of the initial testimony would include:

- The manner in which RPost's server(s) are used in the generation and sending of a Registered E-mail® messages, the generation and sending of a Registered Receipt™ e-mail and the generation and sending of an Authentication Receipt™;
- The reliability of these servers;
- Procedures for manual data entry and system controls;
- Safeguards to ensure accuracy and identify errors. Testimony within this point may include the following:
    - RPost® has safeguards, access rules and other controls on the environment that govern the flow of information through its system that meet or exceed industry standards;
    - No tampering with RPost® software can have any impact on the authentication process due to safeguards inherent in the process and technology;
    - All of the evidentiary materials in the RPost® Registered Receipt™ and Authentication Receipt™ are protected by RSA/PKI signatures and encryption using the S/MIME protocol, and Rpost®'s cryptographic certificates are purchased from Verisign;
    - The only data elements retained by RPost® in connection with a particular e-mail are the PKI algorithms, and RPost® secures such algorithms within an electronic environment that meets or exceeds industry standards in terms of levels of secured entry, role-based access rules, strong-form password protections, rules for changing and reusing passwords, etc.;

[75] *In re Vee Vinhnee*, 447.

[76] Many of the accreditations and certifications received RPost® and results of reviews of Registered Email® by or at the request of customers or prospective customers would be admissible in the context of such testimony.

- Each e-mail that routes through Rpost® is assigned a unique PKI algorithm which is then retained permanently by RPost® and is subject to reuse rules meeting or exceeding industry standards;

- RPost®'s technology, business policies and practices, and physical and network facilities have been inspected and certified by certain U.S. agencies as meeting federal standards for the handling of critical and confidential messages, including a full risk assessment and sensitivity, criticality, accreditation review and privacy compliance review of the RPost® Registration System™; .

- RPost® conducts random and periodic testing, monitoring or auditing of its system to ensure that all functionality is properly operating and that no unauthorized access to the system has occurred, and the system is equipped with continual monitoring devises such as anti-virus, anti-spyware, etc.;

- RPost® tracks and records all changes and updates to hardware and software that occur along with all instances of access to its systems and these logs are included in the monitoring process;

- RPost® maintains logs of client usage; and

- RPost® maintains its system with appropriate disaster recovery and business continuity backup systems and provisions to ensure its continued functioning during power and other disruptions, and since going on-line RPost® has not experienced any disruption-related downtime.

- Aside from ensuring the integrity of the information within the RPost® system, many of its safeguards also serve to keep the electronic system in good repair;

- The system verified that the e-mail was authentic, contained a true and accurate representation of the message as it was sent to the recipient, and contained true and accurate embedded and transaction metadata;

- RPost®'s standard process was used in the generation of the Registered Receipt™ and the Authentication Receipt™;

- The system was in proper working order and functioning appropriately when this information was retrieved;

- The witness recognizes the e-mail exhibit, including the Registered Receipt™ and the Authentication Receipt™, as authentic, and is able to explain how he is able to recognize it based on its unique character or content; and

- Finally, given the plain English content of the Registered Receipt™ and the Authentication Receipt™, the witness will describe how to read that information and can offer it to the trier of fact to review it for themselves.

> As stated throughout the case law involving computer generated information "'reliability must be the watchword' in determining the admissibility of computer generated evidence."[77] The "factors [similar to Imwinkelried's] effectively address a witness' familiarity with the type of evidence and the method used to create it, and appropriately require that the witness be acquainted with the technology involved in the computer program used to generate the evidence."[78].

2. FRE 902

Although in a major dispute testimony may be necessary regarding the RPost® system and its integrity as noted above, RPost®'s Registered Receipts™ may also be admitted as self-authenticating documents under F.R.E. 902(7). Judge Grimm in *Lorraine*, stated that: "Extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to the following:…(7) Trade inscriptions and the like. Inscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin."[79] "Under Rule 902(7), labels or tags affixed in the course of business require no authentication. Business e-mails often contain information showing the origin of the transmission and identifying the employer-company. The identification marker alone may be sufficient to authenticate an e-mail under Rule 902(7)."[80] Judge Grimm goes on to note, however, citing Weinstein again, the problem that one does not know the author of an e-mail.[81]

RPost®'s Registered Receipt™ e-mail and Authentication Receipt™ e-mails offer the best case for the self-authentication of the content of e-mails and their attachments through providing a coherent process incorporating controls at the data level and tamper-detectability. The Registered Receipt™ preserves the contents of the e-mail and of its attachments in an automatically encrypted form to which RPost® alone possesses the decryption algorithm, and the Authentication Receipt™ compares the proffered e-mail to the decrypted original using hash values and other replicable cryptographic processes.

---

[77] *Swinton,* p. 812.

[78] *Id.*, 813, 814.

[79] *Lorraine*, p. 549.

[80] *Id.*, quoting *Weinstein's Federal Evidence* § 900.07[3].

