April 1, 2024

VIA Email: secretary@cftc.gov
Mr. Christopher Kirkpatrick
Secretary of the Commission
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, N.W.
Washington, D.C. 20581

Re: RIN 3038-AF23: Operational Resilience Framework for Futures Commission Merchants, Swap Dealers and Major Swap Participants

Dear Mr. Kirkpatrick:

National Futures Association (NFA) appreciates the opportunity to comment on the Commodity Futures Trading Commission's (CFTC or Commission) notice of proposed rulemaking to require futures commission merchants (FCMs), swap dealers (SDs) and major swap participants (MSPs)[1] to establish, document and implement an Operational Resilience Framework (ORF) consisting of an information and technology security program, a third-party relationship program and a business continuity and disaster recovery plan.

As the Commission suggests in the preamble, recent events in the financial industry, including the Covid-19 pandemic and increased cyber attacks targeting financial sector institutions, highlight the importance of risk management practices targeting operational risk. NFA understands the Commission's desire to adopt requirements designed to ensure that FCMs and SDs have actionable plans in place to address key operational risks. However, for the reasons discussed below, NFA is concerned that the Commission's current proposal may impose undue and unnecessary burdens on FCMs and SDs. We further believe that the Commission can achieve its objective to have appropriate oversight in this area by utilizing the existing framework that NFA currently imposes on all Member firms, including FCMs and SDs, with respect to operational resilience.

NFA respectfully requests that the Commission consider the following comments on this important proposal.

[1] Although NFA's rules cover the activities of MSPs, currently there are no entities registered in that category. Therefore, this comment letter will not discuss the proposed ORF as applicable to MSPs.

NFA's Existing Framework for Member Firms Including FCMs and SDs

As the Commission is aware, NFA currently requires ***all*** Member firms, including FCMs and SDs, to have written policies and procedures and implement supervisory programs addressing each of the components included in the Commission's proposed ORF. NFA has separate examination modules for each operational resilience area, and we test FCM and SD compliance with these requirements as part of our examination program. All Members are subject to an initial review of their compliance with NFA's requirements, and we conduct follow-up testing using our risk-based methodology.

Information Systems Security Programs

NFA Compliance Rules 2-9 and 2-49 and its related Interpretive Notice entitled *NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs* (ISSP Interpretive Notice) require FCMs and SDs to have an information systems security program (ISSP) that identifies a Member's information technology risks, adopts safeguards to address those risks, adopts an incidence response plan, includes procedures to notify NFA of specific events and requires ongoing training for impacted employees. NFA's Interpretive Notice also requires Members to monitor and regularly review the effectiveness of their ISSPs and make appropriate changes, as well as maintain records relating to the adoption and implementation of their ISSPs.

In adopting NFA's ISSP Interpretive Notice in 2015, we recognized that U.S. financial institutions were facing increased and complex information system breaches. We further noted that other regulators already imposed systems' security requirements[2] on many dually registered or otherwise licensed NFA Member firms (*e.g.,* broker-dealers, investment advisors and banks), and we found these other regulators' frameworks and requirements completely satisfactory. Before adopting NFA's ISSP requirements, we spent significant time reviewing these existing systems' security requirements and best practices from internationally recognized standard-setting organizations. NFA also worked closely with NFA Members across our Member categories, NFA's Member Advisory Committees, NFA's Board of Directors (Board), as well as Commission staff.

Since not all Member firms were covered by other regulatory regimes' security requirements, NFA's Board adopted NFA's ISSP Interpretive Notice to provide guidance on acceptable best practices to potentially mitigate the significant information security risks, threats and damages posed to NFA Member firms' derivatives business,

[2] As noted in NFA's August 2015 submission letter to the CFTC, NFA reviewed guidance issued by other financial regulators including FINRA's February 2015 Report on Cybersecurity Practices that presents an approach to cybersecurity for broker-dealers grounded in risk management and the Guidance Update issued in April 2015 by the SEC's Division of Investment Management that discusses cybersecurity measures for investment companies and investment advisers. NFA also reviewed SIFMA's July 2014 Small Firms' Cybersecurity Guidance and the U.S. Department of Justice's April 2015 Best Practices for Victim Response and Reporting of Cyber Incidents.

their customers and counterparties and the U.S. derivatives industry. A key objective, however, in doing so was to ensure that NFA's information security requirements materially aligned with those of other financial regulators so that Members covered by other satisfactory frameworks did not need to rework them. Today, we continue to monitor developments in this area to ensure our requirements remain consistent and up-to-date and make changes, if necessary.[3]

