2024 IAA CONFERENCE: KEY TAKEAWAYS

A CONVERSATION WITH THE SEC DIVISIONS OF EXAMINATIONS AND ENFORCEMENT
Speakers: Nataha Vij Greiner, Corey Schuster, & Gail Bernstein

The Securities and Exchange Commission ("SEC") commenced the session by clarifying that a shift in examination priorities from previous years does not imply scrutiny over previously highlighted areas has stopped. The SEC discussed the framework of an examination, emphasizing that firm engagement streamlines the examination process. Preceding the conclusion of an examination, an exit conference is held, offering an opportunity for firms to address any misconceptions and furnish additional documentation, if warranted, followed by the receipt of a deficiency letter, if applicable.

The discussion included the liability of Chief Compliance Officers ("CCO") in small firms, highlighting a limited number of cases that involved CCO fault. These cases predominantly involved CCOs either misguiding their firms or witnessing wholesale failures. The SEC encouraged Investment Advisers ("IAs") to be aware of risk alerts throughout the year.

Panelists focused on off-channel communications and the use of artificial intelligence ("AI") during examinations. Regarding off-channel communications, IA firms are advised to tailor supervisory procedures to their unique organizational structures. Panelists stated that compliance policies should be enforced, and firms should maintain comprehensive records of any disciplinary actions taken, highlighting the critical importance of record-keeping.

The SEC also emphasized heightened scrutiny surrounding the integration of AI within financial firms. The SEC emphasized the importance of firms to disclose their use of AI technologies. Enforcement efforts emphasize the necessity for firms to implement controls to market their AI capabilities accurately and to establish clear and comprehensive policies and procedures. These measures aim to ensure adherence to regulatory standards and promote integrity and accountability in AI-driven financial practices.

Helpful Links:
- *Observations from Examinations of Newly Registered Advisers*
- *Investment Advisers: Assessing Risks, Scoping Examinations, and Requesting Documents*

AI, BEHAVIORAL PROMPTS, AND OTHER EMERGING TECHNOLOGY – RISK GOVERNANCE AND CONFLICTS MANAGEMENT
Speakers: Ken Klass, Seth Rosenbloom, Danielle Nicholson Smith, and Sanjay Lamba

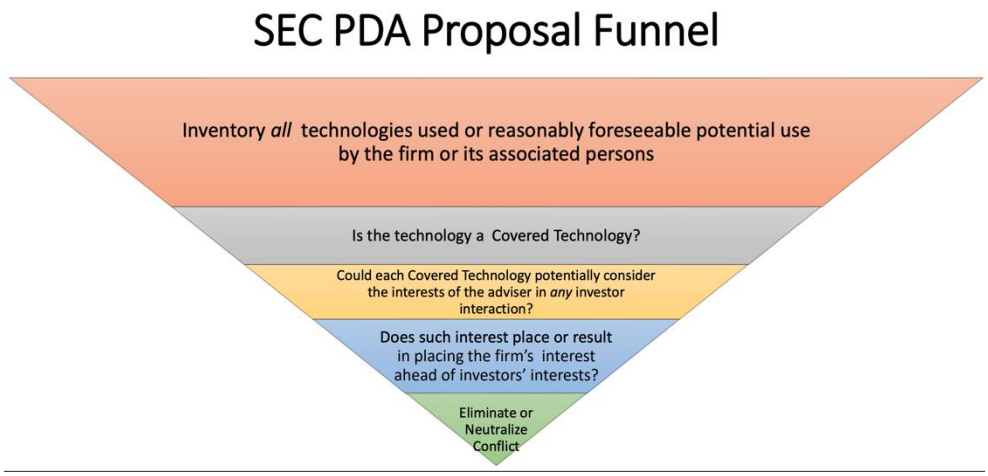
The Predictive Data Analytics ("PDA") proposal entails several key requirements and considerations:

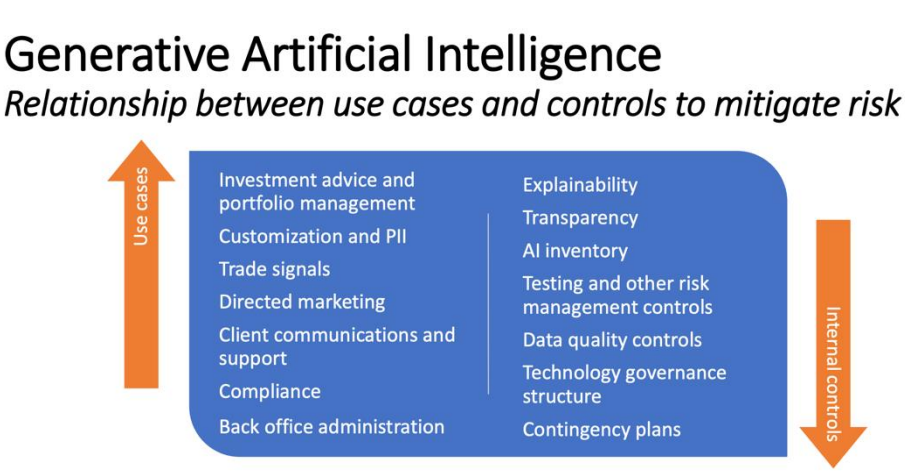
1. Conflict of Interest Mitigation: Firms must address conflicts of interest arising from their use of covered technologies in investor interactions, ensuring investor interests are prioritized over the firm or its associated person's interests.

2. Written Policies and Procedures: Firms engaging in investor interactions via covered technology platforms must establish written policies and procedures to prevent violations and to achieve compliance with the proposed rule.

3. Recordkeeping Obligations: Firms are mandated to maintain records relevant to the proposed rules. This includes documentation regarding the use of covered technologies in investor interactions, promoting transparency, and facilitating accountability in compliance efforts.

However, the IAA requested that the SEC's PDA proposal be withdrawn. The IAA believes the proposal could replace fiduciary duty principles with unproven regulations, impose burdensome compliance obligations, stifle innovation, and underestimate economic impacts, especially within smaller advisers.





Source: IAA Conference PowerPoint

SMALLER ADVISERS: MAKING THE MOST OF COMPLIANCE
Speakers: Bliss Bernal, Katie McGinley, Erik Olsen and Patrick D. Hayes

This session focused on best practices for smaller advisers and focused on several areas of importance including risk assessments, compliance testing, disclosures, annual review, and technology and resources. The panelists made helpful suggestions to assist compliance in the day-to-day operation of an adviser. Unique recommendations included the following:

- Conduct risk assessments annually to understand gaps. A risk assessment can run parallel to an annual review and ultimately assist with the annual review. While conducting a risk assessment, it is important to understand if there are fail-safes in place and the ultimate impact of the largest risks. While conducting risk assessments, it can be extremely helpful to speak with employees to gain insight into other perspectives and solutions.
- Ongoing, day-to-day compliance testing requires multiple controls. For example, disclosures are not stagnant documents, they require ongoing review, and, if applicable, amendment. Due to the influx of rules, it is helpful to maintain an updated list that outlines the areas that require change and the associated control. This type of checklist can be helpful to ensure the compliance team understands its responsibilities.
- Electronic communications are a trending topic, and advisers should be prepared for the SEC to ask questions during exams.
- When making updates to Form ADV, Form CRS, or an Investment Management Agreement, it is important to update the adviser's policies and procedures as well. Disclosures and policies should be aligned.

INFO SEC: DATA PRIVACY AND REGULATION S-P
Speakers: Davie Baccei, Ryan Burch, Wei Zhao, and Jacob Prudhomme

The speakers discussed three (3) critical challenges concerning data protection:

(1) Notification
(2) Data Protection, and
(3) Third-Party Risk Management

The first challenge, *Notification*, pertains to promptly informing supervisors of any data breach incidents. Comprehensive training sessions must be conducted for all associated persons to recognize and report breaches. Associated persons should not assume the responsibility of diagnosing breaches independently. Instead, a cautious approach to promptly identify potential breaches is recommended. Associated persons need explicit guidelines on when and how to disclose breaches to ensure timely and appropriate notifications. When it comes to *Data Protection*, the key is to establish a well-defined protocol for breach response procedures, including designated points of contact and specific response actions. With *Third-Party Risk Management*, firms need to maintain an open dialogue with vendors to promptly address any breaches and implement an action plan.

