JACKO LAW GROUP, PC

Legal Risk Management Tip
July 2016

REGULATORY REQUIREMENTS AND RISKS ASSOCIATED WITH CONDUCTING DUE DILIGENCE ON THIRD-PARTY SERVICE PROVIDERS

There are a variety of reasons why financial firms choose to partner with external third-party service providers ("TPSPs") for the performance of essential tasks, rather than performing such tasks internally. Such reasons often include, but are not limited to, the financial firm's experience in performing certain tasks, cost/time restrictions and common industry practice. Regardless as to the impetus for these relationships, regulators require financial firms to conduct initial and ongoing due diligence on TPSPs. This article will discuss the legal requirements of financial institutions to perform due diligence on TPSPs, examine recent enforcement cases where financial firms failed to properly perform such diligence and offer guidance on what financial institutions should consider when performing due diligence on service providers.

Regulatory Obligations

Due diligence is the level of prudence, judgment and care a reasonable person exercises prior to entering into an agreement or transaction in order to avoid harm.[1] For the past several years, regulators such as the U.S. Securities and Exchange Commission ("SEC") and the Financial Industry Regulatory Authority ("FINRA"), have placed a high priority on ensuring that financial institutions have strong due diligence programs in place covering their use of external TPSPs.[2] In enforcing this requirement, regulators, among other sources, typically rely upon the following:

A. Rule 206(4)-7 under the Investment Advisers Act of 1940

Under Rule 206(4)-7 of the Investment Advisers Act of 1940, as amended (the "Advisers Act"), investment advisers are required to adopt written policies and procedures reasonably designed to prevent violations of federal securities laws. Part of this requirement is for investment advisers to conduct due diligence on TPSPs to ensure any tasks outsourced by the adviser to such third-parties are being conducted pursuant to federal law. While the SEC's formal guidance does not give a great amount of detail as to the extent and scope of such due diligence requirements, the SEC generally looks for due diligence which are "reasonably designed" to detect and prevent violations of federal securities laws.

B. Rule 38a-1 under the Investment Company Act of 1940

Similar to the rules imposed on investment advisers by the Advisers Act, Rule 38a-1 under the Investment Company Act of 1940 requires investment companies to adopt written policies and procedures reasonably designed to prevent violations of federal securities laws. Performing due diligence on TPSPs are required under this rule. Just this year, the SEC emphasized this requirement as part of a *Guidance Update* when the Commission stated, "because funds…outsource critical functions to third parties, the [SEC] staff believes that they should consider conducting thorough initial and ongoing due diligence of those third parties."[3]

---

[1] *See* http://definitions.uslegal.com/d/due-diligence/.
[2] *See* http://www.finra.org/sites/default/files/2016-regulatory-and-examination-priorities-letter.pdf.
[3] *See* https://www.sec.gov/investment/im-guidance-2016-04.pdf.

C. FINRA Notice to Members 05-48

In this Notice to Members, FINRA established that "outsourced activities, performed by a third party, are required to be subject to a supervisory system and written supervisory procedures pursuant to NASD Rule 3010, as if they were performed by the member itself."[4] FINRA further reminded its members that outsourcing an activity or function to a TPSP does not relieve broker-dealers of their ultimate responsibility for compliance with all applicable rules, including oversight, supervision and monitoring a TPSP's performance. Notably, more recent guidance in appears in Notice to Members 11-14, and Letters to Members March 9. 2009 and March 1, 2010.[5]

D. Other Regulatory Guidance and Considerations

There are a number of other regulatory areas where due diligence of service providers is essential. For example, in order to comply with Regulation S-P (privacy controls), the financial firm must understand the confidentiality and privacy controls of the TPSP. Cybersecurity requires the financial institution to understand what personally identifiable information the TPSP may have relating to the firm's clients in a cyber-environment and take steps to ensure the TSPS's cyber controls are adequate.[6] Moreover, it is imperative that a TPSP understands their role within the firm's business continuity plan[7], particularly if they are a critical service provider.

Recent Enforcement Actions

The activities a TPSP may perform for a financial firm will vary. Firms must review their internal business practices to identify those services performed by TPSPs, and what due diligence reviews will be necessary to ensure TPSP is performing such services in accordance with relevant law. The following cases, while not an exhaustive list, provide a sampling of enforcement actions relating to a financial firm's failure to perform proper due diligence:

A. *In the Matter of Cantella & Co.*, IA Rel. No. 4338 (Feb. 23, 2016)

In this matter, the SEC alleged that Cantella, a registered investment adviser, took insufficient steps to confirm the accuracy of F-Squared Investments, Inc.'s historical data and other information contained in advertising materials distributed by Cantella. Had Cantella performed adequate due diligence on F-Squared, its proposed data and calculation methodologies, such inaccuracies would have been identified. As a result of failing to perform such diligence, the advertisements showed results that were inflated substantially over what F-Squared's actual performance had been. Cantella consented to the entry of the order finding that it violated, among other things, Section 206(4) of the Advisers Act, and, without admitting or denying the findings, agreed to pay a $100,000 penalty.