Third-Party Service Providers

NFA Compliance Rule 2-9 and its related Interpretive Notice entitled: *NFA Compliance Rule 2-9 and 2-36: Members' Use of Third-Party Service Providers* (Third-Party Service Provider Interpretive Notice) requires FCM and SD Members to have a supervisory framework relating to outsourcing functions to a third party that must include an initial risk assessment, onboarding due diligence, ongoing monitoring, termination and recordkeeping. In adopting the Third-Party Service Provider Interpretive Notice in 2021, NFA tailored the Notice's applicability to Members using third-party service providers to perform functions or activities related to their regulated derivatives business, including their compliance functions. NFA was concerned that although a Member outsourcing a regulatory function remains responsible for ensuring its compliance with related CFTC and NFA requirements, no specific rules required a Member to have a framework in place designed to ensure that the activities conducted by the third party on behalf of the Member actually comply with applicable CFTC and NFA requirements.

Therefore, NFA's Third-Party Service Provider Interpretive Notice requires Members that outsource regulatory functions to adopt and implement a written supervisory framework over this activity. Among other things, NFA's Interpretive Notice requires that a Member conduct appropriate due diligence on third-party vendors before making outsourcing decisions and have policies and procedures to monitor the third-party relationship from start to finish. Specifically, the Third-Party Service Provider Interpretive Notice requires a Member's supervisory framework to address: an initial risk assessment, onboarding due diligence, ongoing monitoring, termination and recordkeeping.

In developing the Third-Party Service Provider Interpretive Notice, staff followed a similar process to the one employed in adopting the ISSP Interpretive Notice. In addition to discussing the components of the program with NFA Members, NFA Member Advisory Committees and NFA's Board, we also considered guidance issued by other regulators and standard setting organizations, including the Federal Financial Institutions Examination Council, the International Organization of Securities Commissions (IOSCO), and the National Institute of Standards and Technology (NIST), and developed requirements consistent with these organizations. NFA's Third-Party Service Provider Interpretive Notice is also consistent with the June 2023 Interagency Guidance on Third-Party Relationships issued by the Board of Governors of the Federal

[3] For example, in November 2018, NFA's Board amended NFA's ISSP Interpretive Notice to adopt incident notification requirements to NFA and further describe the Notice's approval and employee training requirements.

Reserve System, the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency.

Business Continuity and Disaster Recovery Plans

NFA Compliance Rule 2-38 and its related Interpretive Notice entitled *NFA Compliance Rule 2-38: Business Continuity and Disaster Recovery Plan* adopted in 2003 requires FCM Members to have a business continuity and disaster recovery plan (BCDR). The Interpretive Notice details the practices of an acceptable BCDR plan. NFA Compliance Rule 2-49 adopted in 2013 (incorporating CFTC Regulation 23.603) has similar requirements for SDs. Over the years, NFA's BCDR requirements and our Members BCDR plans have been tested by hurricanes, wildfires and a global pandemic, and our BCDR requirements have stood firm.

The Commission's Proposed Rulemaking is Prescriptive and May Cause Conflicts with FCM and SD Existing Frameworks

NFA believes that the three-prong operational resilience requirements we have in place are currently appropriate for NFA Member FCMs and SDs. NFA's requirements are principles based and while they impose certain minimum requirements, they also permit each FCM and SD to develop specific policies and procedures that are appropriate given differences in their type, size and complexity of business operations, including but not limited to their customers and counterparties, markets and products traded and the access provided to trading venues and other industry participants. Our approach is essential to ensuring that FCMs and SDs adopt programs that have a minimum level of necessary safeguards and additional protections that meet their specific needs.

NFA appreciates that the Commission in developing its proposed ORF considered requirements imposed on FCMs and SDs by other regulators, including NFA and prudential regulators. Further, we understand that the Commission's objective in proposing the ORF's requirements was, in part, to build upon and be generally consistent with other regulators' requirements, including NFA. Our own experience over the years adopting the components of the Commission's proposed ORF found that fulfilling this objective can be challenging.

Upon review of the Commission's proposed ORF, NFA is concerned that the Commission's proposed ORF is not generally consistent with NFA's and presumably other domestic and non-US regulators' requirements in key parts of each of the operational resilience areas. This lack of consistency is largely driven by the proposed ORF's prescriptiveness and detail in certain areas, which NFA believes is incompatible with a principles-based approach and does not produce significant regulatory benefits. In short, as for NFA alone, if FCM and SD Members have adopted programs to meet our years-old operational resilience requirements, they would not comply with the CFTC's proposed ORF's more prescriptive requirements.