The speakers recommended the establishment of dedicated teams tasked with ensuring regulatory compliance within both the firm and vendors, thereby facilitating streamlined management, response, and recovery processes. When formulating data protection plans, key considerations include managing personally identifiable information ("PII") across systems. Implementing robust measures such as encryption, multifactor authentication, and password protection are simple yet effective strategies for safeguarding PII.

MARKETING RULE COMPLIANCE: BEST PRACTICES
Speakers: Robert Shapiro, Alejandro Staroselski, Karyn D. Vincent and Michael McGrath

Panelists in this session discussed the marketing rule. Since the implementation date, the updated marketing rule has brought about many questions. One area that is relatively new with the onset of social media, is paid influencers marketing investments. It is critical to conduct due diligence on any paid influencers to understand all the adviser's partners. It is also important to ensure the legal department understands who partners with the adviser.

Another area the panelists focused on was the substantiation requirement. Advisers should always ensure that advertisements have a reasonable basis of fact. Controls that could be implemented include a whitelist of verified sources. It is imperative to maintain documentation to exemplify the basis of fact, cite websites, and ask the question: "Would a reasonable person assume this as fact?"

OFF-CHANNEL COMMUNICATIONS
Speakers: C. Dabney O'Riordan, Adam Aderton, Mukya Porter, Adam Reback

As of last year, there were 16 cases related to the failure to preserve records due to the use of personal devices, text messages, WhatsApp, and personal email accounts. Since then, the SEC has announced 23 additional settled orders involving broker-dealers, dual registrants, and affiliated advisers. Penalties ranged from $1.25 million to $35 million within the last seven months.

Key issues for advisers include ensuring compliance with regulations such as Advisers Act Rule 204-2(a)(7), which mandates the preservation of all written communications related to recommendations and advice. For example, a case involving Guggenheim Securities LLC, highlighted the importance of capturing off-channel text exchanges discussing securities transactions. Advisers must draft policies and procedures that are firm specific.

The panelists gave examples of best practices to ensure compliance with books and records requirements:

- Senior management must understand and abide by electronic communication policies.
- Policies should outline the repercussions for someone who violates the electronic communications policy.
- If an associated person is utilizing two phones, email can be removed as a capability from a personal phone.
- Ensure there is consistency to repercussions for violations and violation explanations are maintained.
- Social Media:
    - Ensure there are policies regarding social media permissions and prohibitions.
    - Implement social media attestations and conduct quarterly screenings.

Looking ahead, the SEC may pursue standalone cases against investment advisers without affiliated brokers through its Division of Enforcement. The Division of Examinations no longer considers this an examination priority. These developments suggest ongoing regulatory scrutiny and potential changes in compliance requirements for investment advisers.

ETHICS FOR ADVISERS: COMPLIANCE WITH FIDUCIARY STANDARDS – PART 1
Speakers: Max Mejiborsky, Kim Versace, Steven A. Yadegari, A. Valerie Mirko

The Investment Adviser Standard of Conduct, as outlined by the SEC, encompasses two main components: the Duty of Care and the Duty of Loyalty. The Duty of Care includes providing advice in the client's best interest, seeking best execution, and offering advice and monitoring services. The Duty of Loyalty emphasizes prioritizing clients' interests, disclosing material facts, and disclosing conflicts of interest with considerations for mitigation or elimination.

One area the panelists focused on was the practical challenges that arise in identifying Access Persons, particularly regarding consultants and determining beneficial ownership of securities held by immediate family members. Tailoring Codes of Ethics to align with the firm's business model is essential, avoiding the adoption of generic or off-the-shelf procedures. Preclearance requirements for certain transactions, such as IPOs or private placements, necessitate a risk-based approach, and consideration should be given to recordkeeping practices and software implementation. Escalation procedures for violations, including penalties and actions for C-suite violations, also require careful consideration and planning.

Panelists offered several best practices for administering and enforcing policies:

- Ensure the Code of Ethics includes a Whistleblower Policy.
- Clearly define Access Persons – this is something the SEC could ask on your next exam.
- Consider an escalation policy for violations of the Code of Ethics.
- Consider handling internal issues with outside counsel.

