



Registered E-mail®

**Protect your Organization.
Protect Yourself.**

- ❑ E-Records Retention & Management
- ❑ E-Evidence / Litigation

CAUTIONARY NOTE: E-BUSINESS PROVIDERS & ADVISORS

BACKGROUND

Business and governmental people are soon to realize that along with the many intended benefits derived from electronically generated business and filings, come unintended consequences. Commerce and government have traditionally relied upon paper documents for records and defense: characteristically tangible, complete, readily accessible and defensible. Electronically stored information, however, requires more sophisticated treatment, given its nature: intangible, amorphous, without context and oftentimes impossible to authenticate or re-present the "original."

While electronically driven transactions allow for increased productivity, reduced costs and enhanced customer/taxpayer and information access, such benefits do not come without a price. The trade-off is that many users are experiencing a reduction in management and reporting controls, reduced employee accountability and inadequate records retention.

The practical effect is that inadequate e-records systems, compounded by evolving e-discovery and admissibility issues, combine to jeopardize management's ability to establish a successful defense against all manner of legal and regulatory challenges.

NEW LEGAL REQUIREMENTS DEMAND PROPER RECORDS RETENTION & MANAGEMENT SYSTEMS

1) Sarbanes-Oxley

- ❑ Section 103: maintain audit-related records for up to 7 years
- ❑ Section 404: certify effectiveness of internal controls

2) SEC

- ❑ Rule 17a-4: Broker/Dealer communication preservation

3) USA Patriot Act, Title III

- ❑ 31 CFR Part 103: Anti-Money Laundering regulations

4) Zubulake V and the Philip Morris cases

- ❑ The requirements of preserving e-mail are becoming clearer, and the penalties are becoming more visible and demonstrable. Particularly the Zubulake decision shows that the days when an attorney or his client could claim ignorance are no longer a valid defense. Consequently, a company policy of deleting e-mail on a regular basis is not a reasonable defense against a legal challenge. Business and important e-mail must be retained as an official record for proper legal defense.

RECENT REGULATORY CAUTIONS AND STUDY RELATING TO ELECTRONIC TRANSACTIONS

1. Office of the Comptroller of the Currency Advisory Letter 2004-9 (6/9/04) "Electronic Record Keeping." The OCC Advisory Letter highlights issues regarding bank electronic record systems in light of the E-SIGN Act with respect to electronic record keeping systems. [Note: while this advisory relates to banks, the underlying message applies to all who enter into electronic transactions because of the statutory changes to the legal framework relating to electronic records.] The main thrust of the advisory is to highlight the importance of establishing a proper recordkeeping management system for all electronic delivery systems. The OCC underscores the fact that the E-SIGN statute does not resolve all legal or practical issues relating to electronic records. Nor does E-SIGN guarantee the admissibility of

electronic records in litigation, so the burden is on bank management to consult with legal counsel to ensure that its electronic record retention systems, containing records that banks may need in litigation, are sufficient to ensure admissibility in relevant courts. "This is important because the practical effect of having electronic records that are not admissible into evidence in judicial proceedings may be to render the electronic contract or record effectively unenforceable."

2. Pew Internet & American Life Project, "Instant Messaging gains a following in the US Workplaces" – This recent study found that 21% of 53 million American, adult Internet users use Instant Messaging at the office. Of concern is the trend towards more business/government people relying upon IM to shortcut official processes that otherwise would be more appropriate and more importantly, establish a proper transaction record.

3. Federal Deposit Insurance Corporation (FDIC) Financial Institution Letter 84-2004 (7/21/04): "Guidance on Instant Messaging" – The FDIC cautions that... "The risks associated with the use of IM include revealing confidential information over an unsecured delivery channel... IM is vulnerable to denial-of-service attacks, hijacking sessions and legal liability..."

CONCLUSION

We are at a point in time where our legal system of evidence is being tested because of the movement from paper to electronic records. "Authenticity" is key in determining that the underlying information found in a record is what it purports to be. Absent the ability to authenticate information, the search for truth becomes impossible. Unlike physical evidence of years past, today's electronic records can be easily manipulated by anybody, which is one of the many benefits of this intended design feature. This conundrum partially explains the recent focus on the nature of electronic evidence and the conclusions that are prompting the underlying law of evidence to adapt. Likewise, information's new electronic phase is responding with technologies that can record an entire electronic transaction as a digital snap-shot, that can meet the burden of proof as electronic evidence.

