

May 2010

IN THIS ISSUE

- United States
 - Recordkeeping Critical to Comply With Rule 2330
 - How to Succeed as a Chief Compliance Officer
 - Focus on FINRA RN 10-06: The Principle of Adoption in Social Media
- Canada
 - The Challenges and Rewards of Risk-Based Regulation — Mining the Canadian Experience
- Global
 - The Spirit of the Times: A Global View of Regulation

This complimentary newsletter addresses current regulatory concerns around the world and provides broker-dealers, investment advisers, and insurance companies with tips and suggestions for meeting regulatory obligations.



United States

Recordkeeping Critical to Comply With Rule 2330

Recently FINRA announced in [Regulatory Notice 10-05](#) the consolidated Rule 2330 (formerly NASD Rule 2821) that establishes sales practice standards regarding recommended purchases and exchanges of deferred variable annuities. In addition to the main sections of the Rule, which have been well covered in FINRA notices and guidance, it highlights some recordkeeping issues. The purpose of this article is to discuss what 10-05 offers about establishing and maintaining supervisory procedures and a variety of issues on the handling of customer funds and checks.

Although all of the rule's provisions were effective on February 8, 2010, the notice seeks to answer some questions regarding FINRA's limited interpretive relief from the requirements of FINRA Rule 2150(a) and FINRA Rule 2320, which respectively, prohibit firms from making improper use of customer funds, and require firms to transmit promptly to issuers all applications and purchase payments for variable contracts.

FINRA provides guidance in Regulatory Notice 10-05 which is intended to help firms understand what is required to preserve the limited interpretive relief from the consolidated rules. This allows firms to perform comprehensive and rigorous reviews of recommended transactions in deferred variable annuities under FINRA Rule 2330 without causing firms to 1) establish burdensome practices around accounts for the exclusive benefit of customers, or 2) try to meet unreasonable requirements around prompt forwarding during review.

Improved recordkeeping will play a critical role in assuring compliance with this rule. FINRA originally stated that "a firm may hold an application for a deferred variable annuity and a customer's non-negotiated check payable to an insurance company for up to seven business days without violating either NASD Rule 2330 or 2820 if the reason for the hold was to allow completion of principal review of the transaction pursuant to NASD Rule 2821." To avoid violations, firms must be able

MEET WITH YOUR PEERS

► Webinar: Record-Keeping Implications of FINRA Regulatory Notice 10-05

June 9, 2010

Join LIMRA's Senior Regulatory Advisor Larry Niland on June 9th for our next free Webinar. Larry will lead a conversation on the record keeping implications of FINRA Regulatory Notice 10-05 regarding the sale of variable annuities. With the recent announcement of NAIC's Annuity Suitability Model regulation, this webinar will have broad appeal. Limited "seating" is available — [register today](#).

NOTABLE

► AML Independent Testing and Consulting addresses firms' AML/BSA/OFAC concerns. Contact us at compliance-regsvs@limra.com.► Follow us on Twitter (http://twitter.com/LIMRA_CRS) to receive crucial industry news, as well as information about our upcoming Webinars and new services.► Join the LIMRA/NSCP Compliance Roundtable group on LinkedIn. To request membership, visit <http://www.linkedin.com/groupRegistration?gid=2249752>.

CONTACT US

To subscribe to *LIMRA Regulatory Review* or read previous issues, please [visit us online](#).

To suggest article topics or request article reprints:

Stephen Selby
sselby@limra.com
<http://www.linkedin.com/in/stephenselby>

For more information about LIMRA's services:

LIMRA Compliance and Regulatory Services
 300 Day Hill Road, Windsor, CT 06095
 Phone: 877-843-2641
 Email: Compliance-RegSvs@limra.com
www.limra.com/compliance

Recordkeeping Critical to Comply With Rule 2330

(continued from page 1)

to demonstrate at every step in the process that they met the requirements for limited interpretive relief.

In response to industry commentary on 2821, FINRA proposed, and the SEC approved, amendments that changed the starting point for the review period — from the date when the customer signs the application to the date when a firm's OSJ receives the complete and correct application. The notice explains that limited interpretive relief continues to apply even though the triggering event for the principal review period has changed, but **only** if seven (7) certain conditions are present.

1. The reason that the firm is holding the application for a deferred variable annuity and/or a customer's non-negotiated check payable to a third party is to allow completion of principal review of the transaction pursuant to FINRA Rule 2330.
2. The associated person who recommended the purchase or exchange of the deferred variable annuity makes reasonable efforts to safeguard the check and to promptly prepare and forward a complete and correct copy of the application package to an OSJ.
3. The firm has policies and procedures in place that are reasonably designed to ensure that the check is safeguarded and that reasonable efforts are made to promptly prepare and forward a complete and correct copy of the application package to an OSJ.
4. A principal reviews and makes a determination of whether to approve or reject the purchase or exchange of the deferred variable annuity in accordance with the provisions of FINRA Rule 2330.
5. The firm holds the application and/or check no longer than seven business days from the date an OSJ receives a complete and correct copy of the application package.
6. The firm maintains a copy of each such check and creates a record of the date the check was received from the customer and the date the check was transmitted to the insurance company or returned to the customer.
7. The firm creates a record of the date when the OSJ receives a complete and correct copy of the application package.

