LIMRA Regulatory Review

ADVANTAGE IN A REGULATORY WORLD

Broker-Dealer
Investment Adviser
Insurance
Research

300 Day Hill Road • Windsor, CT 06095 • www.limra.com/compliance • Issue 2011-1 • Bimonthly

February 2011

IN THIS ISSUE

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.

LIMRA

United States

The Privacy Challenges of Technology

Collecting personal information is nothing new in the financial services industry. For decades financial professionals collected information in order to determine a client's financial needs. Years ago they collected information over the phone, or on paper forms transported in briefcases. This meant limited exposure, which still a concern, but one that comes nowhere near today's issues. In addition, without email everything was typed, copied, and sent hardcopy to clients and other advisors.

Fast forward to today, and these functions happen via email and the Internet. You can easily attach and email a file of client information. And that is just basic technology — we have barely scratched the surface when it comes to social media, or the ability to transport millions of pieces of personal data via a flash drive.

So, how do we as compliance professionals deal with all of the potential challenges introduced by these technologies?

Email

Continued education and constant reminders about how to use email can't happen often enough. Email continues to be the easiest way for regulators and lawyers to find a "smoking gun" from a legal perspective. Accidental emails go out with information that should never have been sent over the Internet. Someday, someone may invent a program that will, just like spell check, go through an email and check for personal information. It will "read" the email and warn — "Do you really want to send this email?" — thus preventing a potential email liability. Until this dream comes true, however, we will have to make due with email review programs to catch these problems. You may want to review your lexicon lists and add privacy words to help identify potential emails that may have used personal information.

Another suggestion I have is to work closely with the company that hosts your emails. It can be a valuable source of information, especially when you start using multiple devices to access your emails. By now, you're beginning to ask if you've done everything possible to protect yourself. A quality company understands these types of privacy issues, and constantly tries to make sure that their systems are state-of-the-art. While we all tend to focus on emails for the financial professionals

LIMRA SPOTLIGHT

CONFERENCE

➤ Regulatory Compliance Exchange

March 30 – April 1, 2011
Created by compliance professionals for compliance professionals, this conference features sessions on a broad range of timely topics. To learn more and register, please visit us online.

NOTABLE

➤ **Cost-effectively meet the NAIC's Suitability in Annuity Transactions Model Regulation.**
LIMRA's new **AnnuityXT** training program and Compliance Suitability Survey can help you to: (1) ensure that producers complete basic suitability and product-specific annuity training before recommending an annuity product; (2) monitor sales; and (3) share findings with distribution partners. For more information or to see a demo of the new AnnuityXT training system, please contact Meggan Tufveson at 860-285-7859 or usclientservices@limra.com.

➤ **Help producers compliantly leverage social media.**
LIMRA and Socialware have teamed to create **Insights: Advisor Series,** an always-current curriculum that helps producers grow sales — and protects your firm. Courses already available include *Social Media 101, Compliance Basics, LinkedIn, Twitter, and Facebook*. For more information, please contact Meggan Tufveson at 860-285-7859 or usclientservices@limra.com.

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

Follow LIMRA Compliance and Regulatory Services on Twitter at http://twitter.com/limra_crs.

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
Web site: www.limra.com/compliance

in the field, we also need to pay attention to anyone in the home office who deals with personal data. For instance, IT areas tend to work with data that contains personal information so we must ensure that this information remains protected. Compliance areas deal with regulators and respond to regulatory inquiries that sometimes include personal client information. FINRA recently published Regulatory Notice 10-59 in which they announced that the SEC approved encryption procedures as part of FINRA Rule 8210. (For additional information please see the article titled "Encryption and Other Secret Messages (Hw wx, Euxwh?)" in this issue.)

