Interpretive Notices

Effective September 30, 2021 this new Interpretive Notice will be added and read as follows:

9079 - NFA COMPLIANCE RULES 2-9 AND 2-36: MEMBERS' USE OF THIRD-PARTY SERVICE PROVIDERS

(*Board of Directors, February 18, 2021, effective September 30, 2021*).

NFA Compliance Rule 2-9(a) places a continuing responsibility on every Member futures commission merchant (FCM), commodity trading advisor (CTA), commodity pool operator (CPO), and introducing broker (IB) to diligently supervise its employees and agents in all aspects of their commodity interest activities. NFA Compliance Rule 2-9(d) places the same supervisory responsibilities on swap dealer and major swap participant Members (collectively, Swap Dealer Members) regarding their swap activities and NFA Compliance Rule 2-36(e) places identical supervisory obligations on NFA forex dealer members (FDMs) for their forex activities. Over the years, NFA has issued Interpretive Notices to provide more specific guidance in certain areas on acceptable standards for supervisory procedures.

NFA recognizes that a Member may fulfill, in part, its regulatory obligations by having a third-party service provider(s) or vendor(s) (Third-Party Service Provider)[1] perform certain functions that would otherwise be undertaken by the Member itself to comply with NFA and CFTC Requirements. NFA understands that outsourcing certain functions may provide benefits to a Member. If a Member outsources a regulatory function, however, it remains responsible for complying with NFA and/or CFTC Requirements and may be subject to discipline if a Third-Party Service Provider's performance causes the Member to fail to comply with those Requirements. To mitigate the risks associated with outsourcing, a Member must have a written supervisory framework over its outsourcing function.[2]

NFA recognizes that a Member must have flexibility to adopt a written supervisory framework relating to outsourcing functions to a Third-Party Service Provider that is tailored to a Member's specific needs and business as described below.[3] This Interpretive Notice establishes general requirements relating to a Member's written supervisory framework,[4] which requires Members to address, at a minimum, the following areas: an initial risk assessment; onboarding due diligence; ongoing monitoring; termination; and recordkeeping relating to Third-Party Service Providers.[5]

A Member must comply with the general requirements set forth in this Notice only with respect to a Third-Party Service Provider(s) that performs functions to assist the Member in fulfilling its regulatory obligations that address NFA and/or CFTC Requirements. Further guidance relating to each of these areas is discussed below.[6]

Initial Risk Assessment

At the outset, a Member should determine whether a particular regulatory function is appropriate to outsource and evaluate the risks associated with outsourcing the function.[7] For example, a Member may determine that it is appropriate to engage a third party to conduct annual branch office reviews, but based on its circumstances, determine it is not appropriate to engage it to conduct initial due diligence on a potential branch office. Similarly, a Member might conclude that it is appropriate to outsource the collection of long-term outstanding debit balances, but determine that it should monitor outstanding daily margin calls. Moreover, a Member may determine that it is appropriate to outsource certain core regulatory functions that are required to be performed by the Member on a frequent or even daily basis (e.g., issuing swaps confirmations, calculating and issuing margin calls, or reporting swaps data to a swap data repository).[8]

Although the potential risks associated with outsourcing a function may vary, a Member should analyze and identify certain primary areas of risk including:

> *Information Security* — The type of confidential, personally identifying information or other valuable information a Third-Party Service Provider may obtain or have access to and the measures it puts in place to protect the information;
>
> *Regulatory* — The impact to the Member, customers, and counterparties if the service provider fails to carry out the function properly; and
>
> *Logistics* — The location of the service provider and whether it has the resources to meet its contractual obligations and provide the Member with access to required records.

In addition to these primary areas of risk, a Member should consider other potential areas of risk applicable to its business and the regulatory function that is being outsourced. 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.

Onboarding Due Diligence

Scope of Due Diligence. A Member should perform due diligence on any prospective Third-Party Service Provider prior to entering into a contractual outsourcing arrangement in order to determine whether the service provider is able to successfully carry out the outsourced function in a manner designed to comply with NFA and/or CFTC Requirements. For example, in choosing to utilize a third party to examine a Member's branch offices or to comply with recurring or operationally intensive swaps regulatory requirements, Members should ensure that the service provider is aware of relevant NFA and CFTC rules and regulations, has sufficient regulatory experience, and has the operational capabilities to fully and accurately carry out the outsourced function(s). A Member's level of onboarding due diligence should be commensurate with the risks associated with outsourcing a particular regulatory function, be tailored to a Member's business needs, and provide a Member with an appropriate level of confidence in the Third-Party Service Provider's ability to properly carry out the outsourced function.

Additionally, a Member's onboarding due diligence process should be heightened for Third-Party Service Providers that obtain or have access to a Member's 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.). In these instances, a Member should consider assessing the following key areas relating to a Third-Party Service Provider: IT security (e.g., practices regarding data transmission and storage),[9] financial stability,[10] background of key employees, regulatory history (e.g., regulatory actions or lawsuits), and business continuity and contingency plans, particularly those related to data availability and integrity.

