MAYER·BROWN

ELECTRONIC DISCOVERY & INFORMATION GOVERNANCE

Tip of the Month

Enforcement Actions and the Use of Data Analytics

Scenario

The US Securities and Exchange Commission (SEC) is investigating a global investment bank for alleged compliance violations. Although the bank has experience with responding to regulators, this particular SEC request is more targeted than those the bank has received in the past, demanding specific electronic communications from management, traders and sales staff. The bank's legal and compliance departments are concerned about recent announcements about the SEC's new investigative approaches and use of innovative data analytics, and the bank wants to evaluate its overall readiness in light of these recent regulatory announcements.

Agency Enforcement Initiatives

The SEC filed 755 enforcement actions in the fiscal year that ended in September 2014. These covered a wide range of misconduct and resulted in $4.16 billion in disgorgement and penalties based on preliminary figures. Comparatively, in FY 2013, the SEC filed 686 enforcement actions resulting in $3.4 billion and in FY 2012 filed 734 enforcement actions resulting in $3.1 billion in disgorgement and penalties. The SEC recently announced that it believes its use of data and analytical tools contributed to its strong enforcement results and helped detect misconduct and other potentially violative activities that otherwise may have gone unnoticed.

The Financial Industry Regulatory Authority (FINRA) demonstrated its commitment to data analytics by proposing a Comprehensive Automated Risk Data System (CARDS). The CARDS proposal is a rule-based program that would allow FINRA to collect account, account activity and security identification information from regulated entities on an automated basis. The first phase of CARDS would require approximately 200 carrying or clearing firms to periodically submit certain information in an automated, standardized format while *excluding* the collection of personally identifiable information (PII). The purpose of CARDS is to give FINRA more insight into transaction patterns and to allow it to more closely monitor trading activity.

Summoning Resources To Meet the Challenge

Preparing to respond to future regulatory initiatives may require summoning a host of resources, including a company's legal, information technology (IT), information governance (IG), knowledge management (KM), compliance and e-discovery support personnel.

Activities and recommendations may include:

- A comprehensive analysis of the company's readiness to manage litigation and

investigations.

- Applying “Big Data” analytics tools for managing regulatory oversight, “red flagging” key events and enabling teams to proactively respond as needed.
- Leverage prior experiences using data analytics technology for litigation preparedness in order to manage costs and risks.
- Use knowledge management tools and resources to evaluate mission critical functions, including compliance with the reporting requirements from regulatory authorities.
- Engage executive-level stakeholders to lead a coordinated approach to managing information.
- Employ project management personnel and techniques to track governance and build better efficiency into the process.

An increasingly regulated environment may also require companies to:

- Enhance KM programs to build broad-based teams to transfer and share information between groups and divisions.
- Preserve knowledge and expertise from departing employees.
- Leverage advanced technologies to allow for quick and reliable access to key information.
- Maintain a well-designed program that effectively identifies and investigates potentially disruptive events.
- Devote resources to updating policies and procedures related to ongoing regulatory changes and educate employees about those policies and procedures.

Concerns about Data Security and Privacy Given Increased Regulatory Oversight

Financial services firms, in particular, will be challenged to maintain superior defenses against data security threats while attempting to comply with regulatory rules designed, in part, to make the financial services sector more transparent to investors and regulators. In addition, the industry is being asked to regularly provide specific information to regulatory agencies that are not immune to security breaches themselves. Technology advances throughout the industry also make it increasingly difficult for firms to monitor and control user activity. For instance, the expanding use of Bring Your Own Device (BYOD) policies requires firms to consider how to give employees the tools they need to do their jobs while allowing IT to exert some level of control over these tools. Among the issues to consider are:

- Blending the use of devices for both business and personal applications.
- Use of insecure connections, such as open Wi-Fi sources, use of Bluetooth technology and cloud storage.
- Allowing employers to wipe a device when lost or stolen while managing employee concerns about the loss of personal information.
- Developing processes and procedures that allow for supervision and oversight.

Be Prepared

Some financial services firms might find themselves at a technology crossroads. In addition to regulators seeking specific information to be maintained and provided on a regular basis, the SEC and FINRA stepped up their efforts to provide firms with more guidance and potentially increased scrutiny around the industries’ cyber-security policies. Both agencies made announcements warning financial firms of the need to assess their cyber-security measures and to be prepared to address their security policies and procedures if and when the regulators seek the information. These announcements appear to be a prelude to greater cyber-oversight in the days to come.

For inquiries related to this Tip of the Month, please contact Patrick Garbe at

pgarbe@mayerbrown.com from Mayer Brown's Electronic Discovery Services Department, which supports the Firm's case teams and its clients in handling the demands of managing electronic discovery, or Eric Evans at eevans@mayerbrown.com or Kim Leffert at kleffert@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Eric Evans at eevans@mayerbrown, Ethan Hastert at ehastert@mayerbrown.com, Michael Lackey at mlackey@mayerbrown.com or Edmund Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.