If any of these seven conditions are not present, FINRA's interpretive relief will not apply and it will enforce Rules 2150(a) and 2320(d), as appropriate. So what must firms do to preserve this interpretive relief?

The first step is to review firm procedures to confirm that policies and procedures exist that ensure that checks are logged and safeguarded prior to principal review being carried out, and that all applications and checks are processed within the required timeframes. Procedures should include:

1. Logs that indicate the customer name, check information, application date, and the date the package is received at the OSJ.
2. Logs should also include the payee, amount of the check, and time of day.

3. Ideally this log should be accessible to firm supervisors and auditors for periodic review.
4. Similar logs should be in place at the locations used to safeguard checks during the review.
5. Firms should review procedures for specificity in detailing who, by named role, should review and log in packages including checks and applications, how such review is conducted, and clear processes, logs and procedures and timelines around forwarding of complete packages for principal review.
6. Procedures should spell out the process to be used for logging and safeguarding checks until transmitted, and what steps are to be taken in the event the application package is deemed incomplete, or check payee information is incorrect (e.g., payable to the firm and not the insurance company); and
7. Procedures must include specific instructions for returning checks to clients and safeguarding checks at firm offices.

Many firms already employ a centralized electronic log, where updates are made in real time by all locations receiving check and application packages, and the firm's compliance or supervisory staff are able to monitor centrally, to see in real time the status and location of any cases that may be approaching the seven-business-day limit and take appropriate action to avoid violations. Firms may also employ a "travel log" or "transmittal form" or "jacket" that follows each application package and documents each step or actions along its route to transmittal to the insurer. While a paper form can be used, an electronic travel log would allow the firm to see each step a package makes in its progress through the firm, and use those records to demonstrate to FINRA that prompt processing and review did occur.

Finally, don't forget to include in your FINRA Rule 3130 testing of supervisory controls (formerly NASD Rule 3012) testing of all of the above to the extent the firm is relying on the limited interpretive relief.

By Larry Niland, Senior Regulatory Consultant, LIMRA, and former CCO of the John Hancock Financial Network. Please contact Larry at 877-843-2641 or lniland@limra.com if you have any questions about this article, or would like to learn more about LIMRA's Web-based [Supervisory Controls System](#).

Join Larry Niland on June 9th for a free Webinar on the record-keeping implications of FINRA Regulatory Notice 10-05 regarding the sale of variable annuities. "Seating" is limited, so [please register today](#).

How to Succeed as a Chief Compliance Officer

"Risk is like fire: If controlled it will help you; if uncontrolled it will rise up and destroy you."

My introduction to the compliance business was 18 years ago, with the creation of a compliance function. Back then, in the early 1990s, compliance was not the term of art, nor the practice it is today. When we started, we did not even know what to call the function. At first we called it Management Internal Control (MIC), a name representative of a risk management function owned by business. Later we changed the name to Risk Management and finally to Compliance and Risk Management.

During those years, I had a number of titles including MIC Officer, Risk Management Officer and Chief Compliance and Risk Officer. Now, almost 20 years later, it seems that every business has a compliance function headed by a Chief Compliance Officer (CCO). The function generally has responsibility for business, operational, legal, and regulatory risks and matters. It extends to all parts of the business including home office, front-end and back-end operational functions, systems, sales, marketing, product development, as well as some financial roles (generally controls required by Sarbanes-Oxley).

Being a new CCO and having to establish a new risk function can be challenging. But it creates an opportunity to establish excellence in the business and to be a key player in leading the business to success. While there is not a formula that guarantees success of the CCO, there are steps that can lead to that success.

Step 1: Creating the "Right" Culture

First and foremost, a successful CCO must create the "right" culture. What is the right culture? Consider this example:

You are driving in your car down the street toward an intersection. As you approach the intersection, the traffic light turns from green to red. What do you do? You stop. You wait until the light turns green again and then proceed. Why don't you pull up to the intersection and look all ways for cars or a policeman and if none are present, then proceed through? Culture is why.

In addition, stopping and waiting for a red light is second nature for us. We react without really thinking. Why? Culture is why.

Culture is the impetus for adherence to the rules. In the right culture, most people act with honesty, integrity, and high ethical standards. Further, such behavior comes naturally, without thought.

Without the right culture in the traffic light example, the streets would be chaos and/or we would need a cop on every corner for prevention, or to apprehend the drivers. Society can neither operate nor survive under a system of chaos. Nor can we afford a cop on every street corner.

The same is true for business. We want officers and employees to act with integrity, honesty, and high ethical standards. We want them to behave accordingly, not necessarily because we have controls in place, but because the culture fosters and accepts such behavior. We want the right behavior to become second nature. They should not have to think about how to act properly.

Personal responsibility is at the core of the right culture. The compliance function should not need or want a cop at every juncture of the business. It would cost too much, and in the end would fail. So a CCO must work to build a culture where “doing the right thing” is expected from all officers and employees. Consequently, that culture should penalize bad behavior and reward right behavior.

It is important to note, however, that while personal responsibility is a core element of the right culture, a CCO cannot operate with blind faith. The system of internal control must include a detection element to identify those who violate the culture.

