CONCEPT RELEASE ON POSSIBLE REVISIONS TO THE PCAOB'S STANDARD ON AUDIT CONFIRMAITONS –

Memorandum of Public Comment

To: Office of the Secretary, PCAOB
(Submitted via e-mail to comments@pcaobus.org)

From: Frank Maguire, Vice President, Business Planning & Strategy
RPost, the Registered E-mail® Company

Reference: PCAOB Rulemaking Docket Matter No. 028

Overview: Noting two divergent points of view contained in this release relating to the questioned **effectiveness** of Audit Confirmations due to **low response rates** and **PCAOB's desire to enhance audit quality and investor protection** by possibly "expanding the presumption to request confirmation of accounts receivable to also include confirmation of other significant terms in certain transactions and agreements" these comments attempt to reconcile and address those concerns and desires by speaking to the **mechanics of confirmations** using advanced technology**.**

First, to improve response rates the confirmation process must be simple to use for both sender and recipient; and reliable and trustworthy, which would promote the use of properly protected e-mail confirmations.

Second, the more "user friendly" the electronic confirmation request process the more likely a compliant response will follow thereby allowing for a broader range of information requested. Again, this would encourage the use of properly protected e-mail confirmations to insure authenticity, admissibility and enhanced accountability.

Background: ESIGN and UETA - ESIGN, the federal Electronic Signatures in global and National Commerce Act and UETA, the state-enacted Uniform Electronic Transactions Act were drafted with the intent of ensuring that electronic transactions would be afforded the same validity and legality as paper transactions – to accommodate and promote the efficiencies of digital information.

The foundation upon which these two laws are based can be broken down to the following rules:

- A record or signature may not be denied legal effect or enforceability solely because it is in electronic form;
- A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation;

- If a law requires a record to be in writing, an electronic record satisfies the law; and

If a law requires a signature, an electronic signature satisfies the law.

Digital Information – Burden of Proof: Permitting electronic records to substitute for writings serves little purpose if the records are not admissible as evidence in the event of a dispute. A record or signature may not be excluded from evidence solely because it is in electronic form. An electronic record also qualifies as an original, even if that record is not the original form of the document, and satisfies statutory audit and record retention requirements. Beyond that, the ordinary rules of evidence will apply.

APPENDIX QUESTIONS – Additional Background and Discussion on Possible Changes to AU Sec. 330

3) What direction should the standard include regarding the use of electronic confirmations and third-party service providers?

Given the technology available in the market it would not be too burdensome to require that e-mail confirmations be capable of generating legal proof that the confirmation went to the correct e-mail address, was deemed delivered under electronic law and that the subsequent electronic response, including third-party service providers, originated from the proper source and was properly controlled.

A. Delivery Proof: RPost's Registered E-mail® service provides a record of sending and receiving in accordance with UETA by recording the recipient's server's receipt thereof;

B. Content Proof: The encryption and tamper-detectability of RPost's Registered E-mail® service preserves the contents of e-mails and their attachments so as to satisfy process requirements designed under UETA or ESIGN and evidence law and to establish evidence of content;

C. Official Time Stamp: RPost's link to a trusted and objective time source provides essential and credible evidence in disputes in which the time an e-mail was sent or received is material to the case;

D. Admissible Evidence: RPost's Registered E-mail® service receipts (Registered / Authentication Receipts) are admissible as to their fact of delivery, as to their legal time of delivery and as to the authenticity of their content;

E. Functional Equivalence: RPost's Registered E-mail® service under UETA and ESIGN, can 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

F. Electronic Original: RPost's Registered / Authentication Receipt provides a true electronic original of the message content, message attachments, and transmittal meta-data including the delivery audit trail.

4) What procedures should the auditor be required to perform to address the risk that the information is not from source and the risk that the integrity of the data has been compromised?

Market product / service advances are such that an auditor should be held to a standard whereby he or she is capable of validating the integrity of both source and content of an e-mail confirmation response. RPost's Registered E-mail® service was carefully constructed in light of rapidly evolving electronic law, including applicable U.S. treatment of electronic message transmissions, information security and the admissibility of electronic evidence.

The ease of replication and modification of electronically stored information (ESI) and the openness and decentralization of networks, systems and the Internet pose significant challenges for rendering and keeping ESI secure against tampering after the relevant event, as well as for finding a credible custodian with firsthand knowledge of the process followed to create, execute, preserve, send and receive ESI, and to generate or recreate the ESI when it is to be proffered as evidence. ESI also presents opportunities for achieving reliable security, authentication and custodianship that paper documents do not. However, primarily due to its potential (1) for being created or securely bundled to contain its own internal controls, and (2) for instantaneous, reliable detection of tampering through comparison of ESI identifiers such as "hash" algorithms, Registered E-mail service takes advantage of both such opportunities to incorporate data-level controls and tamper-detectability that do not, like layers of information security, become more expensive and less effective over time.

Finally, RPost's use of hash values and public key infrastructure encryption to demonstrate that a proffered e-mail is the same as the original sent (as well as the reply where desired as an option feature) is very important given the potential for tampering with such content (again, greater than for paper mail).

10) Should the standard include the requirement for the auditor to test some or all of the addresses of confirming parties to determine whether confirmation requests are directed to the intended recipients? Why or why not?

"Yes," given the service capabilities described above it would not be an onerous task for auditors to verify legal delivery of confirmation e-mail under terms of electronic law. Registered E-mail service is capable of capturing the e-mail confirmation receipt by the recipient's server and without any compliant action on the part of the recipient, an RPostRegistered / Authentication Receipt is automatically returned to the sender to provide legal proof of delivery to the designated e-mail address. A "Delivery Failure" notice would be generated were the e-mail confirmation was not successfully delivered.

This is very important in view of the "deemer" provision of UETA – the law in 46 states – that generally deems receipt by the server as receipt by the recipient.

12) What direction is necessary in the standard regarding maintaining control over confirmations in electronic form?

Relative to e-mail confirmations and the concerns raised with respect to possible tampering of both content and recipient identity, and proof of delivery, given the capabilities that exist in the market as described above in response to questions numbered 3, 4, 10 and 12 it would be prudent to amend the standard to require that auditors, when sending confirmations by means of e-mail should be capable of:

- Verifying correct, legal receipt by the recipient's server
- Verifying original content by use of hash values and public key infrastructure encryption to authenticate confirmation sent and response received (as well as attachments) to provide necessary tamper detection
- Verifying official time stamps to fend off possible disputes as computers can be set to read any time desired as opposed to commercial paper mail services, where neither sender nor recipient controls the time stamp.