Regulatory Notice 08-18

Unauthorized Proprietary Trading

Sound Practices for Preventing and Detecting Unauthorized Proprietary Trading

April 2008

Notice Type

- Guidance

Suggested Routing

- Compliance
- Legal
- Operations
- Risk Management
- Senior Management
- Trading

Key Topic(s)

- Books & Records
- Internal Controls
- Risk Management
- Supervision
- Proprietary Trading

Referenced Rules & Notices

- NTM 99-92
- NYSE Rule 342
- NYSE Rule 351

Executive Summary

In the wake of several recent cases involving allegations of unauthorized or "rogue" trading resulting in substantial losses by firms both in the United States and abroad, many FINRA firms are undertaking comprehensive reviews of their internal controls and risk management systems designed to prevent such trading activity. FINRA is issuing this *Notice* to highlight sound practices for firms to consider as they undergo that process. We also remind firms that even profitable unauthorized trading can result in regulatory exposure if it involves falsification of the firm's books and records, failures in supervisory control systems, market manipulation or fraud. Therefore, internal control systems should be designed to address regulatory as well as business and reputational risk.

Questions regarding this *Notice* may be directed to:

- Laura Gansler, Associate Vice President, Emerging Regulatory Issues, at (202) 728-8275; or
- Rosemarie Fanelli, Surveillance Director, Risk Oversight and Operational Regulation, at (646) 315-8452;
- Kathryn Mahoney, Director, Emerging Regulatory Issues, at (212) 858-4101.

Background and Discussion

The risks associated with unauthorized proprietary trading by "rogue" traders are not new, and most firms that allow traders to commit the firms' capital already have policies and procedures in place designed to prevent unauthorized trading. In 1999, the SEC, NYSE and NASD issued a Joint

FINRA™
Financial Industry Regulatory Authority

Statement on Broker-Dealer Risk Management Practices that summarized weak and strong risk management practices identified through a survey of mid-sized and large firms.[1] In it, the regulators concluded that senior management must play a significant role in the adoption and maintenance of a comprehensive system of internal controls and risk management systems, and that those controls and systems must be adequately funded, independent of revenue-generating activities, and updated as changes in technology, the firm's business activities or other circumstances warranted.

Since then, many firms have refined and strengthened their internal controls around unauthorized trading. However, recent events highlight the importance of routinely reassessing the adequacy and effectiveness of those systems, particularly in light of the increasingly global nature of the financial services industry, the highly competitive trading environment and the complexity of many of the products being traded. In particular, the immediacy required as a result of pervasive electronic trading and market linkages has increased pressure on some firms to relax internal controls that might arguably affect a trader's competitive advantage in the short run, but protect the firm from undue risk in the long term.

Unauthorized trading under any circumstances, but especially in the case of proprietary trading, can pose significant risk from a business perspective, and it can create serious regulatory risk as well, even when the trading generates profits for the firm. Substantial losses can affect financial viability and several recent incidents appear to raise other regulatory concerns, including falsification of the firm's books and records, lapses in supervisory controls and fraud. Moreover, it is sometimes difficult to tell from early red flags whether suspicious trading activity is generating profits or losses; vigilance against regulatory exposure as opposed to simply focusing on business risk can help protect the firm against both. Therefore, a firm's internal controls around unauthorized proprietary trading should be designed to deter and detect all unauthorized trading by the firm's employees.[2] This deterrence is important even when the firm profits from that trading; firms that "look the other way" or reward profitable unauthorized trading are creating incentives for this prohibited behavior and the potential for future risk of loss.

Sound Practices

To assist firms in the process of reviewing and, where necessary, modifying, their current internal controls against unauthorized trading, we have recently solicited input from a range of firms regarding their internal controls, as well as the preliminary results of internal reviews. We are publishing those practices now with the expectation that doing so will help other firms as they undergo their own review process. While FINRA believes that these practices are worthy of consideration, we understand that their relevance and feasibility will vary depending on a firm's size and business model. We also note that this is not an exhaustive list, and is not intended to create a safe harbor from regulatory exposure or to discourage firms from completing their own comprehensive internal audits.

Mandatory Vacation Policies

An increasing number of broker-dealers have identified "sensitive" jobs, and adopted mandatory policies requiring employees in those positions, including traders, to be away from the office for a minimum amount of time, typically ten consecutive trading days. During that time away, the employee is barred from having physical or electronic access to the firm, its facilities, or systems. The theory behind this policy, which has been common in the banking industry, is that if an employee has engaged in unauthorized activity and is concealing it, the activity will likely be exposed in the firm's trade reconciliation process within that time, because the employee is not able to continue the concealment while away from the firm and its systems.

