Proskauer

Fund Manager Securities and Compliance

June 2023

This Webinar aims to provide some practical advice regarding Generative AI ("Gen AI") and the issues its presents for private fund managers related to securities law and compliance. To the presenters, this is an dynamic time and will perhaps be thought of years from now as the inflexion point where generative AI launched into the securities and compliance world. There is the potential for GAI to be helpful in compliance as a tool to analyze large amounts of data, and the potential for GAI to be used in the investment making process. Generally speaking, the presenters stressed that while this is not the time for private fund managers to "go crazy" over generative AI and its potential securities law and compliance issues, it is prudent for firms of all types to start thinking seriously about GAI and its potential use cases and associated legal risks and begin to offer internal guidance to employees and thereafter assemble a team to start to craft general policies and procedures that can be shaped going forward. As the presenters stated, it's important to get ahead of these issues, yet avoid the hype, and instead take a level-headed, prudent approach to examining what an organization is doing with AI and how to address risk.

There are different types of generative AI available for use: publicly available (e.g., GAI tools available online and used by the general public), GAI used under an enterprise agreement, and GAI provided under a bespoke enterprise agreement for particular use cases that gives the organization more of a private "sandbox" to experiment in and offers protections and controls over the inputted data. From a confidentiality perspective, the latter bespoke GAI arrangement is preferred, according to the presenters. It should also be noted that the GAI space is changing quickly and what's right for an entity today may need to be reevaluated in a few months.

The presenters outlined three main components that fund managers should think about when addressing GAI usage:

1. **Use**: How is it going to be used in your organization? How is it already being used? How might it be used in the future?

Depending on the type of shop, firms should recognize that there are a variety of ways to use GAI, and undoubtedly, employees have already been playing around with ChatGPT and other GAI products. The presenters suggested that organizations speak with employees about potential use cases and then determine if the firm is interested in an enterprise license or a bespoke license with a provider (that would allow internal and proprietary data be used to train and fine-tune the GAI model).

The presenters noted that considerations of GAI use necessarily involve issues of confidentiality and data security. It's important for organizations to understand that GAI products, such as ChatGPT, have settings that allow users to opt-out of having inputs used to train a public GAI product. Moreover, every organization should be concerned about the potential for chat histories to be disclosed or leaked due to a data breach, with the potential being far worse if inputs contain confidential or sensitive information. Thus, the presenters stressed that it's important to consider how a GAI is being used: is it more for external research, akin to a Google search, or more of an internal tool and whether inputs contain internal material or just queries on public information.

2. **GAI Team**. An organization should assemble your team to address AI policies and training and set rules. The team should consist of the Chief Compliance Office and other stakeholders at the firm (e.g., research, analysts, technology and legal) and be concerned with drafting the protective email that should be sent company-wide to establish basic guidance and thereafter with developing policies and procedures surrounding GAI. The presenters noted that a big aspect of a GAI policy should be confidentiality, especially inputs to any public GAI platforms that might use or store such inputted data, as well as GAI inaccuracies or "hallucinations," a reality that mandates output being double-checked by an employee.
3. **Develop guidelines**. Once in place, the team can assess usage needs and craft procedures or guidelines to address risk.

Thereafter, the presenters addressed specific issues that fund managers have been asking, including:

Should firms be entering into long-term enterprise agreements with AI providers?

The presenters replied that a long-term agreement with a GAI provider may not necessarily be a good idea for all organizations at this point, given that future advances in technology or the market are unknown at this point and the first developer to market may not be the "winner."

What are some of the securities law concerns for asset managers that involve using GAI in the investment making process?

The majority of questions the presenters have received from clients involve the use of GAI to generate alpha in the investment-making process.