For compliance to succeed, the “tone from the top” must be one that communicates and supports the right culture. Senior leaders must exhibit a zero tolerance standard through their words and actions. However, the tone from the top cannot alone create the right culture. There are many steps and activities that the CCO must take to create, foster, and maintain a culture that results in people doing the right thing, the first time, all the time.

So how does the CCO build the requisite culture? Here are some simple and practical actions.

Actions and Steps to Build the Right Culture

- Get buy-in at all levels of the business — not just from management. The CCO should partner with everyone; not just senior management.
- Act so that all are comfortable coming to the compliance function, not only to report violations, but also to seek advice and counsel. The CCO should proactively offer advice and solutions. Advice is better when provided up-front when new processes, sales, etc., are being proposed and planned. The CCO should be seen as part

of the solution that supports the company’s business objectives.

- Consequently, the CCO should make every attempt to say “yes.” When the law prohibits this, of course, a CCO must say “no.” But the CCO should also offer alternatives and other options for the business.
- Develop, communicate, and train based on the standards, rules, policies, and expectations of each and every function and individual.
- Be easy to do business with. The CCO should be easy to approach and readily available.
- Act with speed; act fast. A CCO should not slow the business down; but should instead be viewed as part of the business process.

Without a doubt, compliance with laws, rules, and policies is the primary responsibility of the CCO. An environment of zero tolerance for absolute risks should be the case without exception. Beyond that, the CCO should establish an acceptable risk appetite and risk mitigation process to manage those inherent risks. Such a culture and environment ensures compliance with all mandatory laws, rules, regulations, public policy standards, and internally generated standards such as policies and procedures, codes of conduct, etc. And it provides for an internal control system where risks are identified up front and managed in furtherance of business success.

(Note: Absolute risks are laws, rules, policies are clear; violations should never be tolerated. Inherent risks may or may not happen. In a compliant culture, controls are designed and built to manage and mitigate inherent risks.)

Creating the right culture is a critical task for a CCO. It requires hard work. But without a culture of honesty and integrity a CCO will not succeed. Achieving the right culture will not *guarantee* success, but it will get you most of the way there.

Step 2: Developing a Risk-Based Environment and Management System

“Take calculated risks; that is quite different from being rash.”

— General George S. Patton, World War II General

Compliance is more than adhering to laws and regulations — it is making sure that a company and its employees adhere to the risk culture, policies, procedures, and controls. The CCO should steer and direct the organization to stay within mandatory boundaries of laws and regulations as well as the voluntary boundaries of risk culture, tolerance, appetite, and values.

So How Does the CCO Do This?

The CCO should establish a risk-based environment and management system with zero tolerance for absolute risks. No doubt, compliance with all laws, rules, and policies is the primary responsibility of the CCO. An environment of zero tolerance for absolute risks should be the case without exception.

A quality, risk-based environment and management system communicates and ensures absolute compliance with all mandatory laws, rules, regulations, and public policy standards.

However, not all risks can be avoided or eliminated. Thus, the CCO should establish an acceptable risk appetite and risk mitigation process to manage these inherent risks. Inherent risks are intrinsic to a business activity and arise from exposure to, and uncertainty of, possible future events, or changes in business or economic conditions. Inherent risks may or may not happen. Under a risk management system, controls are designed and built to identify, manage, monitor, and mitigate inherent risks. The risk management system is the systematic application of processes and structures that enable an organization to identify, evaluate, analyze, optimize, monitor, improve, or transfer risk.

The only way an organization can manage risk appropriately is if acceptable and unacceptable risk is defined. The CCO should clearly define, establish, and communicate the environment of risk taking, acceptance, tolerance, and appetite. If the CCO does not do this — risk taking is up to individuals and the integrity of the organization is in jeopardy.

Steps to Build a Risk Environment and Management System

The first step in developing a risk-based environment is to identify the risks and potential areas of vulnerability in the business. Risks can be identified from different sources:

- Internal audit reports
- Ethics reports
- Regulatory examinations and inquiries
- Management reports
- Self-initiated risk assessments
- Results from preventive controls
- Information gleaned from business partnerships

Once the risks have been identified, the second step is for the CCO to determine the proper action regarding the risk.

This requires the CCO to establish an acceptable risk appetite. There are three options for managing inherent risks:

- **Reduce and mitigate** — This is for those risks that are too great to accept. Action and strategies are developed and implemented to reduce or mitigate exposure.
- **Transfer** — The exposure for some risks can be transferred through outsourcing or by the purchase of insurance.
- **Retain and accept** — Some risks will be acceptable without any mitigation efforts. However, the organization should consider budgeting for the exposure.

Each identified risk should be evaluated to determine the desired course of action. One of these three courses should be applied to each risk.

Finally, once the risks have been identified, a risk appetite has been determined, and a management plan has been implemented, a monitoring and reporting process needs to be instituted.

This is a continuous process. It never ends. The CCO must continually identify risks, determine risk treatment, implement, and monitor.

Step 3: Building an Internal Control Framework

“We are constantly working towards the highest level of compliance possible.”

— Mike Davidson, 20th Century American Author

Along with a compliant culture and a risk management system, a CCO needs to build a framework and process of internal control. A framework of internal control gives the CCO reasonable assurance that the culture and risk management system is working. The CCO should construct an internal control framework that surrounds the compliant culture and environment created in Steps 1 and 2, to ensure that compliance works “first time and every time.”