Laptops and Personal Computers

Anyone who uses a laptop or PC for business needs to use encryption and passwords as part of their normal everyday habits. No one wants to notify clients that their personal information may have been stolen because of a missing password or encryption code. Firms should put encryption and password procedures in place to protect not only the company, but also its clients. If firms research the companies that provide these encryption services and then set up a process for the remote users in agencies to utilize these companies — this will go a long way toward getting field personnel to encrypt their laptops and PCs. The next step would be to ensure that any mobile devices that are linked to the company email system are also encrypted, as there are ways to push out the encryption to these devices used by the financial professionals.

Once companies have implemented these processes, they need to implement supervisory procedures to make sure that the computers remain encrypted and that their new representatives get their equipment encrypted. These procedures should be included in a firm's on-boarding process for any new representative: providing privacy and AML training, setting up an email account, and confirming that business computers and mobile devices are encrypted. In addition, these processes should be part of the annual certification process.

And, don't forget to encrypt the administrative assistants' computers, and the agency servers.

Firms are now at the point where they either need an individual in the firm with IT expertise or they need a local company that can provide IT services to the firm in order to advise them on these issues. Another concern is throwing out old equipment. While it is great to donate old equipment, you need to make sure that you first properly dispose of all information on the PCs or laptops. There are services that will remove and properly dispose of all the data on the computers.

Future Technology

One thing I think we can all agree on is that technology will continue to develop, and we must find ways to deal with each development if we are to remain competitive. How can we do this? First, become very close to your IT associates and continually work with them to identify areas to protect as the technology develops.

Second, any company needs an overall plan for how to protect personal information in any business line. The FTC has a great video on their website that includes a five-point plan for protecting personal information:

1. Take stock of who accesses the personal information, what personal information you collect, how you collect the information, and where you store the information.
2. Scale down the information you collect to only the information you really need to do your job.
3. Lock it — Make sure the information you have (whether paper or electronic) is locked up when not in use.
4. Pitch it — Make sure you make it as easy as possible for associates to properly dispose of any personal information that is no longer needed, such as via shredders.
5. Plan ahead — As you start new lines of business and provide new tools that will need personal information, make sure you only collect what is needed, and have a record retention policy for destroying the information when it is no longer needed.

As an industry, we will always use personal information, and technology will continue to play a large part in our business practices. People today want easy access to their accounts and don't want to deal with paper, so we need a process for using technology effectively and efficiently while always making every possible effort to protect the personal information we collect.

By Thomas J. Horack, Chief Compliance Officer, John Hancock Financial Network. He will present at LIMRA's and LOMA's upcoming Regulatory Compliance Exchange.

Everything Old Is New Again…

The insurance industry takes great pride in the way its products facilitate all aspects of international commerce. In addition, insurers are used to dealing with regulations intended to strengthen the industry by improving business practices. U.S. insurance carriers, responding to the needs of foreign clients, routinely offer international insurance to their domestic clients. U.S. insurers form alliances with foreign companies to gain footholds in countries where client bases are rapidly expanding. U.S. underwriters dramatically increase their involvement in lucrative international reinsurance markets. Everywhere you turn traditional barriers — as well as protections — continue to fall, as the world we know becomes increasingly smaller.

However, it is precisely this global role that continues to draw ongoing industry scrutiny under the trade sanction programs administered by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC).

But OFAC compliance is not a new issue — it has roots that extend for decades. And as part of its ongoing efforts, the OFAC has long sought enlistment from the insurance industry (among other financial services members) in defense "against foreign threats to our national safety, economy, and security" by making insurers responsible on a strict liability basis — not only for their own trading practices, but for those of customers who violate the sanction and embargo rules. Importantly, the relevant rules apply to any "U.S. person" who participates in a proscribed transaction. This means that insurers, vendors, shippers, and purchasers all face risks when it comes to compliance with the OFAC's various regulations.

U.S. sanctions go well beyond the borders of target countries. The OFAC identifies and names numerous foreign agents and front organizations, as well as terrorists, terrorist organizations, and narcotics traffickers, as "Specially Designated Nationals and Blocked Persons," with a master list containing well over 7,000 variations of individual names, governmental entities, companies, and merchant vessels located around the world.