A Member should also inquire about whether a Third-Party Service Provider subcontracts any of the regulatory functions that the Member outsourced to the service provider. If so, the Member should request the identity of a subcontractor(s) and, if possible, assess the risks associated with the Third-Party Service Provider's subcontracting of the function. A Member should require a Third-Party Service Provider to notify the Member of any change in a subcontractor(s) and retain the ability to terminate the relationship if the service provider makes any material changes involving a subcontractor that would have an adverse effect on the performance of the outsourced function.

Written Agreement.[11] A Member and Third-Party Service Provider should execute a written agreement[12] that fully describes the scope of services being performed and addresses any guarantees and indemnifications, limitations of liability, and payment terms. NFA recognizes that in some cases a Member, due to its size or otherwise, may have little or no ability to negotiate and secure the inclusion of specific contractual terms, especially in agreements with industry service providers that support critical infrastructure. Each Member, however, should carefully review its Third-Party Service Provider relationships to ensure to the extent possible that contractual terms are appropriate and reflect the outsourcing relationship(s) as intended.

When entering into a prospective written agreement, a Member should make a reasonable effort to ensure that the service provider agrees 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).[13] If applicable, a Member's agreement with a Third-Party Service Provider should address the process for data management at the termination of the relationship.

Depending on the criticality of, and risk associated with, the function being outsourced, a Member should consider whether it is appropriate for a firm principal to either execute the outsourcing agreement or be notified that the Member has entered into an agreement. For example, a large CPO Member should consider if its CFO should execute or be notified that the CPO has entered into an agreement for a Third-Party Service Provider to provide monthly bookkeeping functions or administrative functions for the CPO's pool(s).

Ongoing Monitoring

The Required Risk-Based Review. A Member should conduct ongoing monitoring of a Third-Party Service Provider's ability to properly carry out an outsourced function and meet its contractual obligations. A Member's ongoing monitoring should involve both the ongoing review (e.g., by reviewing any reports generated by a third party for accuracy) of a particular outsourced function(s) to ensure that it is being performed appropriately, and periodic holistic reviews of each Third-Party Service Provider's performance, regulatory compliance and, if appropriate, IT security, financial stability, business continuity and contingency plans, audit or examination results, websites, public filings, insurance coverage, and references. In general, a Member should require a Third-Party Service Provider to notify it of any material changes to the provider's material systems or processes utilized to carry out an outsourced regulatory function. A Member should tailor the frequency and scope of ongoing monitoring reviews to the criticality of, and risk associated with, the outsourced function. For example, a Member may determine to review a Third-Party Service Provider with access to customer or counterparty data more frequently than a service provider that has no access to this type of data.

Some Third-Party Service Providers perform multiple functions for a Member or otherwise provide an essential or critical service (e.g., collect and maintain customer/counterparty onboarding data). NFA recognizes that there may be only one or few service provider(s) to perform certain functions. However, to the extent applicable, a Member should evaluate the risk associated with becoming overly reliant on a particular Third-Party Service Provider and consider the availability of alternatives, including other service provider(s) or in-house solutions in case a viable "exit strategy" is necessary.

Senior Management Involvement . Depending on a Member's size, operations, risk tolerance and the criticality of, and risk associated with, the outsourced function, a Member should consider whether the Member has adequate resources and qualified personnel performing ongoing monitoring. Additionally, a Member should have a process of escalation to senior management when a Third-Party Service Provider fails to perform an outsourced function or its risk profile materially changes (e.g., regulatory fine or business failure). Some Members may maintain internal committees (including risk committees) that must be notified about Third-Party Service Provider relationships and any material changes[14] to them and may also engage an independent party to review their third-party outsourced relationships.

Contractual Renewals. Finally, as part of the on-going monitoring process, a Member should consider incorporating best practices relating to contractual renewals. Throughout the length of its relationship with a Third-Party Service Provider, a Member should identify and evaluate the risks associated with any proposed changes to its agreements.

Termination

A Member's agreement with a Third-Party Service Provider should require that the Third-Party Service Provider give the Member sufficient notice prior to terminating its relationship with the Member in order to ensure that the Member can maintain operational, regulatory or other capabilities supported by the service provider. In particular, a Member must be able to meet all NFA and CFTC requirements, including recordkeeping requirements, after termination. Members will often need to obtain records from a Third-Party Service Provider at the termination of the outsourcing relationship or enter into an agreement with the service provider to continue acting as a records custodian for an appropriate amount of time.

Upon termination, a Member should also make a reasonable effort to ensure that a terminated Third-Party Service Provider no longer has access to confidential information and data of the Member and its customers or counterparties.[15] Further, a Member should ensure that a terminated service provider does not unnecessarily retain and, in appropriate circumstances, returns confidential information and data of the Member and its customers or counterparties. For example, a Third-Party Service Provider that performs accounting functions may have been granted "read-only" access to certain Member back-office systems and internal reports, and a Member should verify that this provider's access is terminated.

