

CHATGPT AND THE COMPLIANCE FUNCTION

Cutting through the clutter



David Choi
Nikunj Khutti
Allen Meyer

INTRODUCTION

ChatGPT has been celebrated for its ability to generate human-like text but concerns about data privacy and accuracy have tempered the hype. As a result, many companies have already prohibited its use in corporate settings. ChatGPT may not be ready for use in compliance functions where security and reliability are essential, but it is just one of many examples of language AI-enabled solutions that compliance professionals should be enthusiastic about. This technology ultimately will offer real opportunities to improve the effectiveness of compliance functions, if a considered analysis of its limitations are taken into account. As new language AI-enabled solutions are developed and introduced securely into corporate environments, compliance professionals will be excited to see solutions that can generate human-like text and effectively analyze large sets of text-heavy data including policies, emails, and instant messages, helping with everyday compliance activities in a meaningful way.

Language AI-enabled solutions have the potential to automate many of the highly manual and inefficient activities that compliance professionals grapple with daily. Language AI-enabled solutions are particularly useful for routine compliance tasks like writing initial drafts of documents or analyzing emails for potential policy/regulatory concerns, allowing compliance professionals to focus on more analytically oriented activities (for example, risk assessments). However, language AI-enabled solutions cannot “think” the way a human does and they should not replace the judgement of qualified compliance professionals.

The use cases in compliance for language AI-based solutions are exciting but in highly regulated and technically complex fields like compliance, there are important limitations to consider. Specifically, these solutions sometimes provide inaccurate, superficial or incomplete responses or even provide different responses to the same question making it unwise to rely on answers without stringent oversight. In addition, the risks of misuse or data privacy are serious barriers to implementation.

Compliance professionals today should be excited by the potential of language AI-based solutions but need to remain cautious with information that is shared with these tools and how these tools are governed in the bank. Language AI-enabled tools have the potential to help Compliance professionals but they are likely best for specific use cases rather than a one-size-fits-all approach.

- Language AI-enabled tools can be helpful in generating drafts (such as procedures or training materials) or summarizing and analyzing large volumes of text data to jump-start compliance processes
- Language AI-enabled tools cannot be relied upon for decisions and cannot replace people in compliance functions. Compliance professionals must demonstrate appropriate oversight and develop governance for responsible AI
- Using language AI-enabled tools for compliance processes will not eliminate existing tools and practices any time soon. Language AI-enabled tools could be good for prioritizing processes with technologies that are already in place to manage risks but should not be relied on fully since they are still error-prone

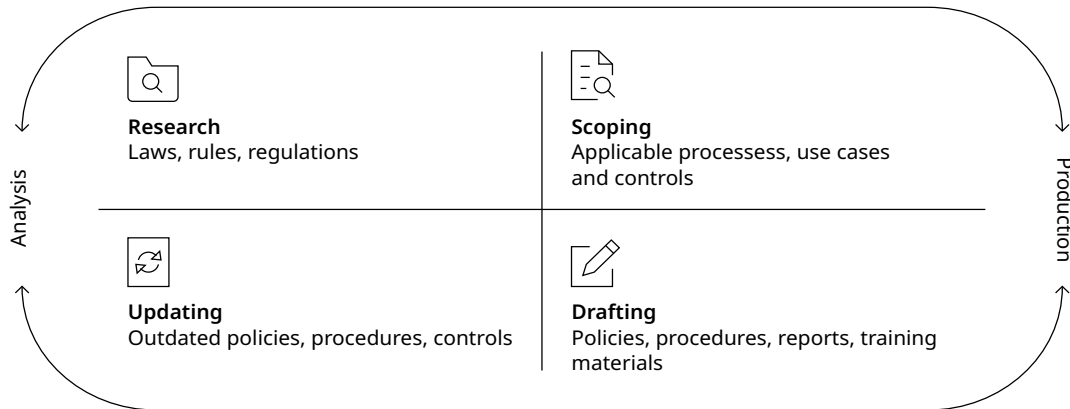
ILLUSTRATIVE USE CASES FOR LANGUAGE AI-ENABLED TOOLS IN COMPLIANCE

Language AI-enabled tools cannot replicate human thinking but are good at providing, summarizing, and analyzing information that could help compliance professionals in the following ways:

Production: Language AI-enabled tools can produce human-like text, such as emails, reports, training materials, and support language-based tasks. It can also summarize how requirements apply in specific situations prompted by the user

Analysis: Language AI-enabled tools can review large amounts of open-ended text information and consolidate that information into reports using observations or user inputs. A barrier to this usage in compliance is the sharing of confidential information with language AI-enabled tools that gets absorbed into the dataset

Exhibit 1: Uses of language AI-enabled tools in compliance



Source: Oliver Wyman Analysis

Production Use Case
Expediting Routine Compliance Processes

Language AI-enabled tools can enable compliance professionals to quickly summarize information about laws, rules, and regulations, facilitating the production of materials in various ways (Exhibit 1). Whether it be through providing research or outlining rough drafts, these tools can jumpstart the process of creating policies, procedures, and training materials for compliance professionals. Language enabled-AI tools could also identify when materials need updating (for example, when a regulation is amended) and suggest possible changes if they are provided with the firm’s policies, procedures and controls.

