CORE COMPLIANCE & LEGAL SERVICES, INC.

**Risk Management Update**
**January 2021**

## Considerations for Advancing Your Compliance Program

As the new year begins, there is a great opportunity to enhance your firm's compliance program and start the year off on a positive note. In this Risk Management Update, we will discuss several recommendations and best practices to consider when reviewing your compliance program.

### *Requirements For Registered Investment Advisers*

An investment adviser registered with the Securities and Exchange Commission ("SEC") is required to comply with Rule 206(4)-7 (the "Compliance Rule") of the Investment Advisers Act of 1940 as amended ("the Advisers Act")[1]. Under the Compliance Rule, it is unlawful for an SEC registered adviser to provide investment advice unless the adviser has:

- Adopted and implemented written policies and procedures reasonably designed to prevent violations of the Advisers Act and other applicable federal regulations;
- Designated an individual as Chief Compliance Officer responsible for administering compliance; and
- Performed a review at least annually of the firm's written policies and procedures to help ensure their adequacy and the effectiveness of their implementation.

The SEC's expectation under the Compliance Rule is that advisory firms have policies and procedures that not only address all regulations applicable to the firm, but that also are designed to fit the firm's business practices.

The SEC has taken enforcement action against firms who did not have sufficient policies and procedures specifically designed to their business. Some recent cases include:

*First Western Capital Management Company*[2]: From October 2010 through July 2017 First Western purchased Rule 144A restricted securities for clients and did not have adequate compliance policies and procedures pertaining to this activity. First Western was also cited for not providing the firm's investment adviser representatives with training and supervision in regard to the purchase of such securities. The firm was censured and required to pay a monetary fine of $200,000.

*Ares Management LLC*[3]: During 2016, Ares failed to implement and enforce written policies and procedures that were applicable to the firm's business practices regarding material non-public information and that were reasonably designed to prevent violation. This failure resulted in censure and a monetary fine of $1,000,000.

---

[1] https://www.govinfo.gov/content/pkg/COMPS-1878/pdf/COMPS-1878.pdf
[2] IA Release No. 5543 / July 16, 2020Administrative Proceeding File No. 3-19882 (https://www.sec.gov/litigation/admin/2020/ia-5543.pdf)
[3] IA Release No. 55510 / May 26, 2020 Administrative Proceeding File No. 3-19812() (https://www.sec.gov/litigation/admin/2020/ia-5510.pdf)

CORE COMPLIANCE & LEGAL SERVICES, INC.

***Ways to Advance Your Compliance Program in 2021***

When considering how best to approach advancing your compliance program, it's important to focus on key risk areas applicable to your firm, especially those addressed by the SEC in Risk Alerts issued by the Division of Examinations.[4] The Risk Alerts outline deficiencies found during recent exams and steps firms should consider to strengthen compliance in the noted areas. Some of the Risk Alerts issued in 2020 cover: (i) an investment adviser's compliance program, (ii) compliance and supervision by advisers with multiple branch offices, (iii) compliance risks and considerations due to COVID-19; (iv) issues for advisers managing private funds; and (v) compliance with Regulation BI and Form CRS.

It's also important to consider regulatory items, such as previous examination deficiencies received and any rule changes that arose in the previous year.

Also, you should review the SEC's "Examination Priorities Letter"[5] that is issued annually by the Division of Examinations, to see if there are any items relevant to the firm's business practices that are not currently or adequately addressed in the firm's policies and procedures.

Additional steps for enhancing your firm's compliance program include:

- Reviewing internal controls to confirm they are set up to ensure compliance with firm policies and applicable regulatory requirements.
- Maintaining accurate and complete books and records, as required.
- Tailoring policies and procedures to fit the business model of your firm.
- Implementing controls to prevent reoccurrence of compliance related issues/violations that had previously occurred.
- Ensuring your firm has appropriate controls and processes in place that address areas affected by the COVID-19 pandemic.
- Revising policies and procedures to comply with the newly adopted amendments made to the advertising rule ("Rule 206(4)-1"), under the Advisers Act.[6]

Given the continued environment of working remotely due to COVID-19, you should also focus on whether any updates are needed to the firm's Business Continuity Plan and Cybersecurity Policy.

When reviewing your firm's Business Continuity Plan, you should consider the firm's continued ability to perform business functions during extended significant business disruptions, such as a pandemic.

---

[4] *See* https://www.sec.gov/exams.

[5] *See* https://www.sec.gov/exams

[6] *See* https://www.sec.gov/rules/final/2020/ia-5653.pdf

In this regard, your Business Continuity Plan should include the following:

- Additional resources or measures taken to secure computer systems and servers.
- An outline of the support and infrastructure for employees working remotely.
- Steps taken to ensure data is protected at remote sites and on any personal computers being used for business purposes.
- Alternative worksites for business operations (i.e., remote working from employees' homes.
- Pandemic response and preparedness steps.

When reviewing your cybersecurity policy and protocols, you should:

- Ensure colleagues are using strong passwords, multi-factor authentication, secure wi-fi networks and have heightened awareness of phishing and other cyber-crime attempts.
- Implement the use of remote desktop servers ("RDS") or a virtual private network ("VPN") for employees to securely connect to your firm's systems and protect clients' information.
- Consider implementing proactive vulnerability and patch management programs that detect risks to the technology environment and firm.
- Have robust incident response and resiliency policies, procedures, and plans.
- Conduct and document a cybersecurity risk assessment at least annually.

As discussed in our previous Risk Management Update titled "Cybersecurity Considerations for Working from Home during COVID-19"[7], training employees on how to identify risks associated with cybersecurity threats is an essential part of your firm's cybersecurity program.

When creating cybersecurity training programs for employees, you should consider taking the following steps:

- Implementing phishing exercises to help employees identify phishing emails and how to handle such scenarios.
- Reviewing the firm's cybersecurity policy and incident response plan with employees to ensure they are aware of how to respond in the event of a ransomware or cyberattack.
- Providing examples of cybersecurity threats and steps to take to address.
- Ensuring all employees are aware of security steps, including having strong passwords and using multi factor authentication for software and devices.

Training provides employees with insight on the responsibilities, awareness, and risk of cyber threats and how to prevent such events from occurring.

---

[7] *See* https://www.corecls.com/news-events/cybersecurity-considerations-for-working-from-home-during-covid-19

CORE COMPLIANCE & LEGAL SERVICES, INC.

***Conclusion***

As you begin a new year, ensuring that your firm's compliance program is strong, and that functionalities are a step ahead, is critical for continued growth and success for years to come.

For assistance with enhancing your compliance program, additional information pertaining to what we have discussed or for any other compliance assistance, please contact us at info@corecls.com, (619) 278-0020, or visit us at www.corecls.com.

**Authors: Tina Mitchell, Managing Director of Consultation Services, Core Compliance. Core Compliance works extensively with investment advisers, broker-dealers, investment companies, hedge funds, private equity firms and banks on regulatory compliance issues.**