To assure that illicit transactions involving target countries and Specially Designated Nationals (SDNs) are not processed, fund transfer departments in most U.S. financial institutions — as well as major corporations which are not banks — have turned to sophisticated "interdict" software to automatically flag questionable

transactions for review. While some of the filters contain every name on the OFAC's list, along with geographical names for embargoed countries and cities, others actually contain even more information about entities associated with named entities on the SDN list.

Penalties

Penalties for failure to properly know whether your customers or their transactions violate OFAC sanctions continue to occur with what seems to be 'eye-popping regularity.' In 2010, penalties for OFAC-related infractions exceeded $200M. In addition, Barclays plc was assessed a $298M penalty in 2010 from the U.S. Department of Justice and the New York District Attorney's Office for altering (stripping) wire transfer messages of references to OFAC-prohibited or blocked entities. Also in 2010 other penalties for OFAC violations included a $15M penalty against an aviation firm for selling airplanes to a sanctioned country, and a $3M penalty against a global shipping line related to 4,700+ unlicensed shipments originating in or bound for Sudan and Iran.

While it is true that, historically, a majority of penalties for OFAC violations have been levied against financial institutions, insurers and reinsurers are by no means off the hook when it comes to their need for effective OFAC compliance programs and the high risks associated with failure to comply. Both Aetna and CNA have previously incurred OFAC penalties, the latter paying a fine of $2.4 million following an investigation that reportedly cost the company an even greater amount in legal expenses.

In 2010 an insurance company provided automobile insurance without an OFAC license to a person listed as a Specially Designated Narcotics Trafficker Kingpin (SDNTK). The insurance company's OFAC compliance program was designed to check only the names of their policyholders against applicable watch lists on an annual basis. OFAC calculated the base settlement at $11,000 and levied the total amount against the company because of that gap in their program.

This last example brings to light several problems, one of which is that the OFAC SDN list experienced 55 changes to entities in calendar year 2010 alone. With this level of activity, it is virtually impossible to comply by only performing a periodic screening of customer names on an annual, quarterly, or even monthly basis. And let's not forget the numerous other business processes and areas where screening should also occur.

When acquiring a business or merging with another organization, it's important to complete proper and thorough due diligence on their compliance processes as part of your overall due diligence effort. This should include a thorough review of the acquired party's OFAC compliance program, processes, and procedures. Not doing this could mean OFAC penalties such as those incurred by two entities in 2010 that were fined based on business dealings that took place prior to their acquisition of other companies. One, an international hotel chain that took over a smaller hotel brand, found that their predecessor was operating hotels in Sudan without the proper OFAC license. As a result, they were penalized $735,407. Another, an oil refiner, gained and continued to maintain local sales offices in Cuba through the acquisition of a foreign corporation, thus violating Cuban sanctions, resulting in a $2.2M penalty assessment by OFAC.

Making Sure Your OFAC Compliance Program Is up to Speed

If you have not yet designated a specific person as your OFAC Compliance Officer, you should do so. In selecting a person for this role, you will want to consider their knowledge and understanding of OFAC-related issues as well as how such issues impact and relate to your business, products, and customers. You should have proper documentation of OFAC compliance policies and procedures that relate to various facets of your OFAC compliance program. Say what you are going to do and then actually do what you said you would do.

If you have not done so (or not done so lately), perform a thorough, independent risk assessment and review of your OFAC compliance program. Such independent review should include assessment of clients, vendors, and any third-party providers that you are involved with, as well as review of payments and disbursements, on-boarding of new clients and agents, and should assess risk of all products provided (and not just those products listed as 'covered products' under your AML program).

This review should identify any risks found and what steps you can and should take to mitigate any risks identified. This risk assessment should include review not only of processes concerning new and existing clients/policyholders but also of claims processes, vendor relations and vendor payments, customer service, and IT areas. The review should also cover record-keeping and compliance documentation.

