BNA, INC.

WHITE COLLAR CRIME REPORT

BNA Employee-Owned Since 1947

VOL. 3, NO. 18 600-602 **AUGUST 29, 2008**

PRIVACY

Good E-Mail Practices Will Help to Avoid 'Smoking Gun' E-Mails

BY JAMES I. GLASSER, JOSEPH W. MARTINI, AND JODY ERDFARB

E-mail has become the preferred method of communication in most business settings and has developed a vocabulary and syntax all its own. E-mail is a remarkably easy and efficient mode of communication. However, because e-mail is less formal, thoughts are often conveyed absent the care, discernment, and social governors that regularly accompany face-to-face communication and formal correspondence. As a result, the phenomenon of the ''smoking gun'' e-mail has emerged. The smoking gun e-mail reads like a water cooler conversation; it is unfiltered and rife with offhand and ill-considered remarks. Such banter, memorialized in black and white, divorced from textual and temporal context, can become incendiary to individuals, companies, and organizations.

This is not a new phenomenon, but recent events demonstrate that not every business and compliance officer has made e-mail training a priority. The scathing report on credit rating agencies issued July 8 by the Securities and Exchange Commission based very predominantly on e-mail evidence, the June 18 indictment of Bear Stearns traders Ralph Cioffi and Matthew Tannin, and the Justice Department's June 3 settlement with Faro Technologies Inc. are recent testaments to the phenomenon of the smoking gun e-mail and the importance of an effective training and compliance program addressing e-mail.

Each of us has committed an e-mail faux pas, such as omitting an attachment, accidentally replying to ''all,'' or hitting ''send,'' only to immediately wish the message could be recalled. This ''hair trigger'' remorse was experienced by the University of California, Berkeley, director of admissions after he accidentally sent an e-mail to all 7,000 applicants to the law school congratulating

Jim Glasser was a federal prosecutor in Connecticut for 19 years, where he held senior positions including counsel to the U.S. attorney, criminal chief, and chief of appeals. Joe Martini was a federal prosecutor in Connecticut for nine years and investigated and prosecuted diverse cases including mail and wire fraud, tax cases, international money laundering cases, health care fraud, and many others. Glasser and Martini are partners in the White Collar and Investigations Practice Group at Wiggin and Dana, New Haven, Conn. Jody Erdfarb is a health care associate in the firm's Stamford, Conn., office and assisted in the preparation of this article.

 ISSN 1559-3185

them on their admission.[1] Such e-mails are often embarrassing, but are not nearly as damaging as the smoking gun e-mail.

The legal landscape is littered with examples of the devastating evidence created by e-mail. Judging by recent events, not everyone has gotten the message. Authors of smoking gun e-mails are either oblivious or purposefully obtuse to the devastating nature of the evidence they are creating, which can ultimately be introduced against them and their employers. For example, not long ago Merrill Lynch entered into a multimillion-dollar settlement with then-New York Attorney General Eliot Spitzer after the AG's investigation revealed private e-mails from Merrill Lynch financial analysts variously describing publicly recommended stocks as ''dogs,'' ''junk,'' and ''crap.''[2]

A recent indictment alleges that five years after the conduct in the Merrill Lynch case, Bear Stearns traders Cioffi and Tannin sent e-mail messages to one another describing the subprime market in which they invested as ''pretty damn ugly,'' ''toast,'' and making them ''sick to [their] stomach,'' while at the same time they were telling their investors the market presented ''an awesome opportunity.''[3] The e-mails are quoted in the text of the indictment and are the foundation on which the prosecution rests.

In June, the Justice Department settled an investigation into Faro Technologies Inc. involving violations of the Foreign Corrupt Practices Act. The investigation turned up e-mails between a Faro employee responsible for sales in China and a regional sales manager inquiring whether he could ''do business the Chinese way,'' which was later explained to mean paying bribes and providing things of value to private and government customers. A later e-mail between the two, quoted in settlement documents, is a candidate for inclusion in the pantheon of smoking gun e-mails: ''Actually, I wish we didn't have to pay this bribery. While in Bejing I saw in the news in CCTV that the Chinese government will start enforcing the laws against bribery too. Be careful!!!''