Some examples of proposed requirements that NFA believes are too prescriptive and would force FCM and SD Members to revise their current NFA compliant program include:

Approval. NFA's ISSP Interpretive Notice permits an FCM and SD Member to meet its obligations through participation in a consolidated entity ISSP as long as a senior official who is a listed principal of the Member approves in writing that the consolidated entity program's policies and procedures *are appropriate for the Member's information security risk.* The Commission's rule also permits an FCM or SD to rely on a consolidated entity program but requires a senior officer, oversight body or senior level official to attest that the consolidated entity program *meets the requirements of the CFTC's rule.*[4]

Risk Assessment. NFA's ISSP Interpretive Notice requires an FCM and SD Member to assess and prioritize the risks associated with the use of information technology systems, identify significant internal and external threats and deploy safeguards to manage those risks and threats. NFA's Third Party Interpretive Notice requires an FCM and SD Member to assess the risk of outsourcing a regulatory function and determine whether it is appropriate to do so. If the Member determines it is appropriate to outsource despite the risks posed, it must conduct onboarding due diligence and ongoing monitoring to determine the ability of the third-party service provider to carry out the function properly. While the Commission's rule contains similar risk assessment requirements, it also requires FCMs and SDs to establish formal risk appetite and risk tolerance limits for each risk area.

Notifications. NFA's ISSP Interpretive Notice notification requirements are more narrowly tailored. NFA's Notice requires a Member to notify NFA promptly of a cybersecurity incident related to the Member's commodity interest business if it involves any loss of customer or counterparty funds; any loss of a Member's own capital; or the Member providing notice to customers or counterparties under state or federal law. The Commission's rule requires notification for any incident that adversely impacts or is reasonably likely to adversely impact the FCM's or SD's information and technology security, the ability to continue business activities or the assets or positions of its counterparty or customer. While NFA's requirements rely on the notification provisions imposed by state law, the Commission's rule contains customer and counterparty notification requirements broadly defined to include any incident that is reasonably likely to have adversely affected the confidentiality or integrity of the counterparty's or customer's covered information, assets or positions.

Potential Safeguards. NFA's ISSP Interpretive Notice requires FCM and SD Members to document and describe in their ISSPs the safeguards deployed in light of identified and prioritized threats and vulnerabilities. The Notice provides Members

---

[4] NFA believes this requirement is particularly concerning because it may not be possible for an enterprise program, which may be subject to multiple regulators, to meet the CFTC's proposed requirements. Therefore, a consolidated entity may need to create a separate ORF strictly for compliance with the CFTC's requirements for its registered FCM or SD, which increases operational complexity and potentially weakens the overall risk framework by adding additional layers of requirements within a consolidated entity.

with flexibility and includes examples of safeguards that Members *may* want to adopt. The Commission's proposed rule specifies a list of controls that all SDs and FCMs *must* consider. Importantly, the preamble suggests that an FCM and SD must document why it does not implement a specific control, a requirement that is inconsistent with NFA's Notice and potentially inserts unnecessary litigation risk into a firm's risk assessment and mitigation practices.

Third-Party Vendor Coverage. NFA's Third-Party Vendor Interpretive Notice applies to vendors that perform functions to assist an FCM or SD Member in fulfilling its regulatory obligations that address NFA and/or CFTC requirements. The Commission's rule sweeps much broader and applies to all third-party relationships of an FCM or SD. Presumably, the Commission's rule would apply to third party vendors (*e.g.*, human resource benefits) that are only peripherally related to a firm's regulated activities without any corresponding regulatory benefit. Moreover, the Commission's proposal includes an Appendix A, which purportedly provides *Guidance on Third-Party Relationship Programs*. The multi-paged Appendix A contains extremely prescriptive requirements in describing factors, actions and strategies for FCMs and SDs to consider in preparing and implementing third-party relationship programs. Further, the due diligence considerations are unnecessarily overbroad and/or may be unattainable (*e.g.,* history of disruptions, incident and BCDR plans, informal industry discussions, internal performance metrics).