Finally, ongoing training on OFAC compliance issues and how these relate to your company, your clients, and products will help to ensure that your program stays fresh, viable, and operates at a highly efficient level.

Summary

Make sure to possess a solid understanding of OFAC regulations and the reporting requirements associated with proper OFAC compliance. This will not only impact your present business but also should apply to any pending plans involving acquisition of another firm or another block of business, or introduction of products to new markets. According to Erich Ferrari, an attorney specializing in OFAC litigation, and author of the blog Sanction Law that follows OFAC sanctions, "the U.S. Department of the Treasury Office of Foreign Assets Control is upping the ante when it comes to the dollar amounts of the fines they issue" (see http://sanctionlaw.com/2010/02/09/ofac-hits-balli-group-plc-and-balli-aviation-with-a-massive-penalty/). The blog also warns those who typically and incorrectly believe they are immune to compliance obligations that, "while OFAC has been moving towards issuing huge penalties against corporate entities, that does not mean that individuals or small companies are off the hook."

The bottom line is that being penny-wise and pound-foolish in your OFAC compliance processes can lead not only to significant penalties for inadequate compliance, but also to substantial reputational harm.

By Shaun M. Hassett, CAMS, LIMRA Regulatory Consultant.

Encryption and Other Secret Messages (Hw wx, Euxwh?)

FINRA, the State of Massachusetts, and the State of Nevada have rules that may require your firm to use encryption.

Encryption has been used for thousands of years. Julius Caesar used a simple alphabet substitution to encrypt letters sent to his friends. Every letter of the message was shifted up by three; A became D, B became E, etc. Shifting by three letters changes Caesar's famous quote (from Shakespeare), "Et tu, Brute?" into "Hw wx, Euxwh?" Another example of encryption comes from the classic movie *A Christmas Story* — when Ralphie writes down a secret radio message and then decodes it with his "Little Orphan Annie Decoder Ring." These methods of encryption are primitive by today's standards of codes based on complex algorithms, but the concept is the same. Information is encrypted, transmitted, and then decoded. FINRA defines "encryption" as "the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key." The process for decoding a message from Julius Caesar is to shift every letter by three, and the Decoder Ring is the key that Ralphie uses to decipher the radio message. Without a process or key, the message is unreadable.

The FINRA requirement for encryption is found in Rule 8210(g) which became effective on December 29, 2010. Rule 8210 requires members to provide information or testimony to FINRA for an "investigation, complaint, examination, or proceeding authorized by the FINRA By-Laws or rules…" Section (g) of that rule applies to information that is sent to FINRA in response to a request under the rule. Information that is sent on a portable media device such as a "flash drive, CD-ROM, DVD, portable hard drive, laptop computer, disc, diskette, or any other portable device for storing and transporting electronic information" must be encrypted. The process or key to unlock the data must also be sent to FINRA but in a separate communication.

Rule 8210 applies to all information sent, regardless of the content. The letter from Stan Macel, Assistant General Counsel for FINRA to the SEC, dated September 14, 2010 (SR-FINRA-2010-021) states that "FINRA believes that the costs of determining and monitoring whether information included on the portable media devices contains the type of information that needs to be encrypted would be much greater than the costs of simply encrypting all such information submitted…" Also, the FINRA rule does not appear to apply to emails, as the same letter states that in the future "…FINRA will explore whether to require encryption of other methods of communication that may contain personal data, such as email." The method of encryption is not specified in the FINRA rule or in either of the state's rules other than it must meet industry standards for strong encryption. Neither the "shift by three" nor the "Decoder Ring" would be acceptable, as the standard is currently viewed by FINRA to be 256-bit or higher encryption. The wording for the encryption standard was designed to allow the rule to remain effective even as technology changes.