The presenters noted that one of the key issues is confidentiality. The first question to ask is: Are you using an external-facing, free GAI program or an internal-facing, enterprise model that is being trained on your own data? The type of GAI product will inform the thinking about issues surrounding material nonpublic information (MNPI) and insider trading concerns and whether an entity has adequate policies and procedures to adequately address risks involving MNPI. As the presenters noted, if a firm uses a public version of ChatGPT that trains on public information scraped from the web, there is necessarily a low risk of any securities law issues in the output; on the other hand, if a firm possesses MNPI or other sensitive information, it may want to be careful about inputting that type of information into an internal GAI product that trains on internal data, as this may still present information barrier issues. For example, if there is a piece of information is restricted within the firm, then that piece of information should not be inputted into a GAI product (without prior approval), as that information could presumably become part of the corpus of data used by the model, with the potential that it "infects" future outputs presented by other team members.

Can an organization input computer code into GAI?

There have been reports of issues with sensitive computer code being inputted into ChatGPT by employees of major companies, so this issue is now on the radar for compliance teams. The presenters replied that the answer depends on whether it is a public GAI product or bespoke GAI product. Using the most prudence, the panelists noted that if a firm had a bespoke agreement and had its own "sandbox" and sufficient guardrails to prevent outside access, then inserting sensitive code might be safe enough with adequate data security precautions.

Can an organization input large alternative data sets into a GAI product?

The presenters stated that entering licensed data into a public GAI product should not be done, but regarding an enterprise or bespoke system, one would need to first check vendor agreements to ensure it is permissible. The presenters noted that it would be prudent to consider this issue in agreements going forward and if necessary, renegotiate existing agreements.

Are queries inputted into a GAI product "communications" under the Investment Advisors Act recordkeeping provisions?

In the presenter's view, such queries are probably not "communications" under the Act, as communications would generally be defined as between two humans; still, it's wise to still proceed cautiously.

If the firm is using GAI somewhere in its investment process, are there are disclosure issues and separate risk factors?

Yes. The presenters advised that if a firm is telling investors or prospective investors that it is using GAI and has GAI content in marketing materials, or going to do so in the future, then it would need to have required disclosures. Still, the presenters cautioned that most firms are not yet using GAI as a material part of their business or selling it to the public as such and that GAI is not materially impacting the investment process within such firms. However, when a firm's use of GAI starts to become a material part of the investment making process, then appropriate disclosures would have to be made.

From a compliance standpoint, are there any business records coming out of GAI?

The presenters stated that, in general, a firm need not keep GAI queries and outputs under recordkeeping policies, as this is not the type of records covered under the Investment Advisors Act, except in special cases. However, the presenters asked: Are there situations where you should probably keep it? Yes. For example, the presenters noted that if the queries and the output go into the investment process, a firm may want to keep the chat histories to consult in the future if a regulator in the future ever asks a question about a particular investment decision or process.

Final Takeaways

The presenters closed the Webinar with some final points:

- Form a GAI team with key stakeholders
- If a firm has not already done so, it should send a protective email to everyone in the organization with initial guidance on GAI use that covers such things as: the importance of maintaining confidentiality of sensitive data (e.g., MNPI, sensitive code, personally identifiable information, protected health information, etc.) when using GAI platforms; ensuring GAI team members are available to answer questions in person or over the phone; stating which platforms should be blocked; and informing employees that policies and procedures may be forthcoming.
- The GAI team should then outline a firm's use cases and what platforms will be considered for use by the firm, and the related risks of each platform. Such platform usage and risks will necessarily evolve over time and policies need to be flexible to address change. The team might also address the level of due diligence that might be required before the firm enters into an enterprise agreement with a GAI provider and what points would be important when a firm negotiates a bespoke license with a GAI provider.
- The GAI team should also document internal use of GAI program and outline any necessary training for employees on GAI programs (particularly with respect to confidentiality of proprietary information and licensed alternative data).
- A GAI policy should address how the firm will respond to investor inquiries about GAI use and when the firm needs to disclose GAI usage that affects investment making decisions in marketing materials.

Related Professionals

- **Joshua M. Newville**
  Partner