The recent SEC report criticizing prominent credit rating agencies, based in part on a review of e-mails, claims that the agencies flouted conflict-of-interest rules and did not routinely conduct the due diligence required to properly rate securities. For example, one analyst's e-mail read: ''Let's hope we are all wealthy and retired by the time this house of cards falters.'' Another e-mail read: ''It could be structured by cows and we would rate it.''[4]

The maker of Fen-Phen, a weight-loss drug, felt the impact of the smoking gun e-mail when it was forced to settle a lawsuit concerning the safety of the drug after an e-mail from a callous Fen-Phen employee was unearthed wondering, ''Do I have to look forward to spending my waning years writing checks to fat people worried about a silly lung problem?''[5]

Other examples abound. An Arthur Andersen LLP executive involved in the Enron debacle gave an instruction to his assistant that ended up in a damning e-mail following receipt of a federal subpoena. The assistant broadcast an e-mail to employees stating: ''Per Dave—no more shredding . . . .''[6] The e-mail led prosecutors to conclude that Arthur Andersen had been destroying documents, and it was damning evidence that contributed to the firm's conviction on obstruction-of-justice charges.

Despite innumerable e-mail horror stories, e-mail writers inexplicably continue to believe that their writings are shrouded in secrecy, will only be read by the intended recipient, and are evanescent and disappear into the ether. Just the opposite is true. E-mails spread like viruses, withstand efforts at deletion and erasure, and show up at the least opportune times.

Because of its evidentiary power, the smoking gun e-mail has become the darling of prosecutors and plaintiffs' lawyers, and it is often the first place scoured for evidence. Tom Greene, a California deputy attorney general, referred to e-mail in general as ''the gift that keeps on giving.''[7] The Bear Stearns indictment and the Faro Technologies settlement are just the latest example proving this point.

Understanding the risks and costs of careless e-mail communications and developing compliance strategies to avoid smoking gun e-mails are imperative for any organization. A strict e-mail policy is a critical component of all efforts to curb the risk of smoking gun e-mails. Employees should regularly be instructed not to use e-mail for personal use and to think critically about the content of each e-mail before it is sent. Employees who are regularly reminded that e-mails, even those deleted from a desktop, are saved on backup tapes and are subject to production are less likely to write smoking gun e-mails. Depending on the sensitivity or potential value of information communicated through e-mail, consideration should be given to employing encryption technology that makes the content of e-mail unreadable to all but the intended recipient.

Training on these issues is imperative. It is hard to change bad habits and hard to convince e-mail authors that their messages, even those written on their private computers, are not immune from review by the government or by opposing counsel in litigation. There are cer-

---

[1] Todd R. Weiss, *Accidental e-mail congratulates 7,000 on admission to UC Berkeley law school,* Computer World, Feb. 24, 2006, available at http://www.computerworld.com/softwaretopics/software/groupware/story/0,10801,108992,00.html.

[2] Daniel Kadlec, *Buy! (I Need the Bonus)*, Time, May 12, 2002, available at http://www.time.com/time/magazine/article/0,9171,237027-1,00.html.

[3] Landon Thomas Jr., *Prosecutors Build Bear Stearns Case on E-Mails,* New York Times, June 20, 2008, available at http://www.nytimes.com/2008/06/20/business/20bear.html?_r=1&oref=slogin.

[4] *Summary Report of Issues Identified in the Commission Staff's Examinations of Select Credit Rating Agencies*, SEC Office of Compliance Inspections and Examinations Division of Trading and Markets and Office of Economic Analysis, July 2008, available at http://www.sec.gov/news/studies/2008/craexamination070808.pdf.

[5] Carl Elliott, *Pharma Goes to the Laundry: Public Relations and the Business of Medical Education*, Hastings Center Report, Sept.-Oct. 2004, available at http://faculty.uccb.ns.ca/sstewart/Pharma%20goes%20to%20the%20laundry%20Elliott%20Hastings%20Centre%20Rep%201.pdf.

[6] *Ties to Enron Bind Andersen*, Chicago Tribune, Sept. 3, 2002, available at http://www.chicagotribune.com/news/chi-0209030210sep03,0,7490166.story?page=1.

[7] *Gathering the E-Evidence: In the E-Mail Age, Scraps of Conversation are Everywhere*, Associated Press, CBS News, Aug. 16, 2002, available at http://www.cbsnews.com/stories/2002/08/16/tech/main518981.shtml.

  WCR ISSN 1559-3185

tain black-and-white issues on which employees can and must be trained.

Attorney-Client Privilege

Employees should be instructed on the contours and requirements of the attorney-client privilege. Broadly stated, in order for the privilege to attach, an e-mail communication between an attorney and a client must be intended to be a confidential communication made for the purpose of securing legal advice, and it cannot be exposed to a third person or made for the purpose of committing a crime or tort. Thus, not *every* communication between an attorney and a client is subject to the privilege, and merely typing ''attorney-client privilege'' in the subject line of an e-mail or ''cc-ing'' an attorney will not protect an e-mail from review by others.