The state regulations apply to the transmission and storage of a resident's personal information. Massachusetts defines personal information (PI) as a Massachusetts resident's "first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account…". The definition of personal information for Nevada is similar but not identical.

The state rules are very broad; if you have a customer in either state, the rule probably applies. The Massachusetts rule applies to "those engaged in commerce" and the Nevada rule applies to any "…corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose… handles, collects, disseminates or otherwise deals with nonpublic personal information."

Both states require encryption if a resident's personal information is transmitted electronically across public networks. For Nevada there are no exceptions. Emails need to be encrypted if they contain personal information as defined by their Rule NRS 603A.040. The Massachusetts rule limits this requirement to "records and files" unless the personal information is transmitted wirelessly. Massachusetts does expect emails containing personal information to be encrypted if technically feasible. Storage devices containing personal information are required to be encrypted in Nevada if they are moved beyond the physical controls of the company. However, Massachusetts requires all personal information to be encrypted when stored on laptops or other portable devices, including backup tapes if technically feasible.

In addition to encryption, the Massachusetts rule requires firms to have a written information security program that includes: one or more employees designated to maintain the program; the use of updated fire walls, security patches, and antivirus software; malware protection; education and training for employees including temporary and contract employees; password protection measures; monitoring systems; contracts with third-party service providers to include appropriate security measures; an annual review; and other requirements.

When considering if the above rules apply, it is important to evaluate all potential sources of personal information. For example, the responsible person at a branch office might assume that the rules don't apply to them because they only access customer information through secured websites. But the office computers might contain personal information in the form of customer correspondence, service request forms, or other documents. Branch personnel may also have outside business activities that require the storage and/or transmission of personal information such as tax returns or insurance policy numbers. FINRA's requirements are found in Rule 8210 and Regulatory Notice 10-59; the Massachusetts rule is 201 CMR 17.00, and the Nevada rule is NRS 603A. This article covers some of the requirements of the rules but readers should refer to the actual rules for complete details.

By Victor A. Shier, LIMRA Regulatory Services Consultant

Gifts, Gratuities, and LM-10

This is the time of year during which many compliance professionals review their policies and procedures to gear up for the new year. It is also a good time to review a couple of topics that most of us are familiar with: gifts, gratuities, and business entertainment; as well as a topic some may not be familiar with: LM-10 filings.

Probably the most well-known FINRA rule regarding gifts and gratuities states: "No member or person associated with a member shall directly or indirectly, give or permit to be given anything of value, including gratuities, in excess of one hundred dollars per individual per year to any person, principal, proprietor, employee, agent or representative of another person where such payment or gratuity is in relation to the business of the employer of the recipient of the payment or gratuity. A gift of any kind is considered a gratuity." (See FINRA Rule 3220 at http://finra.complinet.com/en/display/display.html?rbid=2403&element_id=5665.)

One portion of the gifts and gratuities rule that often causes a firm difficulty is the requirement that gifts and gratuities must be aggregated at a firm level. This can be very tricky for firms that have more than one division. The firm must establish a tracking system that all divisions can access, and that enables the firm to track gifts and gratuities given to any individual at the firm. Staff must be trained to check the tracking system to ensure that they do not go over the $100 limit. In addition to staff training, it is extremely important to train the people who approve the expenses. They are a firm's first line of defense — identifying and stopping potential violations. I bring this up because FINRA is still finding gifting violations during examinations of firms that already have tracking systems in place. The violations are often caused by small items such as holiday gift baskets not allocated properly or gifts that are incidental to entertainment. A good compliance practice to test this is to randomly review expense reports after they have been approved to ensure that they have not violated company policies and procedures as well as FINRA guidelines.

One other point to keep in mind: firms must track gifts received to ensure that their registered representatives do not accept gifts and gratuities over $100. While most reps may tell you that this never happens, a firm was cited for this in 2010.

Business entertainment is an area of concern from a business perspective. At this point most staff are familiar with their firms' compliance policies and procedures as well as FINRA rules regarding business entertainment.

