INVESTMENT MANAGEMENT ALERT

COMPLIANCE & CYBER SECURITY RISK

JLT SPECIALTY USA | FINANCIAL INSTITUTIONS PRACTICE | OCT. 2015

PERSONAL LIABILITY RESULTING FROM COMPLIANCE AND CYBER SECURITY RISKS HAS INVESTMENT MANAGEMENT FIRMS ON HIGH ALERT

During its most recent fiscal year the Securities and Exchange Commission ("SEC") filed a record 755 enforcement actions and obtained orders totalling $4.16 billion in disgorgement and penalties.[1] Although the totals are astounding and reinforce the SEC's commitment to curtail wrongdoing across the financial services industry, very few compliance officers would expect that any of those penalties would be paid out of their personal check books.

However, recent developments involving U.S. government and regulatory bodies have brought corporate compliance to the forefront, and compliance officers across the investment management industry are buzzing about the potential implications. First, chief compliance officers at BlackRock Advisors LLC and SFX Financial Advisory Management Enterprises Inc. were recently charged by the SEC and found personally liable for failing to implement compliance policies and procedures. Both individuals and their respective firms were handed substantial fines as part of corresponding settlement agreements.[2] In addition, the U.S. Department of Justice ("DOJ") recently created a stir when it announced the hiring of "compliance counsel" who will work with prosecutors to evaluate compliance programs of companies under investigation and determine if the companies should be

The SEC has identified cyber security as a core component of the investment management industry's compliance obligations under federal securities laws.

prosecuted when employees engage in alleged criminal conduct.[3] The DOJ even more recently reinforced their commitment to deter misconduct by seeking accountability from individuals who perpetrate wrongdoing and ensure that they are at the core of any investigation of corporate misconduct.[4] Compliance officers are already tasked with the unenviable responsibility of administering corporate compliance programs in the face of an ever-changing regulatory and risk environment, and the SEC's recent actions to hold compliance officers liable for the implementation of such programs are sending a troubling message.

Cyber! Cyber! Cyber!

The heightened focus on austere implementation of corporate compliance programs is coupled with the growing concern of how to address cybersecurity risk, which the SEC has identified as a core component of the investment management industry's compliance obligations under federal securities laws.[5] The SEC has now brought its first enforcement action centered on cybersecurity.[6] In its Guidance Update issued in April 2015, the SEC's Division of Investment Management reiterated the importance for investment management firms to take compliance obligations into account when assessing their ability to prevent, detect and respond to cyber attacks.

Cybersecurity risk will continue to receive attention from various divisions of the SEC, including the Office of Compliance Inspections and Examinations ("OCIE").[7] On September 15, 2015, OCIE issued its most recent Risk Alert[8] which includes an overview of its intentions to test individual firms' implementation of cybersecurity procedures and controls. OCIE also included a comprehensive five-page sample inspection document request letter which provides a guide to what the SEC may be expecting firms to do as part of a reasonable cybersecurity program. The SEC's specific guidance on cybersecurity and OCIE's continued focus on cybersecurity risk as part of its examination process indicate that firms and their designated compliance officers should be prepared to provide details of policies and procedures and evidence commitment to the effective implementation of a corporate compliance program. The events surrounding BlackRock and SFX call into question how protected compliance officers may actually be from similar charges when their own personal assets are potentially at risk.

Cyber Security as Part of a Compliance Program

The SEC provided various measures for the investment management industry to consider when evaluating cybersecurity as part of an operational corporate compliance program:

- Conduct periodic assessments to identify potential cybersecurity threats and vulnerabilities, including assessments to determine if service providers have protective measures in place;
- Create and routinely test strategies that are designed to prevent, detect and respond to cybersecurity threats;
- Implement strategies through written policies and procedures and monitor compliance with cybersecurity policies and procedures;
- Conduct training that provides guidance to directors, officers and employees concerning cybersecurity threats and measures to prevent, detect and respond to such threats; and
- Educate investors and clients about how to reduce their exposure to cybersecurity threats.