Role of Chief Compliance Officer. NFA Compliance Rule 2-9 places a continuing responsibility on every Member to diligently supervise operations, and NFA's ISSP Interpretive Notice requires, as applicable, that sufficient information about a Member's ISSP be provided to its Board of Directors (or similar governing body, committee or delegate thereof) to enable it to monitor the firm's information security efforts. In addition, a Member's incident response plan should consider internal communication and escalation procedures, as well as the creation of an incident response team. While the Commission's proposed regulation includes similar requirements, it also requires that an FCM or SD timely report to its CCO any incident and the results of testing the firm's ORF. The Commission's preamble states that this reporting mechanism allows a CCO to act upon the information to improve compliance and the ORF's overall effectiveness. NFA is concerned that the Commission is expanding a CCO's responsibilities to a highly technical area in which a CCO lacks the critical skills and expertise to either make improvements or even understand the remediation required in the event of an immediate cyber or operational crisis.

Above are just a few examples of areas that the Commission's prescriptive requirements do not align with NFA's current requirements. We are also concerned that the Commission's proposal contains components that are inconsistent with other financial regulators, which NFA spent considerable time evaluating to ensure consistency with our adopted requirements.

The Commission Should Consider Using NFA's Existing Framework to Achieve its Objective

Given the significant risks and adverse impacts associated with operational risks, NFA believes that the Commission should have CFTC-specific requirements that explicitly address cybersecurity and third-party risks and BCDR plans. CFTC-specific ORF requirements will assist the Commission in fulfilling its regulatory oversight obligations and strengthen the Commission's ability to address systemic risks and safeguard customer and counterparty assets. NFA believes, however, that the Commission could achieve its objective without adopting ORF requirements that are unnecessarily prescriptive in nature and may not materially align with other financial regulators, including NFA. Our approach, as outlined below, would continue to mitigate the risks in the ORF's three areas by having the Commission leverage NFA's existing framework's specific requirements.

Specifically, NFA recommends respectfully that the Commission adopt a principles-based requirement that incorporates NFA's ISSP Interpretive Notice, Third-Party Vendor Interpretive Notice and existing NFA and CFTC BCDR requirements. NFA notes that the Commission's proposed rulemaking is replete with references to NFA's various operational resilience requirements and cites no examples of areas in which NFA's requirements are either deficient or require changes. To accomplish this recommendation's result, the Commission could adopt, as slightly amended below, currently proposed Regulation 1.13(b) for FCMs and Regulation 23.603(b) for SDs, along with a provision therein that provides an FCM or SD must further comply with the information system security, third-party vendor and BCDR requirements of a registered futures association (RFA) for which it is a Member. For example, Regulation 1.13 would read as follows:

§1.13 Operational Resilience Framework for Futures Commission Merchants

(a) Each futures commission merchant shall establish, document, implement, and maintain an Operational Resilience Framework reasonably designed to identify, monitor, manage and assess risk relating to:
  (i) information and technology security;
  (ii) third-party relationships; and
  (iii) emergencies or other significant disruptions to the continuity of normal business operations as a futures commission merchant.

(b) The Operational Resilience Framework shall include an information and technology security program, a third-party relationship program and a business continuity and disaster recovery plan. Each component program or plan shall be supported by written policies and procedures.

(c) The Operational Resilience Framework shall follow generally accepted standards and best practices appropriate to the nature, size, scope and complexity and risk profile of its business activities as a futures commission merchant.

(d) The Operational Resilience Framework must at a minimum comply with applicable requirements of a registered futures association of which the futures commission merchant is a member.

This recommended alternative has several advantages. First, the Commission will have CFTC-specific requirements in place to explicitly address cybersecurity and third-party risks and BCDR plans. Further, the CFTC could deem any FCM or SD that was not in compliance with NFA's requirements not in compliance with the Commission's requirements. Therefore, the Commission enhances its ability to fulfill its regulatory oversight obligations and ensure that FCMs and SDs have actionable plans in place designed to address operational risk.

Second, given the evolving and complex security and third-party vendor risks and threats, NFA expects that changes to any ORF requirement will be necessary. In evaluating and adopting changes to an ORF, NFA can act quickly, often in a matter of months, to implement new rules or amend current requirements—self-regulatory organizations are not constrained by the federal rulemaking process. Therefore, if the Commission's ORF leverages NFA's requirements, the Commission can ensure that any specific ORF requirements applicable to FCMs and SDs can be promptly adapted to evolving risks and threats and remain fit for purpose.

