

## Small, Yes, but Still Compliant

### How smaller RIA firms can shoulder the compliance burden

BY CHESTER WRIGHT

**PUBLICLY EMBARRASSED BY** a series of undetected frauds by investment firms, the Securities and Exchange Commission has sharpened its investigative and regulatory inspections. RIA firms too small in terms of assets under management to warrant SEC attention are subject to state regulators who follow the SEC's lead, so essentially the same rules apply.

In addition to considering a plethora of new regulations, the SEC is refocusing its attention on some requirements about which they have formerly been relatively forgiving. Specifically, all investment companies and registered investment advisors must have written policies designed to protect investors, and they must have a designated Chief Compliance Officer. The CCO position must be "empowered with full responsibility and authority to develop and enforce...[and a] position of sufficient seniority & authority to compel."

These requirements place a substantial burden on small financial advisors and until now have been substantially neglected by many small firms. But with the SEC and state officials focusing attention on small firms—in the wake of the financial crisis and the Madoff fraud—that formerly sailed below the regulators' radar, these firms must now take the requirement to have a Chief Compliance Officer and a comprehensive compliance manual seriously. Here is how a small firm can mount an effective compliance program without breaking the bank.

#### MAYBE NOT YOUR SPOUSE

In the past, the response to the specifics of regulation by a significant number of firms has been to simply ignore the regulation completely or by a clumsy attempt to circumvent its intention. One of the most

frequent examples was naming a CCO who had neither the skill nor the authority to effectively exercise the responsibilities of an actual CCO, and oftentimes by having no written policies at all.

A review of filed Form ADVs reveals that in case after case, in small firms the CCO has the same last name as the owner. Naming a spouse as CCO does not mean that this person has the training, the skill, or—most important—the authority to carry out the legal requirements of the job. The practice of calling one's administrative assistant the CCO of the firm has even less possibility of surviving an SEC or state audit.

These clumsy attempts to evade requirements are dangerous and unnecessary. It is possible for the small shop to have a legitimate and effective compliance operation without additional staff or consuming large amounts of time necessary for managing client accounts.

To stay compliant, every RIA firm regardless of size needs:

- A real CCO
- Two written documents
- A process for assuring that the procedures in those documents are carried out
- Scheduled written compliance reviews to document that they have actually followed their own procedures.

We will address each of these requirements in turn.

#### Requirement Number 1: A Real Chief Compliance Officer

The CCO position requires a commitment of time, and the position must have the authority to enforce regulations. Small shop owners should know that they can be their own compliance officer. In fact, if the firm consists of an owner and an admin, the owner is the CCO, like it or not. While looking over your own shoul-

der may be difficult, it can be done. We'll discuss how to do that in a moment.

Those with the luxury of a small staff should choose a senior member for the CCO job. But no matter how experienced, he or she will need a certain amount of time to become and stay familiar with regulations. Then your CCO will need time to establish procedures specific to your firm and time to review those procedures periodically. The time demands will decrease with experience, but they never disappear.

The new CCO is not alone. The SEC actually devotes considerable time and attention to helping new CCOs. It maintains a portion of its Web site ([sec.gov/info/iaicccoutreach.htm](http://sec.gov/info/iaicccoutreach.htm)) where it publishes guidelines and provides a list of phone numbers for questions. When you call the SEC, you will likely get the Commission's voice mail, but its attorneys typically return phoned-in questions within one day. In addition, the SEC conducts training sessions tailored for new CCOs. Despite views to the contrary, the SEC really would prefer that RIAs do compliance right in the first place; there are enough real crooks out there to keep regulators busy.

#### Requirement Number 2: Two Written Documents

All firms must have an organization-specific Policies and Procedures Manual (PPM) and a Code of Ethics. If you can locate an attorney who specializes in SEC regulations, you can pay to have a PPM prepared; or you can buy one already written. First-rate material can be found on the Web for around \$500, a fraction of what an attorney-written model will cost. The pre-written material will require modifications to fit your particular business procedures,

but reviewing the “canned” documents and making appropriate revisions will be invaluable training for your CCO.