Elements of an Internal Control Framework

In order to establish an internal control framework, a CCO must take action regarding:

- **Policies and Procedures:** Formulate a set of policies and procedures and other internal guidelines and standards. Policies and procedures are documents that describe an organization’s policies or rules for operation of the business and the procedures to implement or fulfill them. These rules should be made available to all employees, along with awareness training.

- **Workplace Code of Conduct:** Create a code of conduct that details the basic ethical behaviors expected of employees. Potential topics include: Compliance, Conflict of Interest, Equal Employment Opportunities, Sexual and other Discriminatory Harassment, Gifts and Favors, Government Contacts, Lobbying, Political Campaign Activity, Fair Dealing, Respect and Nepotism. The Workplace Code of Conduct should be distributed to all the organization's employees and mandatory training should be provided.
- **Operational Process Maps:** The compliance function, along with business, should map or outline all operational processes. The results will allow for a review of compliance and subsequent changes to correct any areas out of compliance. The CCO should require the maintenance of the maps and operational adherence to the mapped processes. The business should use the maps as a tool when the process is being changed, to verify that the new or changed elements are compliant.
- **Front-End and Back-End Controls:** Build effective controls into front-end and back-end processes. Front-end controls are "preventive" in that they should prevent non-compliant actions or transactions before they occur. Back-end controls are "detective" in that they detect compliance violations after the action or transaction has occurred. The emphasis should be on front-end preventive controls over back-end detective controls. Business is best served by prevention of non-compliant actions. In the ideal scenario, back-end controls will be a second check for errors or violations.
- **Compliance Objectives:** Formulate compliance objectives. Communicate these objectives and goals to all employees, and ascertain that they understand what is acceptable and unacceptable.
- **Violation Reporting Process:** Create a process for employees to ask questions and to report potential violations. This process should be easy to use and should allow for anonymous reporting. A good approach is three-pronged: (1) A hard copy set of forms; (2) A telephone hotline; and (3) An e-mail address. Communicate this process for reporting to all employees.
- **Management Reporting:** Communicate to management, as well as all employees throughout the organization, the successes, and failures, of the risk management system.
- **Risk Management Committee:** Establish a risk management committee. This group should meet regularly to review projects, proposals, proposed rules and policies, etc. All functions and disciplines should be represented on the risk management committee.

- **Processes to Ensure Against Future Violations:** This includes changing and replacing ineffective controls when identified. Corrective action should include disciplinary action against employees when necessary. Change and replace ineffective controls.

An effective internal control framework allows the CCO to exercise reasonable oversight. An internal control system identifies risks, and allows for planning to eliminate, mitigate, or transfer that risk. Monitoring ensures that the laws, rules, and internal policies are being followed.

Succeeding as a CCO may be daunting. But it is a requisite role for a business to succeed today. Following these three steps: (1) Creating the Right Culture; (2) Developing a Risk Management System; and (3) Building an Internal Control Framework will not guarantee success — but will certainly provide any CCO, old or new, with the robust tools needed to ensure a compliant business.

By James Yoakum, LIMRA Consultant

Focus on FINRA RN 10-06: The Principle of Adoption in Social Media

In Regulatory Notice 10-06, FINRA addresses a firm's obligation to supervise the use of third party content on social media sites, through the Securities and Exchange Commission's (SEC's) theory of "adoption" and "entanglement." This article will explore the theory of adoption, and how a firm might manage the associated risks of "adopting" third party content, based on SEC publications.^{1,2} The theory of adoption was not originally directed at the use of third party content by broker-dealers or investment advisers, but in fact applied to communications of publicly traded companies under Reg. FD.³ The specific application of the theory of adoption to broker-dealer regulation is apparently attributable to FINRA. The SEC's original publications are therefore at least instructive regarding its view of general standards for responsible communications. The language of the SEC in its 2008 publication specifically references "hyperlinks." This article retains the SEC's original language, but keep in mind that by applying the SEC's theory of adoption to the use of social media by broker-dealers, FINRA implies that the adoption of content is of primary importance, rather than the specific *technology* used.

Overview of the Adoption Theory in Electronic Media

The theory of adoption refers specifically to the liability a company assumes when displaying, quoting, referencing, or linking to third party content with the result that

the company has “explicitly or implicitly endorsed or approved the information.”⁴ Third party content is neither intrinsically good nor intrinsically bad. Why then are firms liable for links or adoption of third party content? The SEC states:

*...we begin with the assumption that providing a hyperlink to a third party site indicates that the company believes the information on the third party web site may be of interest to the users of the web site.*⁵

There are two critical points to consider in this statement. First, hyperlinking or otherwise connecting is a deliberate act. Second, the SEC assumes that the linking party has considered the content, and decided that such content is interesting to viewers. In the broker-dealer sales context it is reasonable to assume that broker-dealers adopt content because it is in their economic interest to do so.

By citing the theory of adoption in FINRA RN 10-06, it is clear that FINRA believes that there are mechanisms within social media to which adoption applies. One example of such a mechanism is the “Recommendation” feature on LinkedIn. There has been much made of “Recommendations” as a form of prohibited “testimonials” under registered investment adviser regulations. However, firms should also consider the possibility that the acceptance and display of such recommendations on LinkedIn constitutes adoption, thereby making the broker-dealer liable for the content.