Third, this alternative recognizes that NFA Member FCMs and SDs have been subject to NFA's requirements for several years and have programs in place to fully comply. As a result, the Commission will be able to implement its new requirements much sooner than if they had to provide FCMs and SDs sufficient time to review and appropriately modify existing programs. Moreover, to the extent the Commission believes NFA's current ORF requirements should be supplemented to adequately address a specific risk(s), then we are willing to engage in a dialogue with Commission staff and NFA Member FCMs and SDs to determine what changes are appropriate to mitigate the risk(s).

Our recommended approach is entirely consistent with ones taken by the Commission in several other regulatory areas. While not an exhaustive list, the Commission has proceeded in a similar manner in the areas identified below.

Anti-Money Laundering. CFTC Regulation 42.2 requires FCMs and IBs to have an AML program that complies with the regulations imposed by the Department of Treasury (Treasury) and with 31 USC 5318(h), as well as with a jointly promulgated regulation by Treasury and the CFTC that requires FCMs and IBs to have a customer identification program (CIP) as part of their AML program. 31 CFR 103.120, which outlines the AML program requirements for financial institutions regulated by a Federal functional regulator (which includes FCMs and IBs, which are regulated by the CFTC), specifically provides that a financial institution will be deemed in compliance with the AML program requirements in 31 USC 5318(h) if the financial institution (which includes FCMs and IBs) complies with the applicable regulation of its federal functional regulator (which is the CFTC for FCMs and IBs), the financial institution implements a program that complies with the requirements of its self-regulatory organization (*i.e.*, NFA) and those requirements were approved by the federal functional regulator. Moreover, when

the Commission in conjunction with Treasury adopted the CIP rule for FCMs and IBs, the Commission acknowledged in the preamble that NFA sets forth the minimum requirements for an FCM's and IB's AML program.[5]

Capital Requirements. The Commission's capital requirements for FCMs and IBs (CFTC Regulation 1.17), RFEDs (CFTC Regulation 5.7) and SDs (CFTC Regulation 23.101) require these entities to comply with the capital requirement of an RFA when the RFA's requirement is greater than the CFTC's requirement.

RFED Security Deposits. CFTC Regulation 5.9 requires retail foreign exchange dealers to collect and maintain security deposits for retail forex transactions based on the notional value of the currency pair. A security deposit's amount is lower if the currency pair is a major currency, and Regulation 5.9 provides that an RFA designates which currencies are major currencies.

PQRs/PRs. CFTC Regulation 4.27 permits CPOs to file NFA Form PQR and CTAs to file NFA Form PR in lieu of the Commission's required report.

Pool Break-Even Points. CFTC Regulation 4.24 requires a CPO's disclosure document to provide a commodity pool's break-even point for investors. CFTC Regulation 4.10 provides that the break-even point is calculated pursuant to the rules promulgated by an RFA.

In each of the above noted areas, NFA submitted the applicable requirement to the Commission for review prior to implementation. Similarly, NFA provided its ISSP Interpretive Notice, the Third-Party Vendor Interpretive Notice and its BCDR requirements for review to the Commission prior to implementation, and we would seek the Commission's review of any future changes to these requirements.

Conclusion

Given today's evolving risks and threats, NFA believes operational resilience requirements should be imposed upon all NFA Member firms, including FCMs and SDs. We fully understand the Commission's desire to have CFTC-specific ORF requirements and direct oversight of FCMs and SDs to ensure they have actionable plans designed to address operational risks. However, as fully discussed above, NFA requires FCM and SD Members to adopt appropriate programs in each of the three areas contained within the Commission's proposed ORF. Since NFA's requirements are designed to ensure that FCM and SD Members already have actionable plans in place to address the risks associated with these areas, we encourage the Commission to leverage and build upon NFA's existing operational resilience requirements.

Therefore, we recommend respectively that the Commission achieve its ultimate objective by adopting a principles-based rule for FCMs and SDs requiring an operational resilience framework. In addition to adopting a principles-based rule, we recommend that the Commission by rule require FCMs and SDs to comply with NFA's specific requirements in each of these areas. Based upon our discussions with industry

[5] See Customer Identification Programs for FCMs and IBs, 68 Fed. Reg. 25149 at 25152 (May 9, 2003).

participants, we believe FCMs and SDs would be supportive of NFA's recommended approach.

NFA appreciates the opportunity to provide our views on this important proposal, and we support the Commission's efforts to ensure that FCMs and SDs have appropriate ORFs in place designed to address operational resilience. If you have any questions on our letter or would like to more fully discuss our proposed recommendation, please do not hesitate to contact me at cwooding@nfa.futures.org.

Respectfully submitted,

Carol A. Wooding
Senior Vice President
and General Counsel