Employees should be sensitive to the fact that even the act of sending an e-mail communication through a workplace e-mail system can destroy the privileged nature of an attorney-client communication. This was highlighted recently in *Scott v. Beth Israel Medical Center*, where the plaintiff, a hospital employee, assumed that e-mails he sent to his attorney through the hospital's e-mail system pertaining to his lawsuit would be privileged.[8] A court ruled, however, that his e-mails were not subject to attorney-client privilege because there was no expectation of privacy in the hospital's e-mail system. The hospital's policy explicitly stated: ''Employees have no personal privacy right in any material created, received, saved or sent using Medical Center communication or computer systems. The Medical Center reserves the right to access and disclose such material at any time and without notice.'' In reaching its decision, the court explained, ''the effect of [such] an employer e-mail policy . . . is to have the employer looking over your shoulder each time you send an e-mail. In other words, otherwise privileged communication . . . would not have been made in confidence . . . .''[9]

Data Privacy Issues

Transmitting confidential information through e-mail, whether patient health information or proprietary business information, is a risky practice that can expose a company to significant liability. Employees should be made aware of legal requirements to safeguard confidential information and should be made aware of data breach statutes that have been enacted in many states. Health care providers must be sensitive to the Health Insurance Portability and Accountability Act, which prohibits the disclosure of personal health information for purposes unrelated to health care and mandates the imposition of certain security measures to protect the confidentiality of protected health information.

In short, companies should be sensitive to the type of information likely to be transmitted by e-mail, and e-mail use policies should include restrictions on the contents of e-mail transmissions.

Document Retention and Destruction

Not all smoking gun e-mails achieve their full destructive potential. Many such e-mails are deleted pursuant to a standing company document retention and destruction policy. Employees should be trained on these policies. Organizations are permitted to periodically destroy e-mails so long as the destruction is performed pursuant to a policy that is consistent and reasonable. Furthermore, retention/destruction policies must be instituted in good faith, not specifically to avoid the discovery of damaging e-mails.

Discoverable sources of information should be identified, and retention policies should be designed to keep only what is required by law or what is needed for ongoing business purposes. Most health care providers, for example, are subject to specific legal or regulatory document retention requirements. Other industries are similarly subject to unique retention requirements. Documents and electronic records that are not designated for retention should be regularly destroyed pursuant to established policy.

It is important to develop a retention and destruction policy that can and will be followed. Corporate officers, corporate counsel, and information technology staff should all be involved in formulating these policies.

Most important, these policies must provide that destruction is to be suspended if litigation is anticipated or initiated. In *Kucala Enterprises Ltd. v. Auto Wax Co.* and *United States v. Triumph Capital*, for example, computer forensics experts were able to recover electronic files that had intentionally been deleted in anticipation of litigation using programs named, respectively, ''Evidence Eliminator'' and ''Destroy It!''[10] The damning implications of these efforts to destroy evidence underscore the validity of the old saw about the cover-up being worse than the crime. Employees should be trained on the importance of litigation-hold notices and the devastating impact of failure to heed such notices. Handing over a smoking gun e-mail in response to a subpoena and trying to explain the e-mail in context is a much better alternative than the negative inference that will be drawn from attempting to explain its destruction.

With these considerations in mind, we offer the following 10 tips. While these tips are important, the ultimate test is the ''*New York Times* test'': Never send an e-mail that you would not want to see on the front page of the *New York Times*.

1. Always check the ''To'' field.
2. Use the ''Reply All'' button with extreme caution.
3. If there are multiple recipients, make certain it is OK for each recipient to know about the other. (Think about the psychiatrist who sent her patients a broadcast e-mail notifying them that she would be on vacation but failed to hide the addressees.)
4. Reread an e-mail before sending.
5. Consider whether sending the e-mail will impact privilege issues or result in the dissemination of privileged, regulated, or proprietary information.
6. Remember that pressing delete is not equivalent to shredding.
7. Never use office e-mail for private purposes.

[8] *Scott v. Beth Israel Med. Ctr.*, 2007 WL 3053351 (N.Y. Sup. Ct. 2007).

[9] Id.

[10] *Kucala Enterprises Ltd. v. Auto Wax Co.*, 2003 WL 21230605 (N.D. Ill.); *United States v. Triumph Capital*, 260 F. Supp. 2d 462 (D. Conn. 2002).

8. Always scroll to the end of the e-mail before sending.

9. Regularly review your saved folders and delete unnecessary information.

10. Attorney-client privileged e-mails should be segregated from other communications.

WCR ISSN 1559-3185