

# New Jersey Law Journal

VOL. 202 - NO 1

OCTOBER 4, 2010

ESTABLISHED 1878

IN PRACTICE

## CIVIL PROCEDURE

### You've Got Mail: From the Pony Express to the Digital Highway

By Michael W. Hoffman

As a matter of proofs, how does electronic mail compare to traditional paper mailing in view of the evidential presumption that most ordinary mail is received? Stated lightheartedly, in a court of law, how may a computer and the electronic highway measure up against letter carrier Cliff Clavin from "Cheers" on his route in Boston, Massachusetts?

Pursuant to N.J.R.E. 301, by operation of law, there is a presumption that most ordinary mail posted is delivered. This presumption rests on the rational basis that letters so mailed are almost always properly delivered. Accordingly, proof of mailing, correct addressing and due posting of a letter raises such a presumption. *SSI Medical Services, Inc. v. State, Dept. of Human Services, Div. of Medical Assistance and Health Services*, 146 N.J. 614, 621 (1996). The presumption is rebuttable and may be overcome by evidence that the mailing was never

*Hoffman is an attorney with Maselli Warren in Princeton. The author would like to thank George Wade, the director of digital forensics and IT risk management group of Sobel & Co. in Livingston, for his contributions to this article.*

in fact received by the addressee. Commonly, such presumption of receipt is referred to as the "mailbox rule."

In view of technological advances, in the 1996 *SSI Medical Services, Inc.* decision, the New Jersey Supreme Court dropped footnote 1 reading:

In all cases, courts should evaluate the nature and worth of the corroborative evidence offered to determine whether it meets the preponderance of the evidence standard and raises a presumption of mailing and receipt. As the forms of communication change, different proofs will have to be established in order to demonstrate mailing. One of the fastest growing methods of communication is electronic mail or e-mail. E-mail is a computer-to-computer version of the postal service that enables users to send and receive messages and in some instances graphics or voice messages, either to individual recipients or in broadcast form to larger groups. In order to establish proof that electronic messages have been sent, courts may look, for example, to proof of electronic

mail return-receipt or to confirmation of downloading or printing. As new technologies continue to develop, the sort of proofs required to demonstrate proof of mailing and receipt will likewise change.

While the jurisprudence of evidence based on a common understanding of computers seemingly supports the ready extension of the "mailbox rule" to electronic mail, the question presented is whether computer forensics may provide the corroborative evidence necessary to support an equal presumption that electronic mail is almost always properly delivered or received.

Of course, the ordinary paper mail operation of the United States Postal Service (USPS) is subject to system failure by way of internal or external human error, for example, a dropped and lost letter or an incorrect addressing. Private electronic mail operations are subject to those same failures along with others more complex to the electronic highway as compared to the route of Postman Clavin. Some of these failures may be the consequence of not only human or technical error, but also technical design or mischievous conduct. From this, there are proof problems unique to electronic mail technology.

As examples of human or technical error, an e-mail may fail because a file attached is too large for the receiving system to handle. With proper postage, an ordinary mailing makes its way down a bituminous concrete highway no matter its size. Further, the electronic

mail system of an intended recipient may be set to decline electronic mail from a user who is "not trusted," such as for mail identified as "spam" or a user who is "black listed" by an end user through a software program. But, no matter the source or kind, ordinary mail, including junk and unwanted mail, is placed in a recipient's mailbox, for the postman does not discriminate.

Proof problems are significantly unique to electronic mail as compared to paper mailings. To prove an electronic mail message was sent requires a thorough analysis of message "headers," which necessarily requires the cooperation of the alleged receiving party. Beyond the addressee's "To:," "Cc:" and "Bcc:," the originating "From:" address, and "Subject:" fields being readily apparent, the header fields containing Internet Protocol (IP) addresses of the originating gateway address (the address of the e-mail server visible to the information superhighway), the destination gateway address, and any intermittent servers that transferred the message must be forensically examined as well.

