

UNCOMMON VISION: What Happens Here Stays Here

Once upon a time in the financial services industry, many eyes saw little. Today, thanks to technology, many eyes see more than they actually need to. This exposure of information presents a challenge to management: maintaining confidentiality while building awareness of the *meaning* of confidentiality and its effect on our daily behavior in and out of the workplace.

Establishing Confidentiality

“What happens here, stays here” is a phrase new employees may hear at their orientation. After that, training begins in earnest and the subject of confidentiality is probably not raised again. Yet, upon completion of the training phase the new employee comes face to face with a workstation screen filled with a mind-boggling display of information.

The fact is employees in financial services see much more client information than their jobs require. Here's an example: in most firms, an employee adjusting a transaction from one account to another needs only to see the transaction in question and an adjustment template. Instead, the employee has access not only to the entry to be adjusted, but also the client's name, address, account information, security and money positions and other proprietary information. Some of this information is trivial, some of it alluring, but all of it is confidential.

You can help to raise awareness of the need to keep information in-house by making sure the subject of confidentiality is discussed at staff meetings. It's not only important to delineate confidential and non-confidential information, but also to define who information can be shared with, how and where: Is it proper to discuss with other employees, employees of other firms, friends or relatives? Can it be shared in the company cafeteria, on the phone, or on the way home from work? All too often, employees are on their own when it comes to making these distinctions.

This also applies to talking about the firm. You have to take it for granted, employees talk about the firm outside of the office.

Has this happened to you? One evening, after working late, I was traveling homeward on the train. Half a dozen employees from a Broker / Dealer firm entered the train and, due to the lateness of the hour, were able to spread out on the seats. They talked freely about a system the firm was trying to install, the problems they were having, their opinion of the system and the names of their managers — one of whom I happened to know well.

Another time, while at a business lunch, patrons at a nearby table were loudly joking about an underwriting that their firm had just sold. My colleagues and I were easily able to overhear their banter, which happened to be quite negative. We could only hope that it was wisdom, rather than luck, that prevented the firm's name from being mentioned.

We all know it's not uncommon to overhear confidential information being discussed indiscreetly, so managers have to set standards of behavior that help to control exposure. For example, ask your staff if anyone discusses business on a cell phone on the way to work. It's often obvious to everyone but the person on the phone that everyone can hear them! Another way to emphasize the point is to conduct training sessions that include role-play of real-life scenarios.

Even when safeguards are in place they can begin to crumble when employees are focusing only on their immediate jobs. Here are two examples: Passwords can become legacies from employee to employee or shared with unauthorized staff; and secure workstations are often not

locked or turned off when unattended. Every employee can be made aware that by taking a few simple precautions, confidential information can be better protected.

Building Awareness

A firm can build awareness of potential misuse of confidential information by addressing the topic at staff meetings. This may seem obvious, but all too often, someone who could benefit is left out. Be inclusive when you're addressing confidentiality. For example: the Operations areas are a potential line of defense. Yet, in many cases, they are not prepared to identify questionable activities. Making employees aware of what constitutes sensitive information and providing guidance on what to look for will go a long way toward protecting the firm from financial exposure or just plain embarrassment.

Employees must also have confidence that they will be listened to, as well as protected from retaliation. You may consider invoking the advice we see on the New York City subways: "If you see something, say something." Make sure there are clear reporting lines for questionable activity — two independent reporting lines are even better, especially if anonymity is desired. When the procedures for reporting questionable activities are published in the employee handbook, on your intranet, or in an e-mail, your message is unmistakable. Don't forget to involve your compliance staff or your ethics officer in crafting and communicating the message.

Your Confidentiality Checklist

- ✓ Set the standard
- ✓ Discuss what "confidentiality" means – ultimately protecting the client and the firm's reputation
- ✓ Define appropriate behaviors, on and off the job
- ✓ Reinforce confidentiality with published messages and with training
- ✓ Make sure there is at least one reporting line for questionable activity
- ✓ Involve your compliance staff

Once you've made your checklist, you may also want to consider your own availability to answer questions. A senior manager of a large investment bank once told his staff, "If you see something that doesn't look right, ask. If the answer doesn't sit well with you, ask someone else. If it still doesn't make perfect sense, come and ask me. Together we will find the answer." The firm's culture could be summarized in that statement. This manager wasn't afraid to set the standard and to tell his staff that confidentiality is important enough to discuss with him. The message is loud and clear.

June, 2005

David M. Weiss, Managing Director, Jeremiah Associates