

## BDQUARTERLY

“In this time of market turmoil, where confidence in the integrity and trustworthiness of the securities markets has been damaged, there is an overwhelming need for strong enforcement of the securities laws — by the states, foreign regulators, and the SEC.”

— SEC Commissioner Luis A. Aguilar, North American Securities Administrators Association’s Winter Enforcement Conference, January 10, 2009

---

### How to Manage Compliance During a Financial Crisis

During a financial crisis, the strength of a broker-dealer’s compliance program will undoubtedly be tested. Customer complaints are on the rise and the industry is confronted with the prospect that a broker-dealer’s representatives may try to recoup lost assets and commissions through aggressive sales tactics. Conversely, investors will look to recoup losses, possibly by seeking high risk, high return investments that may pose suitability challenges.

With all of this occurring in the midst of industry-wide layoffs and a reduction in resources available to prevent, detect, and respond to regulatory issues, the role of a broker-dealer’s compliance department has never been more vital.

While job cuts may be unavoidable, this is not the time to cut compliance and legal department staff members, as echoed recently by many high ranking officials at the SEC and FINRA. Former SEC Chairman Chris Cox, in a November 13, (CONTINUED)

---

### INSIDE THIS ISSUE

How to Manage Compliance During a Financial Crisis . . . . .	1
Identifying and Eliminating CyberThreats to Customer Information . . . . .	4
FTC Red Flags Rule Impacts Broker-Dealers . . . . .	6
In Case You Missed It! . . . . .	7
Did You Know? . . . . .	7
Regulatory Notices, Updates, and Rule Changes . . . . .	8
Conferences/Roundtables . . . . .	9
Filing Dates . . . . .	9

2008 speech, stated that: “Now more than ever, companies need to take a long-term view on compliance and realize that their fiduciary responsibility requires a constant commitment to investors. That means sustaining their support for compliance during this market turmoil and beyond it as well.”<sup>1</sup>

As the current financial crisis continues, a broker-dealer should monitor the following areas within its compliance program:

#### **Procedures and Documentation**

This is no time to stray from adopted procedures, especially in the area of suitability monitoring and approval processes. Detailed documentation evidencing the rationale for a recommendation and supervisory approval is a critical review area within the annual compliance testing process and regulatory examinations. Suitability documentation is also invaluable when responding to customer complaints.

#### **Advertisements, Sales Literature, and Product Representations**

The current market environment may cause sales representatives to market aggressively and/or to misrepresent product risks when drumming up new business. Compliance departments must continue their vigilant advertising and sales literature review and approval process to prevent any potentially misleading representations that may lead to sales practice concerns. Regulators have recently focused their efforts on sales materials and representations made at seminars targeted to senior citizens and this will continue to be an area of focus in 2009.

Also, as evidenced by the nearly \$50 billion in settlements resulting from sales of auction rate securities,

be sure to reasonably disclose the features and risks associated with investment products. The settlements were largely related to sales representatives misrepresenting the inherent risks in these very complex investment vehicles and then falsely touting them as money market or cash equivalent investments. In light of this, broker-dealers should remember to revisit and strengthen their new product approval process and training, especially relating to complex investments.

#### **Short Selling**

In a speech by Lori Richards, Director of the SEC’s Office of Compliance Inspections and Examinations, to the National Society of Compliance Professionals on October 21, 2008, Richards stated:

*Examiners are also focusing on firms’ policies and procedures to prevent employees from knowingly creating, spreading, or using of false or misleading information with the intent to manipulate securities prices, and will be concluding a sweep of broker-dealers and hedge fund advisers in this area. These sweeps will most likely target potential “naked” short sale abuses and compliance with recently adopted short selling rules, which include the requirement for broker-dealers to close-out short sales in T+3 and the adoption of the “naked” short selling antifraud rule, or Exchange Act rule 10b-21. Among other issues, broker-dealers should consider the potential operational and procedural changes necessary to adequately document the location of securities and monitor for close-out requirement violations.*

A broker-dealer should implement an adequate combination of manual and automated surveillance controls over both long and short-aged fail-to-deliver securities to identify potential red flags. These controls, coupled with insider trading controls, ongoing trading activity reviews, and suspicious activity reviews, are key to preventing potential compliance issues related to short selling.

(CONTINUED)

<sup>1</sup>– Address to the SEC 2008 CCO Outreach National Seminar, Washington, DC.