A second example of adoption is the embedding of YouTube videos within a company’s Web site. There is a wide range of content available on YouTube, from opinion pieces by private citizens to hard news created by respected news outlets. The mood of multi-media presentations may contrast with the apparent intent of the spoken word or create a subtext that may alter the plain language of the spoken script. When adopting third party multimedia content, broker-dealers should consider not only the script, but also the visual and auditory impact of the presentations.

Is Disclosure a “Safe Harbor”?

*We again remind companies that specific disclaimers of anti-fraud liability are contrary to the policies underpinning the federal securities laws.*⁶

To the extent that the firm knew or should have known that third party content was fraudulent or misleading in nature, disclaimers and disclosure apparently have no curative effect. This position squares well with FINRA Rule 2020 Use of Manipulative, Deceptive or Other Fraudulent Devices, and FINRA IM-2310-2 Fair Dealing

with Customers. The limited benefit of a disclaimer/disclosure approach logically ties back to the SEC’s position that hyperlinking (i.e., adopting) to third party content is a conscious decision of a firm that is based, by extension, in their own commercial best interest. Does this mean that disclosures and disclaimers have no benefit? No. In fact, as we will discuss in the next section, context is critical to clearly communicating the intent behind the adoption of third party content.

What Should Firms Consider When Adopting Content?

The information contained in this section is not intended to be exhaustive. As the use of social media sites matures, it is almost certain that new ways of adopting content will emerge. Companies will need to consider not only the adopted content, but also the manner in which content is adopted. This is significant as it may impact the context in which the adopted content is viewed and used. As noted earlier, both LinkedIn “Recommendations” and embedded YouTube videos represent adopted content, but each is clearly a different mechanism for relaying a message.

Firms might consider treating adopted content differently if it is used in “static” vs. “interactive”⁷ content functions within social media sites. Static content is subject to review (at a minimum) by the company prior to use. Interactive content can be reviewed after the fact. For example, should a broker-dealer allow a registered representative to include hyperlinks in responses to public comments on “walls” e.g., on Facebook? Should a firm allow its registered representatives or marketing departments to “re-Tweet” content on Twitter without specific prior approval from a supervising principal?

What context has the company provided for the adopted content? The SEC sets forth several principles:⁸

- “The company should consider explaining the context for the hyperlink — and thereby make explicit, rather than implicit, why the hyperlink is being provided.”
- “The nature and content of the hyperlinked information also should be considered in deciding how to explain the context for the hyperlink.”
- “The degree to which a company is making a selective choice to hyperlink to a specific piece of third party information...”
- Provide context to “... to avoid the inference that the company is also commenting on or even approving its accuracy, or was involved in its preparation.”

Firms should also consider the impact of adopted content on the intended audience. For example, the magazine *Working Mother*⁹ rates the top companies for working

families. A firm's rating by *Working Mother* might have a different impact in recruiting material than it would in general advertising, requiring greater context.

In addition, compliance professionals should apply the standards for public communication, including disclosures, for all applicable regulatory jurisdictions and products represented.

Are There Best Practices?

The science of social media, like social media itself, is still maturing. It is not therefore prudent, to label any practices as "best practices" yet, other than following the current, general rules concerning communications with the public, and "Standards of Commercial Honor and Principals of Trade." Specific best practices will take time to emerge. One take-away from reading the SEC's publications and by visiting its Web site, is that the SEC does take its own suggestions seriously. For example the SEC states:

In addition to an explanation of why a company is including particular hyperlinks on its website, a company may also determine to use other methods, including "exit notices" or "intermediate screens" to denote that the hyperlink is to third party information.¹⁰

A visitor to the SEC Web site will see just such exit screens in use for the link that the SEC provides to the University of Cincinnati's *Securities Lawyer's Deskbook*.¹¹

Conclusion and Recommendations

The SEC and FINRA are clearly aware of the importance of the Internet and of social media. The SEC notes that "approximately 80% of investors in mutual funds in the United States have access to the Internet in their homes."¹² It is also clear that the SEC, FINRA, and the NAIC are experimenting with social media themselves. The SEC and FINRA both have multiple Twitter feeds and the NAIC has a fan page on Facebook.

While it is too early to talk about best practices in social media, there are guiding principles. Those principles include, but are not limited to the following:

1. Understand the adopted content.
2. Understand the medium used. LinkedIn recommendations and embedded YouTube videos are both adopted

content, but are fundamentally different media.

3. Provide context for adopted content to clearly communicate the intent of adopting specific content.
4. Consider the specific audience and the impact of adopted content on that audience.
5. Follow current regulations for communications with the public for all regulatory jurisdictions in which the company does business and for all products represented.
6. Understand the difference between static and interactive content.

Last, but perhaps most important — become a student of social media. Compliance professionals understand the rules and regulations, but need to fully engage with others in social media to understand how the technology works.

By Stephen Selby, Director of Regulatory Services, LIMRA. Please contact Stephen if you have any questions about social media compliance at 860-285-7858 or sselby@limra.com. Connect with Stephen at <http://www.linkedin.com/in/stephenselby>.