---

[4] http://www.klgates.com/files/Publication/41c5c142-b100-4cac-adee-c26543a79353/Presentation/PublicationAttachment/a48defdd-92da-4424-841d-a60a14b58e05/IMA0805b.pdf.

[5] The complete text of the Notice to Members and Letters to Members referenced may be found at http://www.finra.org/sites/default/files/NoticeDocument/p123398.pdf, https://www.finra.org/sites/default/files/Industry/p118113.pdf, and http://www.finra.org/sites/default/files/Industry/p121004.pdf respectively.

[6] *See* http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

[7] Additional information concerning SEC expectations of firm business continuity plans may be found at https://www.sec.gov/rules/proposed/2016/ia-4439.pdf.

B. *In the Matter of Calhoun Asset Management, LLC, and Krista Lynn Ward,* IA Rel. No. 3428 (July 9, 2012)

In this matter, the SEC alleged that materially false and misleading statements were made by Calhoun, the investment adviser to two funds of funds, and Ward, its principal and sole employee, about the firm's due diligence process. Specifically, Calhoun touted due diligence process in marketing materials and the firm's website, particularly on the selection of investment managers, but failed to conduct such due diligence. Instead, Calhoun outsourced the services to a third-party vendor, who Calhoun did not perform due diligence on or monitor in any capacity. As a result, Calhoun received a $50,000 penalty (joint and several basis with Ward), and Ward was barred from brokerage and advisory business with right to reapply in five years.

C. Merrill Lynch, Pierce, Fenner & Smith Incorporated, Respondent Case 2008014187701

Merrill Lynch outsourced some of its proxy functions for certain accounts of its advisor programs to a TPSP. The TPSP misdirected proxy ballots, utilized outdated proxy delivery designations and conducted clerical errors. FINRA alleged that Merrill Lynch had, among other things, failed to establish a supervisory system to reasonably supervise the delivery of proxies to certain customers. FINRA argued that had such due diligence processes been in place, such errors would have been detected by Merrill Lynch. Merrill Lynch consented to the imposition of various sanctions, censure and a $2.8 million fine.

What to Consider When Performing Due Diligence of TPSPs

Working with TPSPs opens a financial firm up to various types of risks, including operational, legal and regulatory risks. Establishing policies and procedures that dictate how your firm will conduct due diligence on TPSPs, such as when and by whom, is vital for ensuring your firm is in proper compliance. In practice, there are different ways to conduct due diligence. Commonly, financial firms will delegate one or more internal persons to be in charge of overseeing the firm's due diligence process. Checklists, questionnaires and additional forms are often utilized to ensure the firm is capturing all relevant information. Conversely, some firms may opt to outsource their due diligence in order to have an "independent review." However, this can be extremely costly. Others rely on third-party reports. Typically, for this type of arrangement, the cost is borne by the sub-adviser or service provider. However, the disadvantage lies in the party providing the report and whether or not it is reliable. In other words, you still have a duty to conduct due diligence on the third-party who is conducting due diligence on your behalf. For more information on how to create and monitor due diligence policies and procedures, as well what documentation should be collected and retained during such reviews, please refer to JLG's April of 2010 Legal Tip entitled, "Best Practices for the Due Diligence Process," which can be found here.

Conclusion

A financial firm is required to perform due diligence on those TPSPs performing tasks on behalf of the firm prior to engaging them for services and periodically thereafter. Such due diligence should be conducted more frequently for critical services providers and for those TPSPs who have access to firm client's personally identifiable information. Failure to perform adequate due diligence exposes the firm to risk that can lead to enforcement by regulators and complaints by clients. To mitigate these risks, financial firms should develop thorough due diligence processes that are memorialized in the firm's policies and procedures manual and documented when

conducted. Review these internal controls frequently for adequacy, and take steps to address gaps as detected. Most importantly, discuss what the firm should do if or when a "red flag" is detected with a TPSP and continuously keep in mind whether the TPSP has adequate controls in place to provide services to you, and to your customers.

For more information on this topic, please contact us at (619) 298-2880 or at info@jackolg.com.

Author: Robert Boeche, Esq., Attorney; Editor: Michelle L. Jacko, Esq., Managing Partner, Jacko Law Group, PC. JLG works extensively with investment advisers, broker-dealers, investment companies, hedge funds, banks and corporate clients on securities and corporate counsel matters.