Recordkeeping

Any Member that engages a Third-Party Service Provider to perform a function to meet a regulatory obligation pursuant to an NFA and/or CFTC Requirement must maintain records pursuant to NFA Compliance Rules 2-10 and 2-49 to demonstrate that it has addressed the areas described in this Notice.

---

[1] When outsourcing to a Third-Party Service Provider, a Member should ensure, to the extent applicable, compliance with NFA Bylaw 1101. Further, even if a Member outsources a regulatory obligation to an affiliate, or to a Third-Party Service Provider with an existing contractual relationship with the Member's parent entity, a Member should comply with this Notice's requirements.

[2] NFA has previously issued Interpretive Notices relating to specific regulatory areas that also include guidance regarding Members' supervisory obligations related to Third-Party Service Providers. This Notice's requirements supplement the requirements set forth in those Notices. For example, see: NFA Interpretive Notice (IN) 9037 – *NFA Compliance Rule 2-9: Supervisory Procedures for E-Mail and the Use of Web Sites*; IN 9045 – *NFA Compliance Rule 2-9: FCM and IB Anti-Money Laundering Program*; IN 9046 – *Compliance Rule 2-9: Supervision of the Use of Automated Order-Routing Systems*; IN 9055 – *NFA Bylaw 1101, Compliance Rules 2-9 and 2-29: Guidelines Relating to the Registration of Third-Party Trading System Developers and the Responsibility of NFA Members for Promotional Material That Promotes Third-Party Trading System Developers and Their Trading Systems*; IN 9060 – *Compliance Rule 2-36(e): Supervision of the Use of Electronic Trading Systems;* IN 9070 – *NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs*.

[3] A Member may be part of a larger holding company structure that has a dedicated procurement or vendor management department responsible for onboarding and maintaining Third-Party Service Provider relationships for the Member. A Member may meet its obligations under this Notice through the holding company's procurement or vendor management department as long as it addresses the areas described in the Notice with respect to the Member.

[4] CFTC Regulation 1.11(e)(3)(i)(A)-(B) requires FCMs to conduct onboarding and ongoing due diligence on depositories carrying customer funds. This Notice does not impact an FCM's obligations under this regulation. Moreover, an FCM may want to consider the processes and procedures used to meet this obligation when designing the processes for onboarding and conducting ongoing due diligence for Third-Party Service Providers.

[5] NFA recognizes that the guidance relating to several of these areas may overlap and, therefore, a Member's supervisory framework does not have to address each of these areas in isolation provided that the issues and risks associated with each area are addressed when initiating and managing outsourcing relationships.

[6] As additional guidance, Members may want to consider incorporating relevant standards and guidelines including, but not limited to, those set out in the National Institute of Standards and Technology (NIST) SP-800 series of publications (https://csrc.nist.gov/publications/sp800); the International Organization of Securities Commissions' (IOSCO) 2005 report *Principles on Outsourcing of Financial Services for Market Intermediaries* (https://www.iosco.org/library/pubdocs/pdf/IOSCOPD187.pdf); and the Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook sections on outsourcing (https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx).

[7] A Member's size and operations may impact how it onboards and maintains Third-Party Service Provider relationships. Members may have dedicated procurement or vendor management departments responsible for all aspects of these relationships. Other Members may divide the responsibilities of onboarding a vendor to various firm personnel. Members should ensure that all employees involved in this process are aware of this Notice's requirements.

[8] These examples are for illustrative purposes only. The Notice is not outlining functions that a Member is permitted or not permitted to outsource. The determination of whether to outsource a function remains with the Member.

[9] Members should avoid using service providers that are unable to meet NFA and CFTC standards regarding the confidentiality of customer data, which are set out, for example, in NFA Interpretive Notice 9070 – *NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs* and CFTC Part 160.

[10] In assessing financial stability, a Member may want to consider, as appropriate, reviewing a potential service provider's financial statements, audit or examination (internal or third party) results, websites, public filings, insurance coverage, or references.

[11] NFA understands that Members will have existing agreements in place at the time this Interpretive Notice becomes effective. NFA does not expect a Member to re-negotiate these agreements prior to their termination dates, but NFA does recommend that a Member consider the above guidance when re-negotiating, renewing existing agreements, and engaging new Third-Party Service Providers.

[12] A written agreement mitigates the risks of non-performance or disagreements relating to the scope and nature of the services performed.

[13] As noted in the introduction to this Interpretive Notice, if the Third-Party Service Provider fails to perform in a manner that meets the Member's regulatory requirements, the Member is ultimately responsible for this failure, and based on the facts and circumstances, may be subject to discipline.

[14] The definition of a "material change" may differ depending on a Member's size, business, the functions outsourced, and the type of Third-Party Service Provider(s) utilized (e.g., regulated).

[15] Members should also consider requiring Third-Party Service Providers to notify them if a key employee with access to a Member's information is terminated and provide assurance that the employee's access to this information has been shut-off.