The reason that it is a concern is that many firms do not know the policies and procedures of the firms that they do business with. This is a problem because those firms often have policies that state that they will not do business with firms that violate their policies and procedures. In this case, not "knowing your customer" can potentially cost your firm a lucrative business relationship.

Quick Tips

- Check with the compliance/key accounts departments of your affiliates — they are generally more than willing to share their guidelines for gifts, gratuities, and business entertainment.

The Labor-Management Reporting and Disclosure Act of 1959 (LMRDA) provides standards for the reporting and disclosure of certain financial transactions and administrative practices of labor organizations and employers; the protection of union funds and assets; the administration of trusteeships by labor organizations; and the election of officers of labor organizations. The Office of Labor-Management Standards (OLMS) of the U.S. Department of Labor administers and enforces most provisions of the LMRDA (see http://www.dol.gov/compliance/laws/comp-lmrda.htm). One of the requirements of the LMRDA is for firms to file Form LM-10.

During the course of conversations I have learned that many people are not familiar with the Department of Labor's Form LM-10 filing requirements, or that they believe that it is not applicable to them. The LM-10 filing requirement states that employers must file LM-10 annual reports to disclose certain specified financial dealing, subject to a $250 *de minimis* exemption, with a union or office, agent, shop steward, employee, or other representative of a union. The confusion most likely comes from the fact that the LMRDA has a very broad definition of "employer." According to their definition "any employer" could almost be substituted for "employer." In fact, they state that "Except in rare cases, every private sector business or organization within the United States that has one or more employees is considered an employer under this definition, and thus may have reporting obligations under the LMRDA."

So what does this mean for your company? Firms must first determine if they are doing business with or prospecting any unions or "union officials." The filing requirements for this are tricky. All money spent on a union official must be tracked and aggregated over the course of the firm's fiscal year. Unlike FINRA reporting requirements, this includes business entertainment. Everything from a round of golf, a gift, travel expenses, or a business meal must be tracked on an individual basis. Once an individual reaches $250, the firm no longer qualifies for the *de minimis* exception and it must file a Form LM-10 within 90 days after the end of its fiscal year, unless the firm has another reporting exemption.

If a firm determines that it is working with unions and union officials and might be required to file Form LM-10, the company may wish to look into updating their gift and entertainment tracking system to capture this information, as it can be difficult to recreate the information after the fact.

Quick Tips

- Union officials and employees are required to file Form LM-30. Form LM-30 is used to report what union officials and employees have received from firms. Because of this filing requirement it is possible for the OLMS to compare what a firm reports against what the union official reports, to find discrepancies.

For more information about Form LM-10 and your reporting obligations, please visit http://www.dol.gov/olms/regs/compliance/LM10_FAQ.htm.

By Carolyn R. Blake, CFP, LIMRA Audit Services Consultant

Compliance Benchmarking Survey

Regulatory risk is a fact of life in the financial services industry, especially in retail distribution. The way that firms deal with regulatory risk has an impact on many aspects of business, from advisor recruiting to marketing. Compliance departments must balance pressures from regulators to meet certain requirements with the need to work with business units to ensure that supervisory systems are as business-friendly as possible.

LIMRA has initiated a new study that benchmarks U.S. broker-dealer compliance standards. The survey includes both common and uncommon elements of broker-dealer compliance, from outside business activities to MC 400 supervision. Participation is open to LIMRA member firms and non-member firms alike — at no cost.

The goal of the survey is to better understand broker-dealer compliance practices and to provide participating firms with a set of compliance operation benchmarks. The survey has two sections. The first section — comprised of core questions — will help us to identify and track industry trends in compliance. The second section poses topical questions that address current compliance issues.

For example, as new regulations emerge, there may be questions pertaining specifically to the roll out of new compliance policies and integrating the new policies into existing procedures. LIMRA will conduct the survey every six months.