A mandatory vacation policy must be enforced in order to be effective. In at least one recent well-publicized case, the firm had such a policy, but the trader involved had not taken the full, mandatory, consecutive vacation in several years. Exemptions should not be granted except in unusual circumstances and repeated requests for exemptions should be considered a red flag warranting additional monitoring. Firms also should assure that their systems support blocking employees on mandatory vacation from accessing firm systems.

A mandatory vacation policy may not be feasible or reasonable for all firms. However, we urge firms to consider it as part of their risk management procedures. If a firm determines not to adopt such a policy, it should consider other methods of identifying and reviewing the trading activity of traders who have not taken an extended vacation in the past year.

Heightened Scrutiny of Red Flags

As firms review their internal controls, they should pay attention to whether they are both adequately mining available trade data for red flags and following up on those red flags where appropriate. Among other things, firms should monitor, and, when necessary, conduct heightened scrutiny of:

- Trading limit breaches. At least one firm surveyed recently has implemented a tool that allows for monitoring of limit breaches by a trading book or individual trades in real-time, and can be set to generate alerts based on a range of parameters, including the notional value of a trade, share size (net/gross position), amount of orders or traders per day and total dollar value per day.
- Unrealized profit and loss (P&L) on unsettled transactions. Trading desk managers and financial control managers should pay careful attention to sizeable amounts of unrealized P&L and should understand the nature of the transactions creating these amounts.

- Unusual patterns of cancellations and corrections, particularly those involving multiple cancellations or corrections by the same trader or involving the same counter-party. Certain firms prohibit a front-office trader or salesperson from entering cancels and corrects into the trading system and limit the entry of these transactions to mid-office (*e.g.,* those involved in risk management) or back-office (*e.g.,* those involved in settlement services) personnel.
- Transactions in which confirmation and settlement do not occur on a timely basis, or where settlement is outside of normal cycles.
- Reports of aged unresolved reconciling items and aged outstanding confirmations.
- Reports of P&L that exceed a certain *de minimis* amount by traders who are supposed to be flat, or unusually large one-day P&L reports.
- The details underlying a trader's Value at Risk (VaR), including the long and short positions, on a daily or intra-day basis, as appropriate. Firms should also consider other risks associated with a trader's positions, such as liquidity risk, the adequacy of hedges and the risks associated with imperfect hedges. This includes understanding and reviewing the valuation of all positions, particularly positions in exotic instruments or instruments that have little or no market.
- Repeated or unusual requests by a trader to relax existing controls, including position or P&L limits.
- Trading in products that are outside of a trader's known expertise, without prior approval.
- Any other unusual or significant differences between a trader's account positions and the account activity, such as might be detected by comparison of gross and/or net position to the cash flows of positions; *i.e.,* margin/collateral calls to and from counterparties to the trades.
- A pattern of aged fails to deliver for long or short sales.

Whether these data points are reviewed manually, or with the use of automated surveillance tools, or some combination, a firm's controls should not just note deviations from normal trading patterns as red flags that might signal proprietary business risk, but as signals of possible regulatory risk as well. And, to the extent that firms use automated surveillance tools to identify such items, their internal control systems should include adequate and routine maintenance and testing of those systems.

Protection of Systems and Risk Management Information

In some cases, rogue traders have been able to falsify a firm's books and records to conceal illicit trading activity due to lapses in password security and other systems protections. Firms should make certain that each employee's access to systems is limited strictly to what is appropriate for the employee's function within the firm. This control should not be limited to traders; it should be in place for any employee whose role includes access to trading systems. If an employee's function changes within the firm, the firm should make sure that the employee's access changes accordingly. For example, if an employee moves from the back office to a trading desk, that employee's access should be changed to reflect his or her new role, and access to the back-office functions should be revoked. Firms should also make sure that access is suspended during any mandatory vacation period and cancelled promptly if the employee leaves the firm.