#### **Requirement Number 3:**

##### **Compliance Review Process**

One step that the CCO will need to take is detailing the specific procedures that will let you know that your policies are actually being followed. You will need a compliance review process added to your off-the-shelf manual. Policies must be managed and enforced through an ongoing series of reviews that are conducted and recorded on an established schedule supervised by the Chief Compliance Officer.

#### **Requirement Number 4: Scheduled Compliance Reviews**

Routine compliance reviews and reports should be scheduled consistently both quarterly and annually. A review may also be conducted at any time circumstances indicate. The outcome of the review is a report that lists each area reviewed, followed by:

1. Exactly what was examined and how
2. What was discovered
3. Actions recommended

The review should then be submitted to the firm’s senior official and discussed with him or her to determine what actions will be taken. After this discussion, the CCO should amend the review to include what actions were actually taken.

If the CCO’s recommendations were not followed, it is necessary to add an explanation of why that was the case and list what other steps, if any, were taken instead. Under no circumstances should anyone revise or remove the original recommendations.

While your CCO will be responsible for carrying out all of the 30 or so items in your new manual, there are three areas that will be of particular interest to SEC and/or state auditors and should receive immediate attention. They are:

1. Creation, retention, and protection of critical records;
2. Protection of client information;
3. Managing each client’s account

in a manner consistent with their best interests.

#### **ENSURING ACTION IN THE CLIENT’S BEST INTERESTS**

Aside from actual criminal activities, this last element seems to appear most frequently in SEC adverse actions. Legislation currently on its way through Congress is aimed at further strengthening the “client needs” investment requirements imposed on advisors.

Let’s examine each in turn.

- **Records.** SEC Rule 204-2 specifies in precise detail the records that must be created and retained. Actual retention of paper records is no longer required, but the ability to produce paper copies on demand and/or within a short timeframe is essential.

- **Protection of client data.** Identity theft is a growing problem in the population at large. When one considers the amount of personal and financial data an RIA must maintain about clients, it is easy to understand just how important it is to establish and constantly review protective measures. There are two areas of specific concern: inappropriate employee curiosity and criminal access. The first is easily dealt with by limiting access to “need to know” and using password protection. The second is a serious and ever-present danger. Small firms can set up their own secure data management and storage system, but it will require the ongoing services of a specialist and will be expensive. A practical and often less expensive solution is to use a third-party service provider who provides all of the necessary hardware, software, and support services. Not only do such solutions cost much less because of the lack of capital costs for the equipment, but the RIA has effectively hired a full time technology expert to provide continued maintenance and best practices along with ongoing security upgrades. Even with all that, absolute security is not guaranteed, and random reviews

of client accounts will still be required to detect unauthorized activity. For CCOs, paranoia is not a mental disorder; it is a professional requirement.

- **Appropriate Account Management.**

Not only must accounts be managed in a way that reflects clients’ age, financial condition, and account objectives, but you should also have proof that the account management reflects these requirements. The fact that you know that you are conscientious is no longer enough for the SEC; they now demand evidence. If you do not presently conduct an annual review of each client’s financial condition and objectives, by all means do so. Keep written evidence of that activity. Make notes on phone conversations and if any changes occur, confirm in writing with the client, whether by e-mail or snail mail. Then the CCO should periodically review client portfolios to ensure they reflect the clients’ needs. The critical point is to not only carry out the procedures noted above, but to record them in a consistent manner. It must become an inviolate habit because the SEC requires evidence of performance and without it you may be subject to disciplinary actions.

#### **A LITTLE WORK EQUALS A LOT OF SAFETY**

If this seems like extra work and expense, bear in mind that most of the effort involved is in setting up your systems. Once these systems are in place, you should notice very little difference from your daily routine.

Finally, ask this question: “Would a knowledgeable individual, with no other evidence other than the records I can readily produce, be convinced that 1) I am doing what I should, and 2) that I am not doing what I shouldn’t?” The only possible answer must be yes! **IA**

---

**Chester Wright** is the chief compliance officer at Harmony Asset Management LLC, or HarmonyAM, an RIA firm based in Scottsdale, Arizona. He can be reached at [cwright@HarmonyAM.com](mailto:cwright@HarmonyAM.com).