For example, Mr. Smith with Yahoo! Mail sends a message to Mrs. Rogers, who is within the walls of XYZ Company. Since Mr. Smith used Yahoo! Mail, he accessed Yahoo! Mail after first accessing the Internet via an Internet Service Provider (ISP), such as Verizon, or through a free wireless hotspot situated, for example, at a local coffee shop or within a hotel.

Tracing the message path from Mrs. Rogers back to Mr. Smith involves several steps. First, the original message headers must be obtained from Mrs. Rogers through her employer, XYZ Company.

Once obtained, the message headers must be reviewed for the IP address assignments of the servers that transported the message, along with the associated date and time stamps. Consideration must be given to the path the message traveled and the dates and time stamps must be converted to a consistent timestamp, such as coordinated universal time (UTC). In this example, the message

headers will indicate that the e-mail was sent via Yahoo! servers. Consequently, litigation issues may arise from the necessity of serving a subpoena on Yahoo! Inc. to obtain the connection records and account information with converted date and timestamps. Here, the subpoenaed documentation may demonstrate that the subscriber information for the Yahoo! Mail account is fictitious although it will nevertheless indicate the IP address for the connection to Yahoo! Mail.

Next, a subpoena must be served on the ISP to obtain that subscriber information for the connection to Yahoo! Mail. If Mr. Smith used a Verizon account, the subpoenaed documentation will show the subscriber information for that account, which may or may not be the individual who physically sent the e-mail. If Mr. Smith used a free Internet connection at a hotspot, the subpoenaed documentation will show an IP address resolving back to the ISP providing access at the coffee shop or hotel, which likely leads to a dead-end in an attempt to confirm Mr. Smith as the sender.

Here, it is important to note that unscrupulous individuals may use an "anonymous remailer" or "anonymizer/anonymouse proxy" service to cloak their activity on this electronic highway. An anonymous remailer service is a server computer which would receive the message from Mr. Smith and forward it on to Mrs. Rogers without revealing the necessary header information to determine the origination of the e-mail. An anonymizer or anonymous proxy allows a user to make his Internet activity untraceable. For instance, Mr. Smith accessing the Internet through such a tool to use Yahoo! Mail would cloak the ISP involved in that transmission. Such mischievous conduct obviously complicates if not precludes forensic investigation and legal process.

As for the probative value of "electronic mail return-receipts," there is also significant difficulty in proving actual receipt of electronic mail. Although *SSI Medical Services, Inc.* noted proof of receipt by way of electronic mail "return-receipt" almost as a matter of fact, those

return receipts may be incorrect or manipulated electronically. For instance, a return receipt may only indicate that the message was received by the recipient's e-mail system. However, it may never reach the targeted recipient if software on the receiving server incorrectly identifies the message as "spam." Alternatively, some "e-mail clients" (i.e., software running on a recipient's computer) may capture the return-receipt prior to transmission and query the end-user for permission to send the receipt. In such instance, the end-user may selectively decide whether to acknowledge receipt of the e-mail message. If the end-user determines not to permit a return-receipt to issue, the end-user will have in fact received the e-mail, but, denied proof of that receipt from issuing out of the email client.

In view of the above state of technology, absent computer forensics analyzing latent evidence on the electronic highway satisfying a preponderance of evidence standard, receipt of electronic mail should not be presumed. As a matter of technology, there is very little proof towards an evidential presumption in the mere testimony that an author of an electronic mail message correctly inserted the e-mail address of an intended recipient and clicked the "send" button on his computer screen. Furthermore, the mere production of a print out of a return receipt issued for an e-mail or the simple demonstration that such an electronic mail was "downloaded" or "printed" should not invoke the mailbox rule's application. Computer forensics should be called upon to demonstrate that an e-mail was actually generated by the purported sender, traveled properly upon an electronic highway and was received in fact by its intended recipient. In this regard, with or without the benefit or necessity of a presumption charge, it is likely such corroborative evidence as a matter of law effectively goes beyond support for a "presumption" to proof in fact of dispatch and receipt. ■