CYBERSECURITY FOR SMALLER AND MEDIUM FIRMS
Speakers: Gordon Eng, Christian Kelly, Rachel Kuo and Joseph Mannon

The increasing concern surrounding cybersecurity is driven by the likelihood of smaller and medium-sized financial firms becoming more attractive targets for Threat Actors compared to larger institutions with substantial cybersecurity budgets and resources. Cybersecurity breaches pose an existential threat to firms, potentially resulting in significant financial and operational harm, reputational damage, and loss of client confidence.

The proposed Cybersecurity Rule aims to enhance cybersecurity risk management for investment advisers. The rule requires these entities to adopt and implement written cybersecurity policies and procedures, promptly report significant cybersecurity incidents to the SEC, and maintain confidentiality regarding such incidents to facilitate mitigation efforts.

The proposed rule defines a significant cybersecurity incident as one that disrupts critical operations or leads to unauthorized access to sensitive information, resulting in substantial harm to the firm or its clients. The SEC's concerns stem from observations of insufficient cybersecurity preparedness among certain advisers and funds, emphasizing the importance of providing investors with adequate cybersecurity-related information.

If enacted, the proposed Cybersecurity Rule would be under the Investment Advisers Act and Securities Exchange Act, reinforcing advisers' fiduciary duty to protect client interests from cybersecurity risks. Firms are reminded of their obligation to minimize operational risks and safeguard client information under their fiduciary obligations.

The panelists also offered best practices to enhance cyber programs:

- Conduct tabletop exercises to test incident response plans.
- Consider cybersecurity insurance.
- Review vendor contracts on an ongoing basis and request SOC 2 reports.
- Rule of thumb: The smaller the vendor, the bigger the due diligence to identify possible issues.

USE OF AI IN INVESTING AND COMPLIANCE
Speakers: Max Gokhman & James E. Thomas

Mr. Gokhman discussed the many advantages and drawbacks associated with incorporating AI within the financial services industry. Notably, AI possesses the capability to analyze extensive datasets, identify inconsistencies, and highlight suspicious trading activities. Gokhman emphasized that tasks typically performed by junior analysts could be effectively executed by AI, with additional human review necessary to verify the accuracy of AI-generated outputs, minimizing potential miscommunications or input errors. He analogized AI to a puppy, illustrating its eagerness to excel yet susceptibility to distractions. Just as a puppy might chase a stick only to be sidetracked by a passing squirrel, AI may tend to deviate from its primary task in pursuit of alternative solutions. Many ethical concerns surrounding AI were discussed, particularly the potential for bad actors to manipulate data intentionally. Gokhman cautioned that unmonitored input data could significantly impact the reliability of AI-generated outcomes, emphasizing the necessity for oversight.

While acknowledging that AI still has considerable room for improvement, it was widely acknowledged throughout the conference that discussions surrounding its implementation will increasingly shift from "whether to use it" to "how best to utilize it" in the coming years.

OUTSOURCING AND VENDOR DUE DILIGENCE: SMALLER AND MEDIUM FIRMS
Speakers: Joe LaFemina, Gretchen Lee, Jyothi San Juan, & Karen A. Aspinall

The presentation outlined the fiduciary obligations of investment advisers, emphasizing the duty of care to act in the client's best interest and the duty of loyalty to prevent, mitigate, and disclose conflicts. These standards extend not only to supervised persons but also to third parties performing certain functions for the adviser. Outsourcing is prominent due to technical expertise, cost-effectiveness, and the lack of appropriate personnel, leading to the proposed Rule 206(4)-11.

Proposed Rule 206(4)-11 establishes a framework for service provider oversight, emphasizing reasonable due diligence before engaging a service provider and periodic monitoring of their performance. Due diligence processes include assessing services, risk mitigation, capacity evaluation, and recordkeeping assurance. Post-engagement due diligence involves ongoing monitoring and assessing the appropriateness of continuing outsourcing. Methods include tailored approaches, risk assessments, standard reports, onsite meetings, and technology demonstrations. The Rule, in principle, is designed to proactively address conflicts of interest if firms undertake preventive measures.

Panelists offered helpful insight on how to conduct effective vendor due diligence:

- Conduct a risk assessment.
- Collect SOC 2 reports.
- Ask for an on-site meeting with outsourced vendors.