E-mail Retention Policies for Investment Advisers

For some time now, the SEC's Office of Compliance Inspections and Examinations (OCIE) has included on their examination request lists e-mails and other electronic correspondence retained by investment advisers . In July 2003, the SEC brought its first e-mail-related enforcement case against an investment adviser. Advisers should undertake a comprehensive evaluation of their e-mail retention policies and procedures to ensure adequacy and preparedness in the event of a regulatory examination. Further, advisers should evaluate these policies and procedures periodically as new technologies become available and vulnerabilities are identified in an effort to maintain a healthy retention program.

Please be mindful that record keeping requirements differ for investment advisers and broker/dealers. Dually-registered firms are subject to both the Advisers Act and FINRA record keeping requirements. We note some of these distinctions in this document.

Below are some topic areas for your consideration:

What Must You Keep?

Under Rule 204-2 of the Investment Advisers Act of 1940, advisers must keep various categories of books and records. If an e-mail falls under one of those categories, it must be kept, just as it would have if it had been a paper record.

B/D: (a) Securities Exchange Act Rule 17a-4(b)(4) requires broker/dealers to keep "originals of all communications received and copies of all communications sent by such member, broker, or dealer (including inter-office memoranda and communications) relating to his **business as such**." (b) NASD Conduct Rule 3110(a) and NYSE Rule 440 require member firms to create and maintain books, accounts, memoranda, and correspondence as required by SEC Rule 17a-3 and in a format as required by SEC Rule 17a-4.

FINRA is establishing a consolidated FINRA rulebook that will consist solely of FINRA Rules. Until the completion of the rulebook consolidation process, the FINRA rulebook includes NASD Rules and Incorporated NYSE Rules.

What Might the SEC Request?

Past statements by the OCIE staff suggest that the OCIE has taken the position that it is entitled to review all e-mails retained by the adviser, regardless of whether they are covered under the Rule 204-2. This includes personal e-mails. The OCIE has indicated that they will review personal e-mails to determine if they are truly personal. If an adviser does not retain all e-mail, then it should implement a policy to ensure that all required e-mails are being retained and not deleted. The OCIE believes that e-mails are a source for understanding the culture of compliance of a firm.

At various industry conferences and on conference calls, Gene Gohlke, former associate director of OCIE, has stated that examiners at the beginning of an examination might ask for two months of e-mails from senior people, such as the firm's CEO, CFO, CCO, President, portfolio managers, and traders, among others.

An SEC examination request list presented to an adviser requested: "For individuals to be selected upon commencement of the examination, or shortly thereafter, please be prepared to provide all e-mails, including their corresponding attachments, sent and received during a period to be specified. This information should be provided in an electronically searchable format. In identifying e-mails that are responsive to our needs, please be mindful that e-mails may be stored both on servers and on individual hard drives of the persons selected."

How Long Must E-mail Be Kept?

Electronic communication must be kept for the same length of time as if the record was a written/printed record. Generally, records should be kept in an easily accessible place for a period of not less than five full fiscal years after the last entry was made in that record, the first two years in an appropriate office of the investment adviser. Be mindful that if the e-mail pertains to documentation demonstrating the calculation of performance, for example, it may be subject to retention for five full fiscal years after the adviser stops advertising the performance.

B/D: Broker/Dealer record keeping requirements for e-mails are generally three years.

How Must E-mail be Stored?

Investment Advisers may keep records on various electronic storage media, subject to certain conditions.

Advisers must:

1. Arrange and index the records in a way that permits easy location, access, and retrieval of any particular record;
2. Provide promptly any of the following:
    a. A legible, true, and complete copy of the record in the medium and format in which it is stored;
    b. A legible, true and complete printout of the record; and
    c. Means to access, view, and print the records; and
3. Separately store, for the time required for preservation of the original record, a duplicate copy of the record;
4. Maintain and preserve the records, so as to reasonably safeguard them from loss, alteration, or destruction;
5. Limit access to the records to properly authorized personnel; and
6. Reasonably ensure that any reproduction of a non-electronic original record on electronic storage media is complete, true, and legible when retrieved.

B/D: Exchange Act Rule 17a-4(f) specifically requires that broker/dealer electronic records be preserved "exclusively in a non-rewriteable, non-erasable format", often referred to as WORM (write once, ready many). This same requirement does not currently exist for advisers but may serve well as a best practice.

Written Policies & Procedures

In light of the OCIE jurisdiction over an adviser's books and records and of Rule 206(4)-7, which requires advisers to adopt written polices and procedures designed to ensure compliance with the Advisers Act, firms that have not already done so should adopt and periodically review formal written e-mail retention policies.

Policies and procedures should be appropriate for the size and structure of the adviser's business while remaining practical enough for the firm to consistently follow the policy. A manual review process may be appropriate for small firms, while a software-based solution may be necessary for larger firms. All relevant departments should be involved in the creation of the adviser's policy (management, IT, legal, compliance, marketing, trading, portfolio management, operations, etc.)