While language AI-enabled tools can expedite compliance processes, the level of detail and accuracy in the outputs is mixed and would require diligent Quality Assurance (QA) from compliance professionals. In Exhibit 2, we queried OpenAI’s GPT-3 (text-davinci-003) large language model to draft training materials for traders related to spoofing and it provides a draft outline that covers the high-level points but lacks details, demonstrating how large language models can help with initial drafts but require additional careful review by compliance professionals.

Exhibit 2: Illustrative inputs into training materials using language AI-enabled tools

D

Write a draft training guide for traders on spoofing compliance based on FINRA and SEC guidelines

GPT

Spoofing Compliance Training Guide

Purpose

This training guide is intended to provide a comprehensive overview of FINRA and SEC spoofing compliance guidelines and the related laws, regulations, and guidelines. It will also provide a practical guide to help traders understand and adhere to these standards.

Overview

Spoofing is a form of market manipulation involving the placing of orders to buy or sell securities that are cancelled before execution. By doing so, the trader is able to create the illusion of market demand or supply, and in turn, influence prices in their favor.

FINRA and the SEC have implemented a number of regulations and guidelines to prevent and combat spoofing. This training guide will provide an overview of these regulations and guidelines, as well as a practical guide to help traders identify and comply with these standards.

FINRA and SEC regulations and guidelines

1. FINRA Rule 2010: All FINRA members and associated persons must observe high standards of commercial honor and just and equitable principles of trade. This means that they must conduct their activities in a manner designed to prevent fraud and manipulation
2. FINRA Rule 5290: This rule prohibits FINRA members and associated persons from engaging in any manipulative, deceptive, or other fraudulent activities in connection with the purchase or sale of any security. This includes spoofing and other forms of market manipulation
3. SEC Rule 10a-1: This rule prohibits the use of any manipulative or deceptive device or contrivance in connection with the purchase or sale of any security. This includes spoofing and other forms of market manipulation
4. SEC Regulation SHO: This regulation requires market participants to establish and maintain policies and procedures designed to prevent the execution or display of orders that would be in violation of the SEC's anti-manipulation rules. This includes spoofing and other forms of market manipulation

Practical guide

1. Understand the regulations and guidelines: It is important for traders to understand the FINRA and SEC regulations and guidelines regarding spoofing. They should be familiar with the rules and what activities are prohibited
2. Monitor orders: Traders should monitor their orders and the market for any signs of spoofing or other market manipulation. This includes monitoring for orders that are cancelled shortly after being placed, as well as any suspicious changes in prices or trading volumes
3. Report suspicious activity: If traders suspect that spoofing or other market manipulation is taking place, they should report it to their supervisor or compliance officer

Conclusion

Spoofing is a form of market manipulation that can have serious consequences for both traders and market participants. It is important for traders to understand and comply with FINRA and SEC regulations and guidelines regarding spoofing. This training guide provides an overview of these regulations and guidelines, as well as a practical guide to help traders identify and comply with these standards.

Source: Actual responses from OpenAI GPT-3 API

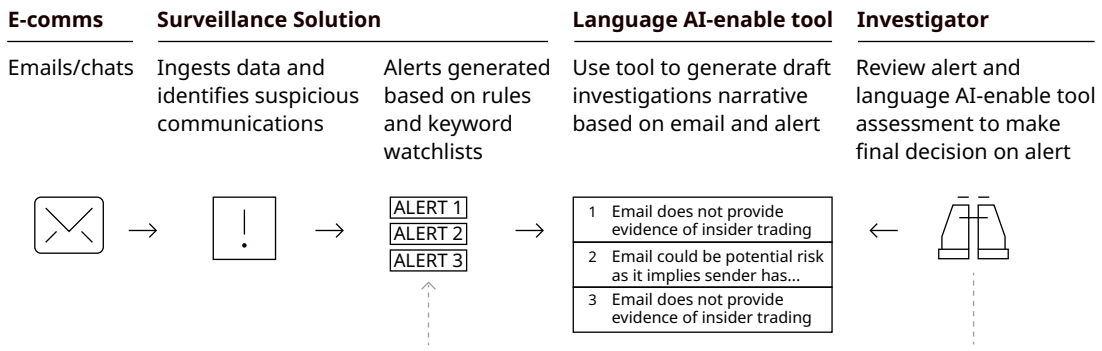
Analysis Use Case

Analyzing Electronic Communications Surveillance Alerts

Language AI-enabled tools can reduce the workload for compliance functions in inefficient areas such as electric communications surveillance where compliance professionals continue to be challenged with high false positive rates. While language AI-enabled tools could eventually surpass currently available surveillance vendor solutions, they are, in the medium term, best suited to work alongside existing surveillance solutions to help compliance professionals make faster decisions on alert investigations.