### **Selling Away**

As sales representatives lose customer assets and commission revenue in the down market, they may be more willing to recover profits elsewhere by selling away, often through unregistered promissory notes or private placements. Selling away can be hard to detect, but at a minimum, be sure that: (1) all sales reps have signed attestations acknowledging that private securities transactions must receive pre-approval from compliance and identifying any outside business activities; (2) all emails, correspondence and communications are retained and reviewed employing a risk-based approach; (3) periodic internet searches are conducted to detect any unreported activities; (4) any unusual or suspicious lifestyle changes are questioned; and (5) any large withdrawals or patterns of customer account withdrawals receive additional scrutiny.

### **Structured Products**

Structured products are increasingly marketed to retail investors and while some of them offer full protection of principal, others do not. Following a market meltdown, it is normal for investors to seek out less risky investments to protect principal and prevent against any further losses. Considering the relatively high commissions charged and the fact that certain structured products offer full protection of principal, continued sales growth for these products is likely. Due to structured products having very different risk/reward profiles, features, and costs, each particular product should be approved separately by a broker-dealer's compliance department.

An October 20, 2008 FINRA webcast on structured products mentioned that it may be useful to consider if the customer's account has been approved for options trading in order to gauge if the customer has the financial knowledge needed to invest in structured

products. As with any investment recommendation, customers must receive adequate disclosures and information regarding product risks, features, liquidity, and expenses. Another thing to keep in mind is that, although structured products are sometimes rated by rating organizations, this reflects the credit risk of the issuer rather than the underlying market risk of the product. Firms should take steps to ensure this rating is not used to mislead investors about the level of risk embedded in the product.

### **Financial Controls**

In the current environment, more than ever, firms should revisit their financial controls over net capital and reserve computations, valuation methods, credit and counterparty exposure, and funding and liquidity access. Consider the following:

- **Capital vs. Liquidity** – Recent market events underscore the difference between having adequate capital and adequate liquidity, so be prepared to tailor your controls accordingly.
- **Valuation** – Investment and inventory positions should be valued based on a well documented, systematic approach that involves multiple departments to maintain pricing objectivity.
- **Counterparty Exposure** – Firms should consider conducting more frequent counterparty credit reviews (monthly or quarterly basis) instead of semi-annually or annually, which has been the industry standard.

In conclusion, while it may seem overwhelming to keep up to date on all of the regulatory issues during a financial crisis, a commitment to ask questions, provide full disclosure, and conduct thorough reviews will go a long way to ensuring compliance and protect against sales practice abuses.

---

## Identifying and Eliminating Cyber Threats to Customer Information

Cyber-crimes continue to be a real threat for brokerage firms on multiple fronts, putting the security of customer information and data at risk. In response, firms have been developing and implementing additional fraud prevention and security procedures. These enhancements and corrective measures are aimed at preventing and detecting cyber-crimes, which in recent years have led to significant losses to customer accounts, as well as financial liability and reputational damage to a number of firms.

Perhaps no area of the brokerage industry is more at risk of cyber theft than the online trading firms. When asked about the existing cyber-crime risks affecting brokerage firms, Shawn Moylan, Fraud Prevention Manager at Tradeking, a broker-dealer located in Boca Raton, Florida, stated, “Fraud prevention stands between a company’s existence and non-existence. Not only are the potential monetary losses substantial, but the loss of a sense of security would be devastating to an industry trusted with its clients’ hard earned assets.”

### Cyber Prevention Communities

As the sophistication and complexity of cyber attacks has increased, so has the number of partnerships among law enforcement agencies, private-sector companies, and academia to combat cyber threats. An example of one such organization is the National Cyber-Forensic Training Alliance (“NCFTA”), a non-profit organization consisting of more than 300 private companies partnering with the Department of Homeland Security, the Federal Bureau of Investigations (“FBI”), and the U.S. Postal Service.<sup>2</sup> Various industries, including financial institutions, credit card companies, pharmaceutical companies, and tech companies, have partnered with the NCFTA. The NCFTA takes a collaborative approach to preventing and detecting cyber crime by promoting cyber awareness,

conducting training, facilitating the sharing of information, and by performing forensic data analysis and testing.