¹Commission Guidance on the Use of Company Web Sites, Securities and Exchange Commission, 17CFR Parts 241 and 271 [Release No. 34-58288], Effective August 7, 2008

²Use of Electronic Media, SEC Interpretation, 17 CFR Parts 231, 241 and 271 [Release Nos. 33-7856], May 4, 2000

³On August 15, 2000, the SEC adopted Regulation FD to address the selective disclosure of information by publicly traded companies and other issuers. Regulation FD provides that when an issuer discloses material nonpublic information to certain individuals or entities — generally, securities market professionals such as stock analysts, or holders of the issuer's securities who may well trade on the basis of the information — the issuer must make public disclosure of that information.

⁴q.v., Commission Guidance on the Use of Company Web Sites, page 32, paragraph 1 and footnote 77, Effective August 7, 2008

⁵q.v., Commission Guidance on the Use of Company Web Sites, page 34, Effective August 7, 2008

⁶q.v., Commission Guidance on the Use of Company Web Sites, page 37.

⁷FINRA Regulatory Notice 10-06, page 5, Question and Answer 5

⁸Commission Guidance on the Use of Company Web Sites, pages 34-35

⁹<http://www.workingmother.com/BestCompanies/work-life-balance/2009/08/working-mother-100-best-companies-2009>

¹⁰Commission Guidance on the Use of Company Web Sites, pages 35-36

¹¹<http://www.sec.gov/investor/pubs/securitieslaws.htm> q.v. "Tip" section

¹²Commission Guidance on the Use of Company Web Sites, page 6, footnote 10

The Challenges and Rewards of Risk-Based Regulation — Mining the Canadian Experience

A glimpse at Canadian insurance regulation indicates that risk-based approaches can be effective, even in tandem with rules-based regimes, when stakeholders agree on principles and outcomes and *consistently* engage in activities that support them. There are some compliance challenges, however, and situations where risk-based programs could falter.

The Office of the Superintendent of Financial Institutions (OSFI), a federal regulator concerned with the solvency of federally regulated financial institutions (FRFIs) including banks and insurers, focuses on risk management, generally providing guidance and allowing companies to determine how to achieve desired outcomes. If the condition of Canadian banks following the recent global economic meltdown is any measure, OSFI's risk-based approach is effective.

It is the job of provincial insurance regulators to protect consumers from illegal and unfair market conduct practices. (Market conduct practices concern OSFI if they pose material financial risk to an insurer.) Provincial regulation is more rules-based. Laws and regulations proscribe practices such as fraud, misrepresentation, and churning. Many provincial regulators also target risks, including mining consumer complaints data to determine whether insurers have systemic market conduct problems that might require their attention.

Corporate governance is a focal point. OSFI provides extensive guidance, while provincial regulations such as Ontario's Duty of Care regulation place accountability on insurers' boards, in this instance to ensure that all producers are screened, monitored, and reported if they are not suitable.

Cooperation, harmonization, and avoidance of duplication are primary themes for Canadian regulators' groups. The Canadian Council of Insurance Regulators, which includes both OSFI and the provinces; the Joint Forum of Financial Market Regulators, consisting of pension, securities and insurance regulators; and the Canadian Insurance Services Regulatory Organization, an association of regulators of insurance intermediaries, all aim to achieve these goals.

Regulators engage in substantial industry consultation before imposing regulation. There are few surprises. By the time a regulation is in effect, the industry has provided input and engaged in discussions with the regulator.

How Should Regulatory Risk Be Measured?

OSFI requires FRFIs to have Legislative Compliance Management programs (LCMs) to manage legal and regulatory risks wherever they do business. The framework established must include an enterprise-wide definition of regulatory risk and must identify, assess, and communicate regulatory requirements. Oversight procedures are expected to ensure that day-to-day compliance is well-managed while "significant problems" are identified, escalated to senior management and the Board, and resolved — requirements similar to those of FINRA 3012 and SEC 38a-1 in the United States.

OSFI concentrates on material financial risk to the larger enterprise, not to its individual businesses, so companies' LCMs tend to be concerned with risk at the macro level. Many FRFIs have adopted enterprise-wide LCMs for their global operations, but local sensibilities and resistance can lead to situations where business units balk at identifying their exposures. Even within the overall compliance organization there can be confusion or disagreement over how to approach risk. Failure to maintain a consistent enterprise-wide approach can raise questions about whether material risk is effectively identified and mitigated, particularly in non-Canadian businesses.

Because the LCM is an OSFI requirement, its attitude toward risk management can dominate a company. Questionable local market conduct activity may hit the radar only if it is *financially material* to the overall organization, whereas market conduct regulators focus on risk to consumers. A global operation may also struggle to properly identify and measure risks outside of Canada, because of obstructed lines of sight and limited understanding of the terrain.

Size Matters

Even within Canada, a "small" business within a large company could dominate its market by engaging in sub-optimal market conduct activities whereas the same activity pursued by a smaller competitor could set off alarms because the risk would be material. At least theoretically this represents an uneven playing field that could contribute to smaller organizations' solvency concerns — the very thing that OSFI is charged with guarding against.

