You've Got Mail… Now What?

September 29, 2015

The inappropriate use of email can spell disaster for registered investment advisors (RIAs), particularly for firms with multiple offices or remote workers, and for those with employees who use personal devices to transact business.

There are measures that RIAs can take to protect themselves in the event of issues involving indiscriminate email usage or regulatory audits. An email policy is a start, but advisors are best served – and in compliance – when they actively monitor emails and enforce policy.
Email Policy Basics

Those responsible for human resources or in charge of firm management often take the lead in drafting a RIA's email usage and retention policies, but the strongest policies typically include input from outside experts such as outside legal counsel or information technology (IT) service partners.
At minimum, a good email policy will state that the contents of every email will not breach firm or client confidentiality. The policy should also explicitly explain that any technology-related tools, devices and services owned by the firm are to be used solely for the purpose of transacting business and are not for personal use.

The firm's email retention policy may also be spelled out. In the event of an audit, RIAs must be able to show that their email policy complies with Rule 204-2 of the Investment Advisers Act, the Books and Records Rule, which requires emails to be retained for five years after the fiscal year they were sent.
All RIA partners and employees should sign and date a written policy when it is presented, with the original being kept by the firm and a copy given to the signatory.

Auditing Emails

Of course, no matter how well written, a firm's email policy must be enforced to be effective and must stand up to regulatory audits. To comply with SEC regulations, RIAs must be able to prove they are systematically checking emails. Random, periodic assessments of emails will not suffice as the firm's email audit protocol.

RIAs and their IT professionals should be working with programs or providers to monitor outbound and inbound emails actively, employing a rules-based approach to look for number and word patterns. The auditing process should flag potentially suspicious or undesirable content, including spotting language such as "I guarantee…," or "I promise…", and also flag emails containing confidential information. Firms must also be vigilant about blocking inbound email spam, as well as outbound emails to undesirable sites.

Email Encryption

RIAs are on the hook for ensuring that emails are delivered and received correctly, which firms can do through encrypted connections and emails. Encrypting outbound email provides the firm with a receipt to prove that this was done correctly and securely, through an encrypted connection. The encrypted connection also offers the firm protection for inbound emails. RIAs should not limit email encryption to the office; access to the firm email platform should only occur through password-protected and encrypted mobile devices as well.

Mobile Devices and Email

RIAs need to carefully consider how or whether employees access email via personal mobile devices. The chief concern is the ability to encrypt, audit and archive inbound and outbound firm emails, and text messages, from any access point.

There are two best practices for maintaining control over mobile email usage. The first is to limit access to firm email to personal mobile devices that are encrypted and password protected. The usage policy should be explicit: “We will not allow firm email on personal mobile devices unless the devices are equipped with our encryption and password protection programs.” If the employee leaves the firm or loses the device, the firm has the right to wipe the device. Unfortunately, very few RIAs choose this best-in-class practice. Many advisors wrongly believe that this type of policy gives the firm the right to unrestricted access and control of all data on an employee’s personal mobile device. But this is simply not the case – the RIA does not get access to the data on the device. Rather, the entire hard drive is encrypted and the device is password protected to be in compliance with regulatory requirements, and to safeguard the RIA from any potential liability resulting from email usage that falls outside of firm policy.

The second best practice is to use firm-issued mobile devices that are password-protected and encrypted for email. This alternative addresses concerns about privacy, data access and ownership. But resistance to carrying two devices can be very strong. It is more often the case that a RIA may offer firm-issued mobile devices; it is rare to find firms that insist on them.

Archiving Emails

All state- and SEC-registered RIAs should be archiving email, but many are surprised to learn that not all archiving tools pass regulatory muster. In fact, any tool that allows emails to be modified or removed is not a true archive and will not stand up in an audit. This means that the default archive tools in Outlook, Mail and most customer relationship management (CRM) systems are not SEC-compliant archives.

Once armed with tools or providers that will archive email in a SEC-compliant manner, advisors should consider using their archive as a tool to be used their own business purposes.

The email archive can be mined and sorted for data, which can compliment the functionality and features of the CRM.

It’s Time to Activate Your Email Policy

RIAs need to safeguard themselves against potential business and reputational damage when events unfold in ways that are outside of their control. Through proper monitoring and enforcement, well-thought-out email usage policies can only help advisors in the event of a crisis or regulatory audit.