

## Tech Talk: E-Mail Compliance: Separating rumor from Reality

by Jo Day and Kevin Day

There is a lot of conjecture and misinformation surrounding e-mail retention specific to the Securities and Exchange Commission's record-keeping rules. Advisors receive disparate advice from compliance consultants software providers, and colleagues who have been audited. Despite claims to the contrary, there are not regulations *specific* to e-mail (the SEC anticipates issuing interpretive guidelines—*not* new rules—regarding e-mail in 2005). While technology solutions may help a firm meet compliance requirements, they are not mandated. If your firm is considering a technology solution to help handle e-mail for compliance purposes, your purchasing decision should be based on whether the time saved is cost effective, not because any of the technological features are required by the SEC (they are *not*).

To get a direct answer regarding recordkeeping requirements, we spoke with Gene Gohlke, associate director of the SEC's Office of Compliance, Inspections, and Examinations. While Gohlke's views do not necessarily represent the views of the SEC, he provided some helpful insight. Because advisors should expect the SEC to "request e-mails of one type or another" during upcoming audits, the following should help confirm whether your process is satisfactory or needs updating.

### What to Keep

E-mails are subject to the same record-keeping rules as other records under Rule 204-2 of the Investment Advisers Act of 1940. Records to be kept (for five years from the time they were produced) include specific information about your business, clients, and services.

The same record-keeping standards apply to e-mail as to paper correspondence. If you throw away advertisements received in the mail, correspondingly you would delete e-mail spam. If you receive an e-mail from a colleague about lunch, you also do not need to retain it.

### Responding to an SEC 'Request for Information'

In addition to specific information required to be retained, Section 204 of the Advisers Act says that any information that is in the possession of an investment adviser at the time a request from the SEC is received needs to be provided to the SEC.

"That statement is very broad," states Gohlke. "There are no limitations...it goes to any piece of information the advisor has in his or her possession and includes any e-mails in the advisor's server or personal e-mail accounts that relate to the advisory business. A much broader set of information is reached under this section but the advisor doesn't have to keep that set of broad information [that is not covered by that rule]."

In summary, you are not required to retain all e-mails (only information covered by the Advisers Act); however, anything you do retain is subject to review.

### Safeguarding Against Destruction

Many, including Oren Chaplin, a compliance attorney with Stark and Stark, advise saving e-mail to WORM (Write Once, Read Many) media, though this is not a requirement of the SEC. The actual requirement, says Chaplin, is to "(1) maintain and preserve the records so as to reasonably safeguard them from loss, alteration, or destruction; (2) limit access to authorized company personnel and the staff of the SEC and other regulatory bodies; and (3) reasonably ensure that any reproduction of a non-electronic original document on electronic media is completely free and legible."

According to Gohlke, advisors are not required to have a "fail-safe process," but rather, a "reasonable" process to

safeguard data against loss, alteration, or destruction. The definition of what is "reasonable" may depend on the size and profile of the firm.

In developing a "reasonable" process to ensure that appropriate e-mail messages are being retained, if a firm has just a couple of employees, low turnover, and everyone "knows what they are doing," states Gohlke, then training employees about what types of e-mail are required to be retained "and periodic reinforcement of those procedures could be enough," providing the firm makes "a reasonable attempt and supervises [the policy] so it is adhered to."

Additionally, according to Chaplin, e-mail "must have a separately stored back-up from the original in order to be in compliance...." Firms should also periodically test their backup system to ensure it functions as expected.

In a larger firm of 20 employees with higher turnover and without the same close relationships as a smaller firm, Gohlke states that relying on employee training to reliably retain compliance-related e-mail may not be adequate. While not a requirement, Gohlke suggests having a means of recovering deleted e-mail may be a useful tool. States Chaplin, "The majority of e-mails are recoverable through a number of sources—for example, the firm's Internet service provider...."

Regardless of which methodology is employed to ensure relevant e-mail is retained, if an e-mail message that should have been retained is discovered to be deleted, under recently enacted rules, the firm must document any compliance violation.

Here are some key suggestions:

- **Gene Gohlke (SEC):** Provide employee training on record retention rules along with documentation that includes examples of what should be retained. Provide (and document) periodic refresher training or reminders to combat forgetfulness.
- **Oren Chaplin (Stark and Stark):** Have employees sign acknowledgment of receipt and understanding of the firm's stated compliance policy.
- **Keith Marks (a compliance attorney with National Regulatory Services):** Prepare for auditors to test employees' knowledge of your policy (for example, what type of e-mail does the firm require you to retain, and how do you follow the policy?).

## Are You Required to Review E-mail?

According to Gohlke, there is "no requirement that e-mail should be reviewed as such. The wording of Compliance rule 206-47 states you must have reasonable and appropriate policies to prevent violations and find those that occur." To prevent and detect any violations, many advisors routinely review e-mail.

While Chaplin states that reviews "can be done electronically,...the firm should have evidence that a review was undertaken."

A common practice among some advisory firms is to train their employees to tag or cc "compliance-related" e-mail to be reviewed by a fiduciary or chief compliance officer.

Keith Marks is skeptical of any policy whereby the chief operating officer exclusively audits e-mails that employees submit for review, as it would be too easy for an employee to circumvent this process. In addition to reviewing submitted e-mails, says Marks, you should review another random sampling of all other e-mails with "no one excepted from that sampling." Gohlke concurs by stating that if your sample is based on a specific set of criteria such as topic or key words to which your employees may become attuned, "you should supplement the

approach with another random sampling of all the rest."