It is important for business and government people to understand that legal requirements dealing with electronic transaction records continue to evolve and that while electronic participants may take comfort in state of the art information systems, it may be a false comfort. True protection comes from a recordkeeping system that is capable of storing, retrieving, time stamping and authenticating original electronic transactions. Keep in mind, a record of what was sent and when is only part of the transaction. One would also need a record of whether it was received, by whom, and when.

It is important to appreciate that the courts are grappling with e-discovery and admissibility issues that are not always clear-cut.

- ❑ While computers can create digital or paper records, enterprise-wide databases do not.
- ❑ Information Management systems support real-time business processes by creating and managing information; they do not provide a recordkeeping function. (One should be careful not to confuse Information systems with Recordkeeping Management systems that actually provide evidence of a transaction.)
- ❑ Business/government information needs, forms and processes change constantly.
- ❑ Systems are upgraded and replaced regularly.
- ❑ Most information system backups are haphazard and inaccessible for record retrieval purposes.
- ❑ Questions of security and reliability impact records management.
- ❑ Informal business/government processes that might be good for smooth transactional operations and public relations usually generate "non-records" that, if created, are poorly managed by Recordkeeping Management systems: e-mail, Instant Messaging, voice communication and virtual meetings.

Legal Protection is Critical: Provisions of electronic law and recent court decisions underscore the fact that E-Business/Government systems require proper **transaction documentation**, and a reliable **Recordkeeping Management** system that can record, retrieve and authenticate electronic transactions (both content of e-mail and attachments, and time sent and received) involving important business/government communications and transactions.

COMMON MISCONCEPTIONS

- ❑ Maintaining copies of standard e-mails sent would not withstand a legal challenge if content or time were questioned due to the simple text format that can be altered easily.
- ❑ Attaching a "sent" affidavit to standard e-mail, as presumed proof of sending proves nothing about whether it left the sender's computer, mail server or was received by the intended recipient's mail server.
- ❑ Anyone can drag a file to his or her "sent" folder, alter the content and time and with a few clicks of the mouse print a copy and attempt to represent it as fact.

E-mail Management Systems

- ❑ IT e-mail management systems might store standard e-mail and lock it down in order to convey a sense of accountability and recordkeeping, however, such files are plain text that can be altered and therefore subject to dispute. Such systems cannot prove receipt and the retrieval process is extremely time-consuming and in vain, as the evidence produced will not withstand a legal challenge.

Standard E-mail "Read Receipts"

- ❑ Depend upon the recipient's computer settings, systems and action to generate a receipt.
- ❑ Provide no evidence of delivery if the recipient does not act to return the receipt to the sender.
- ❑ Provide little evidentiary value as the plain text format can be edited/changed easily.
- ❑ Provide no authentication of the body text of e-mail, or attachments transmitted.
- ❑ List times that can be manipulated easily.
- ❑ Work generally only for internal e-mail and not external Internet e-mail.

SOLUTION: RPOST® REGISTERED E-MAIL® (WWW.RPOST.COM)

Tested and used by the federal government: The RPost® Registered E-mail® system is a service that has been tested, accredited and is used daily by U.S. Government customers, such as the U.S. Government Accountability Office, an arm of the U.S. Congress. It addresses the two most common complaints directed at businesses and government agencies that routinely use e-mail:

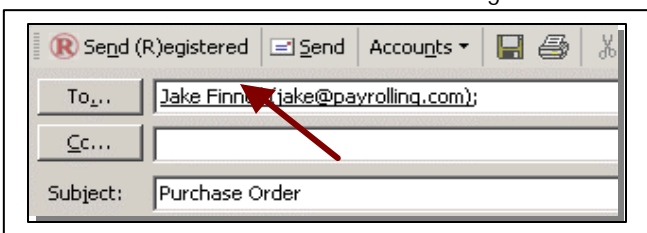
- ❑ "I didn't get your e-mail!"
- ❑ "I got your e-mail but that is not what it said!"
- ❑ And, it provides the sender with assurance of delivery, peace-of-mind, confidence in critical transmissions, and protection in case of a future dispute.