Dane Vandenberg, Program Director of the NCFTA, remarked about the enormity of emerging stock fraud “hack and dump” schemes in an interview with ACA. Vandenberg stated that these sophisticated schemes are typically carried out by “big constellations of both U.S. and foreign persons.” Vandenberg further explained that many times the group that steals account login credentials may sell the information to another party that utilizes the information to access brokerage accounts to manipulate the stock price. Depending on the circumstances of the potential data and security breach, this may result in anti-money laundering implications for broker-dealers, specifically requiring the firm to file a Suspicious Activity Report in response to the breach.

The ongoing exploitation of new technologies and the complexity of computer crimes will assuredly challenge even the best equipped fraud prevention departments. When asked how to stay alert to emerging cyber issues and threats, Moylan added that “the most efficient and reliable source of intelligence is each other.” “We have the NCFTA to thank for creating the free exchange of ideas and strategies by establishing a neutral and trusted network of peers who are working toward the same common goal.” (CONTINUED)

---

<sup>2</sup>— As a matter of policy, ACA does not endorse service providers, including the NCFTA.

In his March 16, 2006 testimony before the House Small Business Regulatory Reform and Oversight Subcommittee, Steven M. Martinez, Assistant Deputy Director of the FBI's Cyber Division, noted the following regarding the success of the NCFTA:

*The NCFTA is a first-of-its-kind public-private alliance located in Pittsburgh, Pennsylvania. At the NCFTA, members of law enforcement work side-by-side with representatives from businesses on addressing the latest and most significant cyber threats. Through this collaboration the FBI has been able to identify and prosecute some of the most serious cyber criminals, including those who distribute computer viruses, operate large networks of compromised computers (known as botnets), and perpetrate fraud schemes such as phishing scams.*

#### Broker-Dealer Actions

A number of broker-dealers are not waiting to become victims of these types of cyber attacks and are deploying a broad array of internal security systems/measures to protect against cyber theft.

- Guarantees against losses caused by unauthorized activities in brokerage accounts is an industry accepted practice to mitigate reputational damage or public concern related to fraudulent transactions caused by identity theft.<sup>3</sup> However, this is also a costly practice, resulting in millions of dollars in firm losses.
- Many firms have begun to combine their information technology and compliance functions. Historically, these areas have operated separately, but now these functions have become allies in an effort to counteract the risks associated with cyber and identity theft.

- Data screening software tracks transaction patterns for strange anomalies that might trigger red flags when an account has been hijacked. For instance, brokerage software may check when a user accesses an online account through a suspicious IP address (the "address" given to every computer or server on the Internet). If the address denotes a foreign location known as a source for cyber crime, such as Eastern Europe, when the real customer lives in the U.S., the software generates an exception report.
- Most firms use security notices and website disclosure to discourage customers from accessing their online accounts from public computers that may be loaded with software designed to record login and password information.
- Existing suitability exception reports and reviews designed to indentify transactions that depart from customers' stated investment objectives can also be used to identify compromised accounts.
- A small number of broker-dealers offer a second level of customer authentication via a secure algorithmic token. These firms distribute handheld electronic units that display a six-digit numeric code that changes every minute. Account access security is enhanced because hackers would need both the customer password and current code displayed on the token to access the account.
- The use of advanced encryption technology has become commonplace. Furthermore, certain state regulations already require employee laptops and other portable devices containing or transmitting sensitive information to utilize data encryption software to prevent theft of data.<sup>4</sup>

(CONTINUED)

<sup>3</sup>— Identity theft crimes can take many forms but, in general, identity theft schemes originate by stealing personal identifiers (e.g. user-names, passwords, social security numbers, and account numbers, etc.) by methods ranging in complexity from dumpster diving and data security breaches to unknowingly installing data-stealing software.

<sup>4</sup>— For example, the Commonwealth of Massachusetts has enacted guidelines that become effective in January 2010 designed to protect the non-public personal information of Massachusetts residents.

- Many firms offer free security software and updates to help protect against keystroke loggers and eavesdropping software by scanning a customer's personal computer. Similarly, many firms have been educating their customers on how to safeguard personal information and protect themselves online.

### Conclusion

Whether your firm is creating an Identity Theft Program to comply with the upcoming Red Flags rules (see related story in this newsletter) or simply

strengthening its current data security controls, ACA recommends that firms conduct a risk assessment to identify security threats based on the specific activities conducted by the firm. Once the risks have been identified, firms should consider existing controls that can be leveraged to detect and prevent cyber theft and other identity crimes and build upon those when enhancing their data security programs. Additionally, firms are reminded not to overlook oversight and due diligence on third party service providers.