Mitigation and Transfer of Compliance and Cyber Security Risks

JLT partners with investment management firms to protect corporate and personal assets by establishing sound policies and procedures and monitoring and mitigating cybersecurity risk. In addition to enhancing internal policies, procedures and training measures, many of our investment management clients have explored the transfer of cybersecurity risk through the strategic placement of a cyber insurance policy. A detailed review of the firm's directors and officers and/or errors and omissions ("D&O/E&O") insurance program can also help ensure appropriate protection for the firm itself and personal asset protection for its employees, including its compliance officers.

Cyber insurance can address many concerns shared by investment management firms while also being an effective piece of a holistic and proactive approach to address cybersecurity risk. However, if the insurance procurement process is not executed appropriately by a cyber insurance expert, firms may be left with a general cyber insurance policy that may not effectively meet their needs or provide adequate coverage to respond to a cybersecurity event. JLT's specialty cyber team brings years of experience and delivers a unique process to help firms and their directors and officers assess and map their exposures, prepare themselves for an incident, and then properly insure their specific risks. Part of that process includes the evaluation of ancillary policies and coverage that could be impacted in the event of a cyber attack, including a D&O/E&O insurance program which may be called upon to respond to allegations brought against senior management for alleged negligence in overseeing the firm's cybersecurity and protecting confidential information. JLT's D&O/E&O brokers work in conjunction with senior management, attorneys from JLT's dedicated Legal & Claims Practice, and the cyber team to conduct a gap analysis on the existing D&O/E&O programs, draft language to address potential coverage deficiencies, ensure coordination between the D&O/E&O and cyber liability programs, and maximize protection for both personal and corporate assets.

Compliance officers should be prepared to provide details of policies and procedures and demonstrate commitment to the effective implementation of a corporate compliance program.

If you'd like to discuss how your firm can put appropriate cybersecurity measures into practice to address cybersecurity risk exposures as part of your corporate insurance program or otherwise, please contact JLT.

prosecuted

1 U.S. Securities and Exchange Commission, SEC's FY 2014 Enforcement Actions Span Securities Industry and Include First-Ever Cases, N.p. 16 Oct. 4. Web. 02 Sept. 2015.

2 *In the Matter of BlackRock Advisors, LLC*, Adm. Proc. File No. 3-16501 (April 20, 2015); *In the Matter of SFX Financial Advisory Management Enterprises, Inc.*, Adm. Proc. File 3-16591 (June 15, 2015)

3 Karen Freifeld, U.S. Justice Department hiring compliance expert, Reuters (July 30, 2015)

4 U.S. Department of Justice, "Individual Accounting for Corporate Wrongdoing" (September 2015)

5 IM, *"Cybersecurity Guidance Update"* No. 2015-02 (April 2015)

6 *In the Matter of R.T. Jones Capital Equities Management, Inc.*, File 3-16827 (September 22, 2015)

7 OCIE, *"Cybersecurity Examination Sweep Summary"* National Exam Program Risk Alert (February 3, 2015)

8 OCIE, *"OCIE's 2015 Cybersecurity Examination Initiative"* National Exam Program Risk Alert (September 15, 2015)

Learn More:

Mark Flippen
Senior Vice President
917.991.4655
Mark.Flippen@jltus.com

Ryan Farnsworth
Vice President
917.207.1392
Ryan.Farnsworth@jltus.com

Steve Bridges
Senior Vice President
Cyber / E&O Practice
312.259.2633
Steve.Bridges@jltus.com

Rachel Beck
Vice President
212.510.1888
Rachel.Beck@jltus.com

ABOUT JLT

Jardine Lloyd Thompson (JLT) is the world's leading specialty focused provider of insurance, reinsurance, and employee benefits related advice, brokerage and associated services. We provide our clients with deep specialist knowledge, advocacy, tailored advice, and service excellence. Our 10,600 experts worldwide are focused on our client industries and are supported by the second largest international placement network with unparalleled capabilities and resources in 135 countries.

JLT Specialty USA is the U.S. platform of the leading specialty business advisory firm, Jardine Lloyd Thompson Group. Our experts have deep industry and product experience serving leading US and global firms. Our key to client success is our freedom to be creative, collaborative, and analytical while challenging conventions, redefining problems, creating new analytical insights, and exploring new boundaries to deliver solutions for each client's unique business and risks.

JLT Specialty USA
400 Park Avenue, 15th Floor | New York, NY 10022
212.510.1800 | jlt.com