The following outline may serve as a guide to developing an e-mail retention policy:

A. Your policy should spell out permissible and non-permissible message ***content*** and ***medium***.

1. Content:
    a. People have a tendency to treat email as an informal form of communication and say things they might not otherwise say in person or in a letter. This can have the unintended effect of a third-person, such as a regulator, taking an email message out of context, potentially creating a problem where there was none. Consider including formal ***email etiquette*** guidelines and a caution to employees about communicating in abbreviated formats in your policy.
    b. Caution your employees on ***forwarding*** messages. They should be mindful of the email content, including the chain of forwarded/replied emails and attachments, so as to avoid violating the firm's privacy policy or attorney-client privilege and disclosing trade secrets.
    c. Get consent from clients to send ***personal nonpublic information*** electronically if not responding to an electronic message.
    d. When sending ***advertising*** or sales literature via e-mail, remind employees that they must follow the same company procedures if they were sending a paper mailing.
    e. If appropriate, prohibit or restrict the sending and receiving of ***personal e-mails*** using company resources.

2. Medium:
    a. Your policy should require employees to refrain from using any electronic communication system not maintained by your firm. Spell out which systems they may and may not use.
    b. Consider all ***types of electronic communication*** your company uses:
        i. What types of e-mail and to whom do your employees send e-mail?
        ii. Do your employees have the ability to send and receive personal e-mails?
        iii. Do your employees have the ability to use ***home computers*** or ***web based e-mail*** accounts to send business related e-mails?
        iv. Do your employees send e-mail via ***laptop*** computers?
        v. Do your employees use Blackberries or other ***PDA***?
        vi. Do your employees use ***instant messaging*** (IM)?
        vii. Do your traders use Bloomberg's instant messaging or e-mail features?
        viii. Do your employees use ***text messaging***?
        ix. Do your employees communicate using ***social media*** sites?
        x. What are the various systems and system constraints?
    c. Identify for all types of electronic communication, how are those communications captured and stored?

B. Require all e-mail sent to include an appropriate ***disclosure*** for the adviser. One sample is provided here:
    1. PLEASE READ THIS IMPORTANT MESSAGE: [Adviser] only transacts business in states where it is properly registered or notice filed, or excluded or exempted from registration requirements. [Adviser] has taken precautions to screen this message for viruses, but we cannot guarantee that it is virus free. [Adviser] accepts no liability for any errors or omissions arising as a result of this transmission, or for any delay in its receipt or damage to your system. All e-mail sent to or from this address is subject to archival, monitoring and/or review by [Adviser's] compliance department and therefore subject to disclosure to someone other than the recipient. This message (including any attachments) is intended only for the addressee(s) named above and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If you are not the intended recipient, you must not read, copy, use, or disclose this communication. Please notify the sender by replying to this message, and then delete this message and any attached materials from your system. Thank you.

C. Identify the person ***responsible for supervision*** of the policy.

D. Determine your ***e-mail retention policy*** and disclose it to your employees: There are two basic approaches to an e-mail retention policy:
    1. Create a policy requiring the ***retention of <u>all</u> e-mail***; or
        a. Inform your employees that all e-mail communications are being archived and may be subject to review.
        b. The expectation by the OCIE that you prove your firm hasn't deleted anything it shouldn't is causing many advisers to keep <u>everything</u>, including spam and personal messages.
            i. This approach requires large data storage capacity. Use effective filters to prevent the receipt of spam. Keep <u>everything</u>, including spam, but segregate spam to a separate folder.
    2. Create a policy requiring only the ***retention of e-mail that falls under Rule 204-2***, but be able to demonstrate that you have in fact kept all required records and what your e-mail destruction policies are.
        a. Inform your employees of the requirements of what e-mails must be retained and
            i. Provide them with specific guidelines on how to identify required records.
            ii. Provide them with specific guidelines on the firm's policy on destruction of e-mail records
        b. Determine who is authorized to purge e-mails.
        c. Develop a policy to ensure that the guidelines are followed
            i. Conduct periodic reviews of deleted e-mails prior to final destruction.
        d. Record-keeping suggestions:
            i. Print required records and file in client or relevant firm file. (Probably only practical for small firms). The disadvantage to this approach is that the SEC cannot use key word searches on the e-mails; therefore, they must read more and may stay longer to review your records.
            ii. Have employees copy or forward a particular e-mail address for required records.
            iii. Have employees store required e-mails in a particular folder.

e. Destroy non-required e-mails with caution, pursuant to written retention policies, and on a regular basis. Your e-mail destruction policy should be ***systematic***, so when a regulator asks why an e-mail was destroyed, you can respond that it was in accordance with your firm's e-mail destruction policy. Do not destroy all e-mails as a matter of policy. Caution: during the course of an investigation, adviser should not destroy any emails, even if not required to keep them.