[81] *Weinstein's Federal Evidence* § 900.07[3]. Note however, case law indicating that a logo or other indicia such as sender and recipient information that is embedded in an e-mail may be self-authenticating for the purpose of establishing the source of the e-mail, rather than the content. See *Burchfield v. State*, 892 So.2d 191 (Miss. 2004), admitted physical evidence based on a label affixed during the usual course of business for the limited purpose of demonstrating the source of the product only. We understand that RPost® has a Digital Seal electronic signature feature that provides a means of authenticating the author to the level of the author's e-mail address (or someone who has access to that address) and did develop a version of this feature with a higher level of authentication of the e-mail's author , but there was insufficient demand for this higher level version of the feature, and we would not expect such demand under existing law.

Each RPost® Registered Receipt™ e-mail provides a complete audit trail of each e-mail transaction, including all transactional metadata. Its decipherability in plain English also goes to its admissibility as a self-authenticating document under F.R.E. 902(7). As noted above, its readability by the trier of fact will also contribute to initial admissibility under F.R.E. 901(b)(9).

The final section of the Federal Rules of Evidence that might be considered for authentication of RPost® Registered E-mail® service receipts is F.R.E.902(11). As Judge Grimm noted: "Rule 902(11) also is extremely useful because it affords a means of authenticating business records under Rule 803(6), one of the most used hearsay exceptions, without the need for a witness to testify in person at trial,"[82]. although it would require written testimony. The apparent reason that one would seek to authenticate e-mail using this rule is that it permits a written declaration by a custodian rather than oral testimony. As noted at the beginning of this memorandum, however, custodianship can be a much more difficult issue with electronic than with paper documents, so any method of admitting evidence that de-emphasizes custodianship and emphasizes the self-authenticating characteristics of the ESI preserved and produced by RPost® may be beneficial in many circumstances. *DirecTV, Inc. v. Murray*[83] provides an example of admitting e-mail based on F.R.E.902 (11). This rule addresses:

> Certified domestic records of regularly conducted activity. The original or a duplicate of a domestic record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority, certifying that the record-
>
> (A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;
>
> (B) was kept in the course of the regularly conducted activity; and
>
> (C) was made by the regularly conducted activity as a regular practice.[84]

"Rule 902(11) was designed to work in tandem with an amendment to Rule 803(6) to allow proponents of business records to qualify them for admittance with an affidavit or similar written statement rather than the live testimony of a qualified witness. The changes were recently adopted together in a 2001 amendment."[85] In addition to the affidavit requirements, there is a notice requirement to afford opposing parties an opportunity to review the document and affidavit to challenge its authenticity.[86] In *DirecTV, Inc.*, e-mail admissibility was characterized as a close [call]

---

[82] *Lorraine,* 552.

[83] 307 F.Supp.2d 764 (D.S.C.,2004).

[84] Federal Rules of Evidence 902 (11).

[85] *DirecTV, Inc.* p.772 at footnote 3.

[86] *Id.* p773 at footnote 4.

since the e-mails were given to the party's attorney who provided one affidavit while the records' custodian provided the second rather than a single chain of custody. The court's decision is indicative as to how carefully courts will consider the admissibility of e-mail records. [87]

## C. Conclusion

Thus RPost's Registered E-mail® service receipts are admissible as to their fact of delivery, as to their time of delivery and as to the authenticity of their content. In addition, RPost's evidentiary benefits may go beyond admissibility to the weight of the evidence.[88] By utilizing RPost® services, we would argue, not only is the e-mail admissible, but the authentication of its content and context may lend it greater credence.

We conclude that, based on the facts provided to us, RPost's Registered E-mail® service will contribute significantly in court proceedings in the United States to the authentication and admissibility of the texts of e-mails and the content of their attachments, as well as of evidence of their sending and legal receipt and the time of sending and receipt.

---

[87] The court stated:
The question is a close one, but Trone's declaration, together with Houck's affidavit, at least in this posture, satisfy the business records exception to the hearsay rule, and simultaneously solve plaintiff's authentication problem. Trone's declaration satisfies Rule 803(6) and rule 902(11) by stating that the e-mail records were kept in the normal course of Whiteviper's business and created at or near the time of the matters set forth. In other words, Trone acknowledges that Whiteviper regularly received orders by e-mail and systematically retained the e-mails as a record of the order. Trone would clearly be able to come into court and testify as to those facts were he available to do so. However, since the e-mail records changed hands, Trone hinged his declaration regarding the specific record in this case on an assurance from Houck that the record came from the collection that Trone turned over to Houck. Houck's affidavit satisfies that condition. Essentially, Trone was the custodian of the records when they were created and when they were maintained by Whiteviper, but once he turned them over, Trone ceased to have personal knowledge of the integrity of the records. Houck's affidavit is evidence of the integrity. *Id.* 772.

[88] *United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. 1988).