OSFI offers guidance on “unmeasurable” non-financial risks such as reputation risk, but LCMs tend to deploy quantitative measurements for all risks, including regulatory risks. Market conduct regulation aimed at consumer protection, however, calls for more qualitative standards. Failure to embed meaningful qualitative elements into regulatory risk management can foster a dismissive attitude toward “soft” unquantifiable risks or things that don’t hit the financial materiality threshold.

Statistically small market conduct issues that might carry a mother lode of risk may be underappreciated when quantitative measures dominate. For example, a company with millions of customers could reason that a systems glitch that results in small underpayments to a few thousand customers is inconsequential because only a tiny fraction of the customer base is affected — a defense not available to a smaller company and one that would convince neither a market conduct regulator nor the public if the problem became known. Witness Toyota’s current troubles over what it deemed to be statistically insignificant problems.

Companies that treat regulatory risk as just one more risk to consider and that do not include substantial qualitative requirements for managing regulatory risk in their incentives for all levels of management can hamper the effectiveness of their compliance programs.

What Happens to Rules?

Insurers still have to identify, track, and obey laws that don’t make it onto their current risk maps. Aside from any risk of regulatory fallout, failure to obey rules can erode a company’s culture. Appearing to cherry pick only the rules that “matter” may empower some employees to take on risks without having the authority to do so, or without an understanding of those risks, while demoralizing others. Compliance officers are challenged to push the compliance agenda, which includes inconvenient rules, without being viewed as irrelevant or “in the weeds” themselves.

Concentrating on risk alone can also obscure the importance and gravity of corporate values such as doing the right thing for its own sake. Senior management has to be clear and persistent in its message and demonstration of those values to ensure that they are embraced at all levels and locations — and incentives and disincentives for all need to be aligned with those values.

What Might Happen in Other Jurisdictions?

Risk-based regulation invites a level of dialogue and consultation among regulators and the regulated that is virtually unknown in rules-dominated environments. The

desired outcome — avoidance or mitigation of risk — requires rigorous ongoing self-identification and repair of problems, sometimes with regulators’ input. Anything that causes an excessive concern about exposure of problems, even if ill-founded, can defeat a risk-based approach.

Where enforcement is a primary regulatory activity, enforcement itself can become the risk that needs to be mitigated, and the desired outcome — who or what needs to be protected from what — may be lost in translation. If there is any mismatch between stated outcomes (i.e., consumer protection) and regulatory activity (heavy-handed enforcement of rules that provide little consumer protection), compliance departments must and will try to mitigate enforcement risk. Regulatory agencies that rely on enforcement for operating revenue could find it difficult to achieve effective risk-based outcomes. Finally, litigious environments or corporate cultures dominated by fear of exposure can hamper acceptance of any program that calls for open identification of issues.

Canadian regulators generally enjoy long tenure in their roles because they are somewhat removed from the political process, which enables them to develop strategic plans separately and in cooperation with other regulators. In jurisdictions where regulators are at the mercy of the political process and have short tenure, such cooperation and long-term planning could be impossible to achieve.

A compelling argument for risk-based regulation and a key reason why Canadian stakeholders embrace it is that it allows for the cost-effective targeting of finite resources to the areas of greatest perceived danger. Dedication to harmonizing and streamlining the regulatory environment is driven in part by this motive. Once again, size matters. What a relatively small group of Canadian regulators can achieve is not easily replicated in fractious or fractured environments where numerous regulators claim the same turf or are unwilling or unable to collaborate.

Despite the challenges, risk-based regulation has gained a global foothold because it allows for flexibility in the face of risk and may produce cheaper yet more effective regulation than traditional, local, rules-driven regimes. More important, perhaps, is the growing belief that a risk-management approach transcends parochial limits and provides the principles, framework, and vocabulary for collaborative and harmonized endeavors.

By Chris Nicoll, president of Chris Nicoll and Associates Ltd., a regulatory compliance consulting firm based in Toronto and the former CCO of John Hancock’s life insurance business.

The Spirit of the Times: A Global View of Regulation

What if compliance professionals had a way to chart the future of regulation? How might such information change strategy conversations with CEOs and boards of directors? Would that knowledge impact the way compliance professionals guide marketing and distribution efforts? Charting the possible future of domestic regulation is merely a matter of raising personal and institutional awareness of international organizations that discuss financial matters and issue guiding principles to which participating countries are expected to adhere. This article will provide an introduction to the current global regulatory conversation, and describe how the United States is already involved in that conversation.

There is strong evidence that future regulation will arise not only out of the domestic experience of the recent “Great Recession” but also out of a coordinated global response. Ultimately, this should not be a surprise given the increasingly global nature of economies, corporations, and the apparent international mobility of labor and money. By focusing on two organizations, the G-20 and the International Association of Insurance Supervisors (IAIS), this article will show that the regulatory zeitgeist of the United States is not a national phenomenon but is international and cooperative in nature; and, that regulatory trends may be knowable before specific legislation or regulation is in fact written.

G-20

Who or what is the G-20, and how will the G-20 impact financial services regulation? The “Group of 20” or “G-20” is an organization of the world’s industrial and emerging economies.¹³ The G-20 was founded in 1999 and is essentially a successor to the G-7.¹⁴ The “mandate” of the G-20 is as follows:

The G-20 is the premier forum for our international economic development that promotes open and constructive discussion between industrial and emerging-market countries on key issues related to global economic stability. By contributing to the strengthening of the international financial architecture and providing opportunities for dialogue on national policies, international co-operation, and international financial institutions, the G-20 helps to support growth and development across the globe.

