TRANSMITTING TRANSACTIONAL AND COMMERCIAL E-MAILS UNDER CAN-SPAM, STATE, AND CANADIAN LAWS

Prepared by Mitchell N. Roth, Esquire

Roth Doner Jackson, PLC
mroth@rothdonerjackson.com

SOCAP 2014 Executive Series on Regulatory Issues
As e-mail has become an increasing part of our lives, the benefits of using e-mail to communicate with customers continues to grow. The use and transmission of e-mail is regulated at the federal level by the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (“CAN-SPAM”). Although this legislation preempts most state laws, many state laws remain applicable. Additionally, earlier this year, the Canadian Anti-Spam Legislation (“CASL”) went into effect which significantly limits the ability of companies to transmit e-mails for marketing purposes. Given the abundance of laws regulating the transmission of commercial e-mails, companies must understand how these laws restrict their ability to interact with their customers.

The CAN-SPAM Act regulates fraudulent, unauthorized and unwanted e-mail. Companies that violate the Act are subject to penalties in the amount of $16,000 per violation. Most provisions of the Act apply only to commercial electronic mail messages (“CEMMs”), while some also apply to transactional/relationship messages. CEMMs are defined as messages whose primary purpose are to advertise or promote commercial products or services. Transactional/relationship messages include messages whose primary purpose relates to an already executed transaction such as those messages that provide warranty information for a previously purchased product, notification of a change in terms or status of an account, account information, or delivery information.

Special consideration must be paid to messages that contain both commercial and non-commercial content. Such dual purpose e-mails will be deemed CEMMs if their primary purpose is commercial. Factors to consider in making this determination are whether the subject lines lead recipients to believe that the messages contain solicitations, the proportion of the overall messages consisting of commercial materials vs. transactional materials, the placement of the commercial language component in relation to the transactional component, relative font size, color, type face, etc.

Regardless of the type of message, e-mails may not contain materially false or misleading header information, and thus may not misrepresent the identity of the person that originated the message. CEMMs have additional requirements: CEMMs may not have a deceptive subject line, their bodies must clearly and conspicuously identify themselves as advertisements or solicitations, and they must contain a valid physical postal address of the sender.

Most importantly, all CEMMs must include an opt-out mechanism to assist the recipient in being placed on the sender’s do-not-e-mail list. This may be through a reply to the original e mail address or through another web-based mechanism. This mechanism must remain available for at least 30 days after the CEMM is sent. If a user makes an opt-out request, the sender must honor it within 10 business days of that request. The opt-out mechanism may provide the user with the ability to opt-out of some messages while continuing to receive other messages, but must include the option to opt-out of all CEMMs.

The federal CAN-SPAM law preempts most state laws on the same subject. However, it does not preempt laws that prohibit falsity or deception, or state laws that do not specifically and exclusively apply to e-mails. Therefore, the provision of the California e mail law, for example, that prohibits the transmission of messages containing false subject lines continues to apply. The California law provides for both actual damages and liquidated
damages in the amount of $1,000 per e-mail, up to a maximum of $1,000,000 per incident. However, if the sender of the CEMM has established and implemented reasonable procedures to prevent violations of the law, the liquidated damage component is reduced to $100 per e-mail, up to a maximum of $100,000 per incident. It is therefore recommended that companies that communicate via e-mail with current and prospective customers adopt and implement such policies.

The Canadian e-mail law, CASL, became effective on July 1, 2014. It applies to any e-mail accessed by computer systems in Canada. While CASL is similar to CAN-SPAM in many respects, it has one glaring difference – companies are prohibited from sending unsolicited e-mail solicitations to individuals unless they have provided prior express consent to receive e-mail marketing messages. However, there is no restriction on non-solicitous messages. Keep in mind, though, that a similar analysis will be required in the context of dual purpose messages. Express consent may be obtained either orally or in writing, but if received orally it must either be verified by a third party or contained on an unedited audio recording. Written consent may be either physical or digital, and though it may be part of the same form, it must be set apart and granted separately from any other consents. At least for an initial transition period, express consent may be implied based upon a business relationship between the sender and the recipient within the previous two years.

As companies continue to rely on e-mail to interact with their customers, more scrutiny is (and will be) placed on those emails to ensure compliance with all applicable laws. Government regulators and private plaintiffs have been successful in policing the legislative requirements. The implementation of effective policies and procedures is crucial to help protect entities from damaging lawsuits arising out of their customer communications.