Gohlke emphasizes that any review process must not be a "fictional exercise." In other words, if during an audit the SEC uncovered a problem e-mail that showed evidence of review and it was not discussed with the writer, "that would be a problem. If you say you are doing it [review], do it competently."

There is no requirement by the SEC to be able to perform keyword searches on e-mail. If the SEC requests to see all e-mail for a particular employee on a given topic and your system does not have the ability to filter or search, then you would need to produce all e-mails. E-mails may be provided electronically or in paper, so long as they are furnished promptly (roughly interpreted to be within 24 hours, according to Gohlke).

## What Does Technology Have to Do with Any of This?

As Gohlke states, there is "not a one-size-fits-all" approach to e-mail compliance; rather, what is "reasonable" is based on the "resources, facts, and circumstances of the firm."

Considering the size of your firm, your budget, and available time for maintaining e-mail compliance, consider whether any of the following resources may be cost effective.

### Small Practice (One to Five Employees)

Many small practices use Outlook in such a way that each employee's mailbox is stored on their local workstation. There are several drawbacks to this. First, there is no central repository of all of the firm's e-mail. Considering the requirement to provide information to an auditor promptly, how long would it take you to extract e-mail from each employee's workstation? Also, if e-mail is being stored separately on each workstation, chances are employees' e-mail is not consistently backed up. If so, it would be difficult to claim you have a reasonable process to ensure that e-mail records are complete.

One way for Outlook users to consolidate scattered e-mail is to install Microsoft's Exchange Server, which acts as a central repository for all e-mail messages. There is generally an ongoing cost associated with this option, as exchange servers require expertise to configure and maintain.

Another option is to buy contact relationship management software to enable employees to link e-mail to a specific client's record. In Junxure-I ([www.gowithcrm.com](http://www.gowithcrm.com)) for example, Greg Friedman, a planner in Novato, California, imports each employee's PST file (the file that stores an employee's e-mail messages) daily. Junxure-I parses the data and matches e-mails from all known e-mail addresses to existing client records in Junxure-I. For e-mails that don't match a record, Friedman either matches the e-mail manually or adds a new record in Junxure-I so that future matches will occur the next time he runs the process. As with other CRM software, the e-mail reports in Junxure-I enable queries of e-mail (such as by client or date range) to aid in review.

Another option for small firms is a service offered by Advisorsites ([www.advisorsites.com](http://www.advisorsites.com)) called "E-mail Archive System" (EAS). This Web-based service provides "live" access to e-mails for the past three months. E-mail may be downloaded, searched, or sorted at any time. Each month the old archives are copied onto tape at Advisorsites for six-year storage. Two CDs containing the prior quarter's e-mails are mailed quarterly to the advisory firm.

Andy Gluck, CEO of Advisorsites, feels that most advisors who back up "think that they are covered, but many of them will find they have a problem doing a restore—something pops up that they don't expect."

### Medium-Sized Firms

Larger firms often employ some type of contact management software, and most CRM systems have built-in functionality to create processes and procedures for e-mail reporting and reviewing.

To oversee the e-mail activity of her 16 employees, Kathie Day of Miami, Florida, prints out an e-mail report from her contact management software. Upon reviewing a random sample electronically, she initials the report to indicate the e-mail she's reviewed, then scans and saves the report to a compliance area on her server that has restricted access.

## Large Firms

When InlignWealth Management in Phoenix, Arizona, grew from 16 to 40 employees, their COO, Beth Pragliola, was tasked with finding a service to help monitor the employees' e-mail for compliance purposes.

After nearly a year of research, Pragliola settled on Seccas ([www.seccas.com](http://www.seccas.com)). As with many other providers Pragliola researched, Seccas is Web-based and includes the ability to filter spam; to capture internal, Internet e-mail, and instant messages, and to text-search e-mail and attachments. Seccas captures e-mail in non-alterable format, provides an audit trail of the compliance officer's review, and provides reports to show monitoring has occurred.

Additional features that attracted Pragliola to Seccas included a keyword dictionary (containing such words as "guarantee") that Pragliola can further customize. This enables her to filter and review questionable e-mails that receive a score of 90 or above, for example. For each e-mail address, Seccas shows statistics on how many e-mails were received versus reviewed.

## It's All About Your Process

As you can see, there are many means of meeting compliance requirements for handling e-mails. The method you select has more to do with your firm's size, characteristics, and pocketbook than it does with a given technology. Regulatory agencies are interested in your process—not the specific tool (if any) to implement the process. This underscores our technology mantra: "Start with your process, then determine which tools help you work the way you want to."

The next time you hear about a regulatory agency requiring a specific technology, ask to see the regulation in writing—you'll be amazed at how many "requirements" disappear when you actually read the regulations. E-mail compliance is something you need to take seriously, but for many, it may be achieved with a combination of processes, procedures, and software that you're already using.

A brief description of software applications to help meet the small, medium, and larger firms with respect to e-mail compliance (along with pricing) can be found at [http://www.trumpetinc.com/nws\\_articles.jsp](http://www.trumpetinc.com/nws_articles.jsp).

*Jo Day and Kevin Day are principals of Trumpet Inc. in Phoenix, Arizona. They provide technology consulting and services to financial planning firms via the Internet. They can be contacted at [info@trumpetinc.com](mailto:info@trumpetinc.com) or <http://www.trumpetinc.com>.*