The survey is confidential. LIMRA only publishes aggregate findings and does not disclose individual firm data.

If your firm is interested in participating in the Compliance Benchmarking Survey, please provide your contact information to:

Scott R. Kallenbach, FLMI
Strategic Research, LIMRA
Email: skallenbach@limra.com

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

Disclosure Requirements for Covered Service Providers under ERISA 408(b)(2)

Last July, the Department of Labor (DOL) released its interim final regulation under ERISA Section 408(b)(2). The interim regulation requires specific disclosures that a covered service provider must make to covered retirement plans in order for a contract or arrangement to be in compliance. Covered plans include ERISA governed plans such as 401(k) plans, profit sharing plans, defined benefit plans, and ERISA 403(b) plans, but specifically exclude SEP IRA and SIMPLE IRA programs.

Underscoring the need to consider all the comments received from service providers, the DOL has announced that the effective date for compliance will shift to January 1, 2012 from July 16, 2011. The regulation's core elements are likely to stay in place, with some possible enhancements such as a summary and roadmap of disclosures. This is a welcome opportunity for service providers to resolve many of the implementation problems they were facing with the July 16, 2011 implementation date.

This article provides a basic summary of the regulation and how it applies to broker-dealers (BDs) and registered investment advisers (RIAs). For more detailed information about the regulation, visit www.reish.com/practice_areas/EmpBenefits/Bulletins.

The Problem

The prohibited transaction rules provide that arrangements between covered plans and covered service providers are prohibited unless they are "reasonable." The regulation defines a reasonable arrangement for Section 408(b)(2) purposes as one that complies with the regulation's disclosure conditions. If a service arrangement does not comply with the regulation, the covered service provider (*e.g.*, the BD or RIA) has engaged in a prohibited transaction. The covered service provider will be required to restore any compensation to the plan and to pay excise taxes. This is a "per se" prohibited transaction; it occurs automatically.

(Please note that the regulation does provide relief to covered providers for inadvertent disclosure errors and omissions if corrected information is provided within a prescribed time frame.)

The Regulation

Who Are Covered Service Providers?

Generally speaking, a covered service provider is one that delivers services described in the regulation (see below) and reasonably expects to receive (along with its affiliates and subcontractors) $1,000 or more in direct and indirect compensation.

RIAs are almost certainly covered by the regulation. For example, an RIA is covered when it provides any service directly to a covered plan as an RIA registered under the Investment Advisers Act or any state law, such as an RIA providing non-discretionary investment advice to the fiduciaries of a participant-directed 401(k) plan or an RIA that manages assets for a pooled profit sharing plan. RIAs are also covered if they provide services to an investment contract, product, or entity that is treated as holding "plan assets" under ERISA and in which the covered plan has a direct equity investment. An example of this latter category would be an RIA that manages a collective trust in which a covered plan invests.

BDs are usually covered in one of two categories, each involving non-fiduciary services, where:

1. Brokerage services are provided to a covered plan that is an individual account, participant directed plan (such as a 401(k) plan) and one or more "designated investment alternatives" are offered to participants; or
2. Securities or other investment brokerage services or consulting (relating to the development of investment policies or objectives, or selection and monitoring of investment providers or investments) are provided to a covered plan where the BD receives "indirect compensation," such as 12b-1 fees or insurance commissions.

What Are the Requirements?

Written Disclosure

The disclosures must address three core issues: status, services, and compensation.

The disclosure must be in writing to the responsible plan fiduciaries (e.g., the plan sponsor or a plan committee). Providing written disclosure will not be a difficult task for RIAs that already use a written advisory agreement and deliver Form ADV Part 2 (or an equivalent brochure). The new Form ADV Part 2, as well as annual update or summary of material change filings, provides an opportunity for RIAs to review their disclosure obligations under the Investment Advisers Act of 1940 and ERISA.

