Appendix E - Use of Third-Party Service Providers Questionnaire

Each NFA Member firm must adopt a written supervisory framework over outsourcing of regulatory obligations to third-party service providers.

Please also consult the following Interpretive Notice when designing your supervisory framework:

> Interpretive Notice 9079 *NFA Compliance Rules 2-9 and 2-36: Members' Use of Third-Party Service Providers*

A Member's written supervisory framework over its outsourcing process should answer all of the following questions as completely as possible. Although you may answer "not applicable" to certain questions, you should carefully consider the firm's operations before doing so. Additionally, firms must maintain records pursuant to NFA Compliance Rules 2-10 and 2-49 to demonstrate that it has addressed the areas included in the supervisory framework.

Initial Risk Assessment

- How does the firm determine whether a regulatory function is appropriate to outsource?
- What risks does the firm evaluate when considering whether to outsource a function? Examples of primary areas of risks include information security, regulatory and logistics. Other applicable risks may be considered depending on the regulatory function that is being outsourced.
- Is the firm able to adequately manage risks associated with outsourcing a particular function? Note: Unless a Member determines that it may adequately manage the risks associated with outsourcing a particular function, a Member generally should not move forward with outsourcing the function.
- How are employees that are involved in the risk assessment process made aware of NFA's Interpretive Notice on outsourcing?

Onboarding Due Diligence

- What is the firm's process for conducting due diligence on prospective third-party service providers?
- Does this process include a review to ensure the third-party is aware of NFA and CFTC requirements, has sufficient regulatory experience and has the operational capabilities to carry out the outsourced function(s) fully and accurately?
- What additional due diligence does the firm conduct on third parties that have access to critical and/or confidential data and those that support a Member's critical regulatory-related systems (e.g., handling customer segregated funds, keeping required records, filing financial reports, etc.)? Examples of key areas of a third-party service provider a firm could review include IT security, financial stability, background of key employees, regulatory history and business continuity and contingency plans.
- What is the firm's process to ensure compliance with NFA Bylaw 1101 when selecting a third-party service provider?
- How does the firm identify whether a third-party service provider subcontracts any outsourced regulatory functions?
- If the third-party service provider uses a subcontractor for outsourced regulatory functions, does the firm's procedures consider assessing the risks associated with subcontracting the function(s)?
- Does the firm require a third-party service provider to provide notice of any changes in subcontractor(s)?
- Does the firm require third-party service providers to execute a written agreement outlining the services provided? A written agreement should describe the scope of services being performed and addresses any guarantees and indemnifications, limitations of liability and other payment terms.

- Does the written agreement require the third-party service provider to comply with all applicable regulatory requirements, including the production of records, and to immediately notify the Member of any material failure(s) in performing the outsourced regulatory function(s)?
- Who at the firm is permitted to enter into an agreement to outsource regulatory requirements?

Ongoing Monitoring

- What and how often does the firm review to ensure the third-party service provider is adequately performing the outsourced function?
- What and how often does the firm review the third-party service provider? Note: A review of the third-party service provider may include a review for changes in IT security, financial stability, business continuity and contingency plans, audit or examination results, websites, public filings, insurance coverage and references.
- Does the firm require the third party to provide notice of any material changes in the processes used to carry out the outsourced function?
- Does the firm require the third party to provide notice if a key employee with access to the Member's information is terminated and ensure this individual's access to this information has been removed?
- Does the firm conduct ongoing monitoring functions on a more frequent basis for regulatory functions that are critical for the firm's operations?
- Does the firm have adequate resources and qualified individuals (internal or external) to perform adequate ongoing monitoring?
- What is the firm's process for escalating instances where a third-party service provider fails to perform the outsourced function or when its risk profile materially changes?
- Does the firm consider the risks associated with any proposed changes to the contract with the third-party service provider?
- Does the firm incorporate best practices with respect to contract renewals?

Termination of Outsourcing

- Does the written agreement with the third-party service provider require they give sufficient notice prior to terminating its relationship with the Member?
- Does the firm have a process for obtaining records from the third-party service provider at the termination of the outsourcing arrangement?
- If the third-party service provider will maintain records, does the firm have an agreement with the third-party service provider that the records will be maintained for an appropriate amount of time?
- Does the firm ensure that a terminated third-party service provider no longer has access to confidential information and data once the service agreement has terminated?
- Does the firm ensure that a terminated third-party service provider does not unnecessarily retain confidential information and data?