Statutory requirements: Legal opinions stipulate that the RPost® Registered E-mail® service meets both federal and state electronic laws relating to evidentiary proof of the delivery (official time sent and received) of each Registered E-mail® message and the integrity of the content and attachments of each Registered E-mail® message. In short, the Registered Receipts™ e-mail will withstand a legal challenge.

Where there is a legal requirement for a document to be retained as originally created, in writing, or sent and received in electronic form, that requirement will be satisfied by retaining RPost® Registered Receipt™ e-mail of the electronic transmission.

Explanation of Registered e-Mail® and how Registered Receipts solve recordkeeping and evidentiary problems:

RPost® Registered e-Mail® is a simple, elegant way for serious e-mail users to address the many shortcomings of standard e-mail that could leave a business/government transaction vulnerable to challenges.



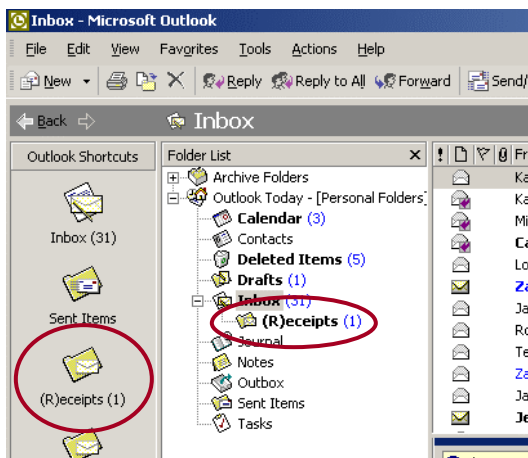
- ✓ **Simple to Use** (Just click the "Send Registered" button)
- ✓ **Intuitive for the Sender**

RPost® Registered E-mail® provides the sender of an e-mail with legal proof of authorship, content, sending and receiving to any Internet address, with the atomic-clock time stamp. This digital snap-shot of the entire delivery transaction, including attachments, is compressed, protected and folded into a tamper-proof Registered Receipt™ e-mail that is returned to the sender by e-mail.

The RPost® system does not require the recipient to have any special software or take any compliant action. It generates evidence of the transaction, proof of delivery, by means of a Registered Receipt™ e-mail returned to the sender (and to the recipient as an optional feature). RPost® does not retain a copy of the original transaction so it would not be discoverable in a dispute.

The Registered Receipt™ e-mail is irrefutable, durable, and self-contained evidence of the entire electronic transaction.

All Registered Receipt™ e-mails are stored in an automatically created "Receipts" subfolder of the sender's inbox that can be archived according to the policies of the company or agency. In addition, a copy of the Registered Receipt™ e-mail can be automatically sent to another e-mail address (such as receipts@agency.com) for permanent storage and routine back-up or in the event an employee is terminated, resigns or upgrades their system in the future. For documentation management purposes, the Registered Receipt™ e-mail can be tagged with any identifying characteristics, such as a client code, customer ID number or project code for simple, fast retrieval of any Registered Receipt™ e-mail message.



Registered Receipt™ e-mails automatically go to a newly created "(R)ceipts" folder within the Inbox for storage and a shortcut is created on the Outlook Shortcuts bar.

In addition, the Registered Receipt™ e-mail is durable and can be forwarded to any party who disputes the delivery or content of an e-mail message. The Registered Receipt™ e-mail enables the complainant to authenticate the delivery or content of the disputed message by forwarding the Registered Receipt™ e-mail to a special verification address, which in turn regenerates the original e-mail and all attachments and returns the original information by e-mail to the complainant. [Note: an added feature of Registered E-mail®, the Digital SealSM, if used by the sender, will likewise allow any recipient to verify authorship, transmission time, and content of the original message and attachments, by forwarding the Digitally SealedSM, Registered e-Mail® message to the verification address. Where the original Registered e-Mail® message has been sent using the Digitally SealSM service, the recipient does not need the sender's Registered Receipt™ e-mail in order to take advantage of the verification process.] In fact, a Registered Receipt™ e-mail can be put on a CD and brought to a courtroom or to an arbitrator where any party can authenticate the delivery and content of a contested Registered e-Mail® message.

Benefits derived from using RPost® Registered Email®: RPost® Registered E-mail® messages save money, increase efficiency/accountability and protect the sender and his or her organization, while enabling the movement of more transactions from paper/fax/mail to electronic delivery systems. Furthermore, it reduces manpower, postage, printing, telecom, storage, archiving and dispute resolution costs.