BDs have a significant challenge because they have not ordinarily used written service agreements with retirement plans in the past. Further, BDs often have distribution/selling arrangements that involve various forms of revenue sharing (which are considered to be "compensation" under ERISA) and increase the complexity of fee disclosure. In our experience, the website disclosures of these payments are not usually adequate to satisfy these new 408(b)(2) requirements.

The required disclosures about BD services and compensation, and ERISA fiduciary status if applicable, must be made in writing. To comply, BDs should consider using service agreements to satisfy the 408(b)(2) disclosure requirements and to better manage the issues and risks of providing services to retirement plans. Alternatively, BDs may consider using disclosure documents to stand alone, or to complement, other BD documentation to provide disclosures to covered plans. In our experience in representing BDs on these issues, BDs are opting to use disclosure documents for their existing covered plan clients, but will use service agreements for new clients beginning by the new effective date at the latest, if not sooner.

The next question is one of logistics. Both BDs and RIAs have to make a decision about delivery of disclosure information via electronic means versus traditional mail. Both have to consider how to reach all of their existing covered plan clients before the new effective date in the most efficient manner; disclosure documents and agreements must be drafted; compliance manuals and supervisory procedures, along with internal training, must be developed and implemented.

Service Disclosure

Services must be described with sufficient detail so that the plan fiduciary can make an informed decision about hiring the RIA or BD.

RIAs undoubtedly describe their services in the Form ADV Part 2a and their advisory agreement; those documents should be reviewed in light of the new requirements. Insofar as RIAs are currently rewriting the new Form ADV Part 2a, this is an opportunity to integrate the 408(b)(2) disclosure requirements.

BDs have a larger issue in describing services. Many BDs and their representatives provide covered plans with services beyond brokerage services, such as participant enrollment and education support, serving as the contact person among plan service providers, and providing investment information to plan sponsors. The important services to be provided to plans by the BD must be described.

Compensation Disclosure

The biggest challenge may be compensation disclosure and, particularly, the indirect compensation in revenue sharing arrangements. "Direct compensation" is defined as compensation that a covered service provider, and affiliates or subcontractors, expect to receive directly from the plan. "Indirect compensation" includes that which the covered service provider, and affiliates or subcontractors, expect to receive from anyone other than directly from the plan or the plan sponsor.

Additional rules apply to "compensation paid among related parties" and "termination compensation". Compensation paid among related parties must be disclosed if it is set on a transaction basis or charged directly against the plan's investment. This would require disclosures in many cases of amounts paid to registered representatives or IARs who are independent contractors.

RIAs typically disclose direct compensation and the offset of indirect compensation received. However, for indirect compensation, the payor of indirect payments and the method of payment (that is, whether the plan is billed or fees are deducted directly from plan accounts) are areas that often need more attention by RIAs.

BDs must disclose direct and indirect compensation, as well as compensation paid among the parties. BDs who receive indirect compensation, such as 12b-1 fees or insurance commissions, must disclose the amount (or the formula for calculating the amount, e.g., a percentage) and the payer of the fee. Many revenue sharing arrangements must also be disclosed.

Final Thoughts

BDs and RIAs must determine if they provide services that are covered by the regulation — and they usually will be. If so, disclosure documents must be distributed to existing clients on or before the new effective date and, beginning on the new effective date, newly acquired clients must be given the disclosures (typically in a service agreement and related documents) reasonably in advance of entering into the arrangement to provide consulting or brokerage services. The disclosures must address the status of the provider, the services, and the direct and indirect compensation. Successful implementation also involves advance planning: the logistics of timely delivery must be addressed, internal programs for tracking and accounting revenue sharing must be developed, and internal training and compliance policies must be modified for the new disclosure regime.

Fred Reish (Managing Partner and Director) and Stephen Wilkes (Of Counsel) are with the law firm of Reish & Reicher. Mr. Reish may be contacted at fredreish@reish.com. Mr. Wilkes may be contacted at stephenwilkes@reish.com.

008124-0211 (622-7E-A-CT7)