---

## FTC Red Flags Rule Impacts Broker-Dealers

Identity theft has been cited as the fastest growing crime in the U.S., impacting more than 10 million Americans annually, according to reports published by the Federal Trade Commission ("FTC").

In response to the rise in identity theft, the FTC has issued procedural requirements for "financial institutions" and "creditors" (as defined below) referred to as the Red Flags rule. The Red Flags rule had an original effective date of November 1, 2008, which was later postponed to May 1, 2009 in order to provide financial institutions additional time to develop the required procedures.

### Impact for Broker-Dealers

Most broker-dealers will fall within the definition of "financial institutions" and/or "creditor." A financial institution is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other organization that holds a transaction account owned by a natural person. A creditor is defined as an entity that extends, renews or continues credit, arranges for the extension, renewal or continuation of credit, or an assignee of a creditor who decides to extend, renew or continue credit. There are additional tests that a broker-dealer also needs to consider, but as

a threshold matter, most firms will be required (or should as a best practice) to develop and implement a written program to detect, prevent, and mitigate identify theft in connection with the opening or maintenance of certain accounts.

### Once Applicability is Determined

Once a broker-dealer determines it is subject to the Red Flags rules, it must put into practice a written identity theft program that is suitable to the firm's size, complexity, and activities. The program must include policies that distinguish relevant red flags for the accounts offered by the firm, detect red flags integrated in the program, respond to these red flags appropriately and ensure that the program is updated regularly to reflect changes in risks to consumers. The program should also consider the risks discussed in the Interagency Guidelines on Identity Theft Detection, Prevention and Mitigation (the "Guidelines"), including the 26 descriptive examples of red flags that may be relevant to the firm's activities and accounts.<sup>5</sup>

(CONTINUED)

---

<sup>5</sup>– See Supplement A to Appendix J within the Guidelines

### Approval and Administration

The Red Flags rules require that the initial written program be approved by the broker-dealer's board of directors, a committee of directors, or a designated senior manager. Ongoing, the program must include one of the above individuals or groups of individuals in the oversight, development and administration of the program. Finally, the broker-dealer must train staff to effectively maintain the program as well as exercise oversight of service provider arrangements.

### Rules for Card Issuers and Consumer Reports

Under the Red Flags rules, a broker-dealer that issues credit or debit cards to customers must adopt procedures to assess the validity of address change notifications received from customers, especially address changes occurring within 30 days of a request for additional or replacement credit cards.

Also, the Red Flags rule requires broker-dealers to develop policies and procedures to verify the accuracy of addresses within consumer reports and to ensure that the consumer report received relates to the customer in question.

### For More Information

FINRA issued Regulatory Notice 08-69 (November 26, 2008) with specific guidance as the application of the Red Flags rule to broker-dealers.<sup>6</sup> Although the FTC is responsible for interpreting and applying the Red Flag rules, the FTC has indicated that it is willing to work with FINRA to establish industry-wide consistency with respect to identity theft mitigation procedures and how the Red Flags rules apply to broker-dealers.

6- <http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p117448.pdf>

---

## In Case You Missed It!

On January 8, 2009, FINRA issued an Information Notice to remind firms that the SEC's December 12, 2006 Order permitting non-public broker-dealers to have their balance sheet and income statements audited by independent public accounting firms not registered with the Public Company Accounting Oversight Board ("PCAOB") expired December 31, 2008.<sup>7</sup> Firms with fiscal years ending December 31, 2008 or earlier may continue to rely on the December 12, 2006, SEC Order to conduct the 2008 annual financial audit of their income statement and balance sheet. Their fiscal year 2009 and subsequent audits must, however, be conducted by a PCAOB-registered accounting firm.

For more information, review the Information Notice at <http://www.finra.org/Industry/Regulation/Notices/2009/P117689>

---

## Did You Know?

FINRA fined more than 200 firms in 2008 totaling more than \$20 million for various regulatory violations. A total of 23 firms were fined approximately \$1.2 million for OATS reporting violations.<sup>8</sup>

---

7- Exchange Act Release No. 54920, 71 FR 75779 (December 18, 2006).

8- As estimated by ACA from published FINRA releases.

## Regulatory Notices, Updates, and Rule Changes

### Financial Industry Regulatory Authority

#### December

**Regulatory Notice 08-82** FINRA Reminds Firms of Their Sales Practice Obligations with Regard to Cash Alternatives.

**Regulatory Notice 08-81** FINRA Reminds Firms of Their Sales Practice Obligations with Regard to the Sale of Securities in a High Yield Environment.