A quick electronic search of *Financial Regulatory Reform — A New Foundation: Rebuilding Financial Supervision and Regulation (Financial Regulatory Reform)* reveals that the G-20 is referenced 43 times in the 88-page document. In fact, it is clear from the document that the United States is convinced of the necessity of raising financial industry oversight standards not only in the United States, but globally. The introduction to *Financial Regulatory Reform* includes five key objectives. The fifth is:

(5) Raise international regulatory standards and improve international cooperation. The challenges we face are not just American challenges, they are global challenges. So, as we work to set high regulatory standards here in the United States, we must ask the world to do the same. We propose:

International reforms to support our efforts at home, including strengthening the capital framework; improving oversight of global financial markets; coordinating supervision of internationally active firms; and enhancing crisis management tools.¹⁵

Financial Regulatory Reform goes on to reference an eight-point declaration¹⁶ issued after the G-20 Summit of April 2009, held in London, England.¹⁷ The overall direction points to a strengthening of regulation globally and in the United States, based on international standards that the United States helps create. At the macro-level the G-20 provides an overview of the direction of the regulation of financial markets and instruments. The G-20 does not however provide a clear picture of how financial regulation in the United States might change. An examination of other international regulatory organizations can be illustrative.

IAIS

Financial Regulatory Reform includes a proposal for an “Office of National Insurance” within the Treasury Department. What final form and name such a body might take on is subject to debate and conjecture. However, it is clear that a centralized insurance regulatory body is within the ultimate scope of regulatory reform:

H. Enhance Oversight of the Insurance Sector

Our legislation will propose the establishment of the Office of National Insurance within Treasury to gather information, develop expertise, negotiate international agreements, and coordinate policy in the insurance sector. Treasury will support proposals to modernize and improve our system of insurance regulation in accordance with six principles outlined in the body of the report.¹⁸

A review of the membership of the IAIS is instructive. The membership is comprised of over 100 countries, organizations like the World Bank, the Organisation for Economic Co-operation and Development, plus the “NAIC and 56 jurisdictions in USA.”¹⁹ The insurance regulatory structure of the United States is an obvious outlier in the global insurance regulatory community. Does this mean that the United States can automatically expect a federal-level super regulator for insurance? No. But consider the fifth objective of *Financial Regulatory Reform* (see above), including the coordination of supervision of internationally active firms.

Will international pressures help move the United States toward a national-level insurance regulator? The IAIS has published a paper titled *A New Framework for Insurance Supervision: Towards a Common Structure and Common Standards for the Assessment of Insurer Solvency*.²⁰ That paper allows, on one hand, for a national supervisory structure that consists of multiple jurisdictions such as that of the United States. However, the paper also refers to the goals of the IAIS which include cooperation “...to ensure improved supervision of the insurance industry on a domestic as well as on an international level in order to maintain efficient, fair, safe and stable insurance markets for the benefit and protection of policyholders.”²¹ The apparent bias, especially considering the position taken in Financial Regulatory Reform to cooperate on an international level, is toward national-level regulation of insurance markets within the United States.

The creation of a national-level insurance regulator is by no means assured, and this article does not attempt to address the merits of such a system. We can, however, draw these conclusions:

1. The United States is an active participant in the global regulatory conversation.
2. The United States government has expressed an interest in cooperating with the international community in matters of regulation.
3. International standards do inform, and are found within plans for regulatory reform issued by The Department of the Treasury of the United States.

National-level regulation of insurance markets in the United States may not ultimately come to pass. Looking at the regulatory structures of other countries, it is understandable how the concept for an Office of National Insurance was introduced into the plans for financial regulatory reform in the United States. By following the international regulatory conversation, the financial services industry does indeed have a means of charting the possibilities for future regulatory change.

By Stephen Selby, Director of Regulatory Services, LIMRA. Please contact Stephen if you have any questions about this article at 860-285-7858 or sselby@limra.com. Connect with Stephen at <http://www.linkedin.com/in/stephenselby>.

¹³The group includes: Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Mexico, Russia, Saudi Arabia, South Africa, Republic of Korea, Turkey, United Kingdom, and United States. The 20th member is the European Union. http://www.g20.org/about/what_is_g20.aspx

¹⁴The G-7 consisted of: Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States.

¹⁵Financial Regulatory Reform — A New Foundation: Rebuilding Financial Supervision and Regulation; page 4, http://www.financialstability.gov/docs/regs/FinalReport_web.pdf

¹⁶http://www.g20.org/Documents/2009_communique_horsham_uk.pdf

¹⁷http://www.g20.org/Documents/Fin_Deps_Fin_Reg_Annex_020409_1615_final.pdf

¹⁸http://www.financialstability.gov/docs/regs/FinalReport_web.pdf, page 13.

¹⁹<http://www.iaisweb.org/index.cfm?pageID=31>

²⁰http://www.iaisweb.org/temp/Framework_fir_insurance_supervision.pdf

²¹Ibid page 3.