Firms also should protect information about surveillance or monitoring systems and procedures that might help employees circumvent those systems. For example, knowledge that the firm divides responsibility for reviewing certain trade monitoring functions by product type might help a trader who is creating fictitious trades to avoid detection by creating trades involving different products, so that the trades would not all be reviewed by the same personnel. In at least one recent case, a trader's intimate knowledge of back-office procedures and risk management procedures, including what would—and what would not—trigger heightened scrutiny, may have allowed him to avoid detection for a much longer period than he otherwise might have. Therefore, firms should limit knowledge about the details of their risk management procedures and systems to the extent possible and consider modifying them in response to personnel changes, such as a back office employee becoming a trader. Firms also should consider whether there are appropriate mechanisms in place to review all activity of a given trader.

Firms may want to consider more than a single password to allow access to certain systems. More sophisticated systems require three-factor authentication before access is allowed, including not only a password but also a security card or other I.D. such as a token ring, and a unique identifier such as a fingerprint. Firms need to weigh both the inconvenience and the cost of these additional security measures in determining which controls are appropriate.

Supervision and Accountability

Certain financial services companies have established matrix management structures such that employees may have both direct and dotted line reporting to multiple managers. While matrix management may make sense for an organization, it is important for employees to understand who they report to and what they are held accountable for in their day-to-day job responsibilities. Correspondingly, both the dotted line and the direct manager must have a clear sense of who is responsible for each aspect of the business. It is critical that responsibility for supervision of each aspect of the business be allocated to a specific manager and that these managers have frequent communications to understand their respective businesses. Documenting these supervisory responsibilities in writing is recommended.

Intercompany Transactions

Many FINRA firms are part of larger, complex financial services organizations. The FINRA member firm generally conducts a large number of intercompany transactions with its affiliates. Often the basic controls that are in place for third parties, including controls around credit risk and market risk, are waived for affiliated transactions. In light of the recent cases of unauthorized trading, firms may want to reevaluate whether certain third-party controls that limit their exposure would be appropriate for affiliated transactions. Further, reconciliations of intercompany transactions and balances should be performed on a regular basis.

Compliance Culture

As recent events have demonstrated, even the most rigorous internal controls and risk management procedures can fail if they are not effectively enforced and the effectiveness of that enforcement is directly related to the "tone at the top." A corporate culture that marginalizes the individuals or departments responsible for trade reconciliation and risk management will undermine the effectiveness of even the most elaborate policies and procedures. In reviewing the adequacy of their internal controls around unauthorized proprietary trading by individual traders, firms should pay attention to any systemic or cultural dynamics that may undermine the effectiveness of those systems. For example:

- Do mid- and back-office functions have sufficient independence, clout and profile within the organization? To whom do they report?
- Are mid- and back-office personnel adequately trained and encouraged to raise issues about suspicious activity, even if it involves successful traders or activity that is generating profits for the firm, or doesn't technically violate any limits?
- If operations, compliance or internal audit personnel receive a questionable or inadequate response by a trader, are they encouraged to challenge such a response and/or raise the issue to their supervisors where appropriate?

- If the firm operates in a global context, do its internal controls take into account any cultural differences that might discourage adequate internal oversight or reporting? For example, anonymous reporting might be appropriate in certain environments.
- Do traders who have incurred losses have incentives to disclose them and limit the damage because they understand that the failure to disclose will be considered an egregious violation of the firm's policies and procedures and dealt with accordingly, or are they encouraged, even implicitly, to incur more risk in order to avoid disclosure?
- Are internal control functions adequately funded, and are those who perform them adequately compensated, in relation to the role that they are asked to perform within the firm?

Conclusion

As firms review their internal controls around unauthorized trading in the wake of recent incidents, FINRA urges them to consider the practices described above, and to rigorously examine the broader compliance culture within which those controls are enforced. FINRA also reminds firms of the importance of ensuring that program areas tasked with detecting and preventing unauthorized trading possess sufficient independence, clout and funding, especially during challenging market conditions.

Endnotes

1 *See NASD NTM 99-92* (November 1999) and *NYSE Information Memo 99-42* (September 1999).

2 FINRA member firms that are also members of the NYSE are subject to incorporated Rules 342.21 and 351(e), which require firms to review proprietary, employee and employee-related trading in NYSE-listed securities and related financial instruments, and to conduct "internal investigations" of trades that may violate securities laws and rules prohibiting insider trading and manipulative and deceptive devices. Members and member organizations are further required to file with the Exchange reports relating to such internal investigations pursuant to Rule 351(e).

©2008. FINRA. All rights reserved. *Regulatory Notices* attempt to present information to readers in a format that is easily understandable. However, please be aware that, in case of any misunderstanding, the rule language prevails.