Exhibit 3 shows how language AI-enabled tools can improve surveillance investigations by generating an initial draft of the case narrative notes based on the email and potentially suspicious behavior. After this, a compliance professional would review the alert and the language AI-enabled tool's draft narrative, and then make the final decision on what to do with the alert, allowing compliance professionals to review alerts more efficiently while still maintaining oversight of the final risk based decisions.

Exhibit 3: Analyzing electronic communications surveillance alerts



Source: Oliver Wyman Analysis

CHALLENGES AND LIMITATIONS

Language AI-enabled tools can improve the processes of compliance teams but, as referenced above, there are substantial challenges with these solutions that limit widespread use in compliance over the near term.

ACCURACY AND COMPLETENESS

Language AI-enabled tools may not always provide accurate or complete answers, despite being trained on large datasets. In some cases, they may generate different responses to the same prompts, which makes them less reliable for compliance. It is also important to note that these tools may have limited training data available. For instance, GPT3 has only been trained on data up to 2021, which means it may not be able to generate answers about events that occurred after that point.

DATA PRIVACY

Language AI-enabled solutions like ChatGPT that are pre-trained on large data sets are currently available through third-party vendors which may limit access in a corporate environment. Companies are already starting to prohibit employees access to ChatGPT due to risks around data privacy and security.

Feeding of confidential information to language AI-enabled tools will require strict controls as to how it can be used in practice. Confidential data exposed to the model may be incorporated into its training and could spur data privacy issues. Firms will need to establish clear boundaries of what is permissible.

While some firms have begun to restrict use of free tools, such as ChatGPT, it may not be enough to squash use among employees as some may turn to using it on personal or unapproved devices. It is becoming increasingly evident that the widespread availability of such tools will require a swift response from firms to advise their employees on acceptable and unacceptable uses to avoid potentially disastrous data breaches and recordkeeping and supervision issues.

COST

Language AI-enabled tools, like ChatGPT, are being offered for free for trial but will have a cost going forward. OpenAI has already launched a paid premium model for ChatGPT for individuals. The cost of using language AI-enabled tools in a corporate environment is not yet clear but given the significant computing power and money invested to train these models, we anticipate that cost could be prohibitive for higher volume processes.

MOVING FORWARD

NEXT STEPS

Language AI-enabled tools are clearly not ready for broad use in compliance and care must be taken in access and oversight. But given the meaningful potential of these tools in compliance, now and in the long term, the CCO should appoint an individual or group (such as the Compliance Analytics or Strategy team) to learn more about language AI-enabled tools and conduct well-controlled experiments to determine how they can be used effectively for common compliance tasks. Only after thorough testing and robust human oversight should compliance consider a more widespread implementation of language AI-enabled tools for its activities.

OVERALL OUTLOOK

Compliance professionals should be excited by the potential of language AI-enabled tools to automate highly manual tasks, and as these solutions continue to mature and improve, we can imagine their use in multiple compliance activities. However, as discussed in this paper, there are reliability and privacy challenges that must be addressed before adopting them more broadly in a highly regulated function like compliance. Nevertheless, we believe that as these tools continue to mature, it is imperative for compliance professionals to become proficient in their use as compliance teams using language AI-enabled solutions will be more efficient and effective at managing risk.

Oliver Wyman is a global leader in management consulting. With offices in more than 70 cities across 30 countries, Oliver Wyman combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation. The firm has more than 6,000 professionals around the world who work with clients to optimize their business, improve their operations and risk profile, and accelerate their organizational performance to seize the most attractive opportunities.

For more information, please contact the marketing department by phone at one of the following locations:

Americas
+1 212 541 8100

EMEA
+44 20 7333 8333

Asia Pacific
+65 6510 9700

AUTHORS

David Choi
Partner
david.choi@oliverwyman.com

Nikunj Khutti
Principal
nikunj.khutti@oliverwyman.com

Allen Meyer
Partner
allen.meyer@oliverwyman.com

Special thanks to **Pippa Black, John Lester, Sian Townson, Sara Cotsakis and Jenny Wan** for their contribution in this report.

Copyright ©2023 Oliver Wyman

All rights reserved. This report may not be reproduced or redistributed, in whole or in part, without the written permission of Oliver Wyman and Oliver Wyman accepts no liability whatsoever for the actions of third parties in this respect.

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. The report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. This report may not be sold without the written consent of Oliver Wyman.