HOW TO MANAGE SECURITIES COMPLIANCE

BY STEVE MACKES

SO MANY REGULATIONS, SO LITTLE CLARITY

Information compliance requirements are on the rise, with penalties, fines, sanctions, and even imprisonment the powerful punishments awaiting any securities firm that fails to meet Federal and State mandates. But with rules that are sometimes subject to interpretation, it's not always clear how to comply. Worse still, many securities brokers, commodities brokers and investment service firms are simply unaware of the specific regulations they need to follow and therefore, totally unprepared to navigate a regulatory audit or investigation.

To set the record (and your records) straight, this paper addresses key regulations that impact the securities segment of financial services and provides guidance on how you can cost-effectively stay compliant.

SEC 17A AND OTHER RULES THAT CAN COST YOU

SEC Rule 17a – 4 has been around since the 1930's. It requires Security and Exchange Commission members to archive all customer communications and billing information for 6 years. In 1997, the rule was amended to require brokers and dealers to maintain records electronically with a designated 3rd party service provider (aka D3P) for possible SEC review. This amendment was largely ignored until FINRA (Financial Institution Regulatory Authority) began to demand proof of compliance. Financial firms, caught off guard by this added risk exposure, scurried to oblige.

According to the rule only those communications that relate to the broker's or dealer's business need to be retained. Relevant information includes securities sales records, ledgers reflecting assets and liabilities, securities borrowed or loaned, dividends and interest received. Retention schedules and document management requirements are also part of the regulation. Originals of all business communications and copies, whether by paper, by email or through audit reporting, must be indexed, easily searchable and stored on unalterable media. Additionally, securities companies are required to ensure the accessibility, security and integrity of their records. Communications unrelated to the business are outside of these requirements and allowed to be deleted/destroyed at will.

Still, with Rule 17a-4 and other regulations, the line between what should be retained and what is eligible for destruction sometimes gets blurred. There have been instances where information that

could be construed as internal and not direct customer communications was determined to be valuable, critical evidence and needing to be saved. This occurred in 2003 with the Mutual Fund Late Trading investigation that sought information related to a firm or its employees permitting, assisting or facilitating late trading.

Consequently, it may be best to err on the side of safety and save all communications when there is doubt, so that a re-interpretation on the part of the SEC or some other regulatory board can't come back to bite you.

Similarly NASD Rule 3010 pertaining to Supervision and Rule 3110 concerning Books and Records demand that members keep all communications with the public. The objective of these rules is to help ensure that National Association of Securities Dealers, Inc. members are not engaged in manipulation or criminal intent. Amendments to these rules in 1997, designed to further protect the rights of customers, allow firms to develop flexible supervisory procedures for the review of correspondence with the public.

Another regulation aimed at safeguarding customer data is the Gramm-Leach-Bliley Act, which requires banks and financial institutions to implement comprehensive written information security policies. With steep fines and up to 5 years of prison for non-compliance, Gramm- Leach-Bliley requires a financial institution to protect non-public personal information from being distributed outside the organization.

Addressing corporate accountability, the Sarbanes-Oxley Act of 2002 requires all publicly held companies to establish and maintain internal controls over their financial reporting systems and ensure their effectiveness. Sarbanes-Oxley holds upper management personally responsible for compliance, so it's wise to retain documents and emails according to the law's specified periods. Depending on the type of information, those time periods range from 3 years to permanent. Failing to comply with Sarbanes-Oxley can result in fines that are as much as 5 million dollars and prison terms up to 20 years.

Additionally, certain states have enacted privacy and security laws in regard to customer financial information that further complicate the securities compliance picture. For instance, the California Privacy Law mandates the same requirements as Gramm-Leach-Bliley, with the addition of allowing "injured" customers to take civil action.

This much is certain: the recent penalties alone for failing to meet Rule 17a-4 and other information-related regulation requirements have cost security-trading firms millions of dollars.

A GOOD D3P IS WHAT YOU NEED

Contracting with a designated 3rd party services provider (D3P), as required by Rule 17a-4, is the best way to meet all Federal and State securities information compliance issues. A D3P such as GRM

brings comprehensive information management capabilities and a wealth of securities compliance expertise to the table. It's a potent and effective combination designed to remove the weight and uncertainty of regulatory compliance from your shoulders. A D3P works to your advantage through the implementation of securities compliance best practices and allowing your firm to better focus on core activities such as introducing new products and building/serving your client base. With compliance mandates cost-effectively identified, interpreted and met, stress, worry and risk are substantially reduced for your firm and its security officers.

A D3P is able to evaluate your firm's current information management systems, including storage, hardware, software programs, retention schedules, security measures and more. It can assess your information content as well, identifying redundant and unnecessary documents that can be eliminated to reduce your information volume to save on costs and to streamline operations, making searches easier. If there are gaps in systems, protocol or even content, the D3P can help you fill those gaps and get your information and the management of it in shape to satisfy the most demanding audits.

GRM, as one of the few D3P organizations that successfully handles both paper and digital information inventories, provides bridge services between the two environments as needed. The company works in partnership with clients to determine the best, most cost-effective ways to move, preserve and destroy (when appropriate) sensitive information offsite. Whether paper or digital, every information item is securely stored and continuously tracked through barcode labeling. Complete chain-of-custody records are maintained on data and digital documents through a single, shared repository called the Online Record Center. This Cloud-supported, SaaS (Software as a Service) system provides flexible, on-demand EDM workflow automation features as well as compliance functionality. Key Online Record Center advantages include low- cost implementation, quick deployment and rapid Return on Investment. Another outstanding GRM feature is eAccess, a remote inventory control interface. Free for any GRM customer, eAccess allows you to search and manage paper or digital inventories around the clock from any web-linked computer.

CONCLUSION

When it comes to securities information compliance, the risks to your business, reputation and personal freedom are far too great to take chances. Ignorance or half-hearted efforts are never an acceptable defense, and the punitive measures for failing to comply are steep. Enlisting the expert capabilities of a D3P services provider, however, cost-effectively delivers the information security, privacy and best practices you need to reduce risk and stay clear of regulatory trouble. And the benefits don't stop there. Many compliance-enhancing services also improve productivity and customer satisfaction.

MORE ABOUT GRM

GRM Document Management is a leading provider of lifecycle records and information management solutions. The company brings proprietary innovation, blended integration and new levels of cost

efficiency to document storage, data protection, digital/electronic document management and certified destruction. With over 25 years of experience, GRM has earned the trust and continued business of more than 5,000 customers—large and small, domestic and multinational—representing a wide range of industries. Clients are served from state-of-the-art, climate-controlled facilities in major U.S. markets and internationally throughout China.