**Regulatory Notice 08-78** FINRA Announces SEC Approval and Effective Date for New Consolidated FINRA Rules Relating to Warrants, Options and Security Futures.

Effective Date: February 17, 2009

**Regulatory Notice 08-74** FINRA Provides Guidance on Amendments to FINRA Rules Relating to SEC Regulation M.

Effective Date: December 15, 2008

**Regulatory Notice 08-73** SEC Approves Amendments to NASD Rule 2220 to Update the Standards for Options Communications.

Effective Date: March 4, 2009

#### November

**Regulatory Notice 08-70** FINRA Provides Guidance Regarding Credit for Extraordinary Cooperation.

**Regulatory Notice 08-69** Alert to Member Firms About the Federal Trade Commission's FACT Act Regulations and the Announcement of the FTC's Decision to Delay Enforcement of the Red Flags Rule until May 1, 2009

**Regulatory Notice 08-66** FINRA Addresses Firms' Retail Foreign Currency Exchange Activities.

#### October

**Regulatory Notice 08-64** Amendments to Incorporated NYSE Rules to Reduce Regulatory Duplication.

Effective Date: November 11, 2008

**Regulatory Notice 08-60** FINRA Announces Temporary Margin Maintenance, Net Capital and Reserve Formula Requirements Related to Money Market Mutual Funds.

Effective Date: October 21, 2008

**Regulatory Notice 08-56** FINRA Announces the Publication of Consolidated Interpretations of SEC Rules Governing Financial Responsibility, Customer Protection and Books and Records Posted on October 15, 2008.

### Securities and Exchange Commission

#### December

**Release No. 34-59062** Amendment to Municipal Securities Disclosure File No.: S7-21-08

Effective Date: July 1, 2009

#### November

**Release No. 34-58775** Amendments to Regulation SHO File No.: S7-19-07

Effective Date: October 17, 2008

**Release No. 34-58774** Naked Short Selling Antifraud Rule File No.: S7-07-08

Effective Date: October 17, 2008

### Municipal Securities Rulemaking Board

#### October

**MSRB Notice 2008-43** First Phase of MSRB Gateway Simplifies Regulatory Tasks

### Financial Crimes Enforcement Network

FinCEN Withdraws Dated AML Rule Proposals for Unregistered Investment Companies, Commodity Trading Advisors, and Investment Advisers, October 30, 2008.

## Conferences/Roundtables

### ACA Compliance Group

#### Spring Conference

April 22-24, 2009 • Bellagio Las Vegas, NV  
[www.acacompliancegroup.com/conference09/](http://www.acacompliancegroup.com/conference09/)

### FINRA

#### Annual Conference

May 6-8, 2009 • Boston, MA

### ACA Compliance Group

#### CCO Regional Roundtables

Feb. 25, 2009 • Washington, DC  
 April 6-8, 2009 • Chicago, IL  
 June 9-11, 2009 • Boston, MA

## Filing Dates

### 2009 Monthly/Quarterly FOCUS Part II/IIA Filings

Month Ending	Due Date
January 31, 2009	February 25, 2009
February 28, 2009	March 24, 2009
March 31, 2009	April 24, 2009

### 2009 Annual Audit Filings

Fiscal Year End	Due Date
December 31, 2008	March 2, 2009
January 31, 2009	April 1, 2009
February 28, 2009	April 29, 2009
March 31, 2009	June 1, 2009

### 2009 Customer Complaint Filings

Quarter Ending	Due Date
1st quarter 2009	April 15, 2009
2nd quarter 2009	July 15, 2009

**ACA Compliance Group (ACA) is a full-service compliance consulting firm committed to offering unparalleled regulatory compliance and GIPS verification services** designed to satisfy the needs of investment advisers, private funds, investment companies, insurance companies and broker-dealers.

In these uncertain times, compliance officers must closely monitor changing regulations while fulfilling their current compliance obligations. As an alternative to increasing their compliance staff, leading financial services firms choose to partner with ACA.

ACA clients benefit from the creation of customized compliance programs that meet the increasingly complex regulatory requirements. Please contact us to discuss how ACA's team of former FINRA, NYSE and SEC regulators can help you effectively manage your compliance burden.

Nothing herein should be construed as legal advice or as a legal opinion for any particular situation. ACA makes no representations about the accuracy of the information contained herein or its appropriateness for any given situation.