E. Consider ***separation*** of e-mail by broker/dealer and investment adviser.

F. Provide ***training*** to your employees.
   1. Provide employees with an e-mail ***etiquette*** policy.
      a. E-mail is a written communication and employees should observe minimal levels of formality and thoughtfulness. The tendency to treat e-mail as an informal communication causes many people to say things in an e-mail that they would never say in person or in a letter.
      b. The ease with which e-mail can be sent or forwarded can often lead to messages ending up in the wrong hands or unintended recipients. Embarrassment aside, sending e-mail to the wrong person, can result in the loss of attorney-client privilege and trade secrets or the violation of client privacy.
   2. Inform employees to treat all e-mail as if ***a regulator will read it***.
      a. The OCIE taking e-mails out of context can cause you enormous amounts of time and money explaining something that should never have been an issue in the first place.
   3. Instruct employees to make appropriate claims of ***attorney-client privilege*** on all correspondence with internal or external attorneys.
      a. Identify what is privileged.
   4. Remind employees that they have ***no expectation of privacy*** in their e-mail communications, that these records are archived, and that they may be reviewed by internal personnel or regulators.
   5. Require a ***written acknowledgement*** from employees of your policy.
      a. Get in writing that employee acknowledges the e-mail policy and will abide by it. Include the policy in your compliance manual, employee handbook, hiring paperwork, or all three.
   6. Train employees on your specific e-mail retention and destruction policies.
   7. Send out periodic reminders and/or hold periodic internal training sessions.

G. Implement ***procedural safeguards*** where practical or feasible.
   1. Don't permit employees to install their own software.
   2. Limit browsing capabilities.
   3. Automatically copy all e-mails to a separate directory.
   4. Implement key-word screening.

H. Conduct ***periodic reviews*** to ensure compliance with firm's policies and procedures and to detect any unlawful activity
   1. Conduct ***spot-checks***.
   2. Use ***key-word searches***. Create a lexicon of search terms that is appropriate for your business, but won't generate too many false positives. Some key words regulators are

using: timing, market timing, frequent trading, excessive trading, churn, soft dollars, guarantee, deal, authorize, agreement, agree, fraud, complaint, superior, performance, best, returns, and outperform.

I. ***Test*** your backups for retrieval.
   1. Make sure your backups are functioning and that you can produce e-mails in a timely manner and according to the record keeping requirements.
   2. The time to test producing e-mails is now, not during an examination.

J. Conduct an ***annual review*** of entire policy.

Note: NASD Notice to Members 03-33 (June 2003) stated that it considers IM to be akin to e-mail and therefore IM is subject to the same record keeping and storage requirements. SEC staff has similarly interpreted record keeping rules for investment adviser.

What to Do during an Examination?

Make sure you understand the nature of the regulator's request:
1. For which employees are they seeking e-mails?
2. For what time period do they want to see the e-mails?
3. For what key words or clients do they want those e-mails or do they want all e-mail?
4. What format do they want you to provide the e-mail in?
5. Provide only what is requested and nothing more.

Produce e-mail "promptly". Generally, the SEC considers promptly to mean within 24 hours. If you are unable to produce all the requested e-mail within 24 hours, inform the regulators up front and provide what you can and then continue to provide e-mail on a rolling production schedule. If your attorney or compliance department is reviewing records prior to production, it must be done quickly.

Disclose up front if you discover records missing, deleted, or you didn't retain then in the first place. DON'T TRY TO HIDE IT. DON'T LIE. PRODUCE WHAT YOU CAN. Use all means of restoring deleted e-mail and backups. Do not say that you didn't know you were required to keep e-mail. This is not a new rule. You should have been keeping e-mail in accordance with the books and records rules all along.

Provide a privilege log of all privileged documents. Not every email sent to, received from, or cc'd to an attorney is privileged. The e-mail must generally contain legal advice or a specific request for legal advice. E-mail copied to third parties will result in waiver of the attorney-client privilege.

Third-Party Vendors – Things to Consider

Finally, e-mail retention can be burdensome. A third-party vendor may provide relief. Keep in mind that you must adopt policies and procedures with your unique business in mind. Below is a list of some third-party vendors providing e-mail retention to advisers and broker/dealers. This is not a comprehensive list and should not be considered an endorsement. You may find another vendor better suited to your particular needs.

www.lightport.com
www.advisormail.com
www.smarsh.com
www.ironmountain.com
www.emc.com
www.zantaz.com
www.ziplip.com

When looking at a third-party vendor, consider some of the following questions:

1. How is the data archived and restored?
2. What format is used for archiving data?
3. What is the time frame for producing requested data? Can they produce it "promptly"?
4. What safeguards to they have to protect the data from alteration, loss, untimely destruction?
5. What safeguards do they have to protect confidentiality?
6. Do they have a written business continuity plan?

To discuss further, please contact:

Advisor Solutions Group, Inc.
949.250.1855
info@advisorsolutionsgroup.com

