

WHITE PAPER

The generative AI phenomenon in anti financial crime: a look under the hood

1.3496

2.5679

3.5290

Table of contents

Generative AI - why now?	3
Criminal exploitation of generative AI:	3
Practical use cases of generative AI in anti financial crime (AFC)	4
Is all generative AI created equal?	4
Understanding the benefits	5
Navigating the potential pitfalls	6
The way forward	7
Awards and accreditations	8

By Charmian Simmons, Financial Crime and Compliance Expert
and Eve Whittaker, Business Solutions Consultant - Financial Crimes

In the ever-evolving financial crime landscape, the emergence of Generative Artificial Intelligence (gen AI) has sparked unprecedented interest. Gen AI's ability to synthesize vast quantities of data, capacity for advanced and nuanced analysis of complex datasets, and rapid learning pace make it incredibly well suited to addressing challenges in the financial crime space. Its untapped potential has catapulted it to the forefront of innovative technologies that are captivating IT professionals and AML compliance/fraud professionals alike.

Integrating gen AI into AML compliance and fraud platforms demands careful consideration. Foundational models design, ethical and operational implications, as well as privacy concerns, model transparency, regulatory alignment, are often top-of-mind. Maintaining balance between automation and human expertise is pivotal to avoid blind reliance on technology and inaccurate outcomes.

Generative AI - why now?

The timing for gen AI's integration into Anti-Money Laundering (AML) and fraud detection and prevention solutions could not be more opportune. The convergence of exponentially growing data volumes, sophisticated criminal tactics, and rapidly developing technology means AML programs will continue to struggle to keep pace with new and existing crime types and stringent regulatory demands through traditional rules-based detection and manual investigation methods. Gen AI offers a timely solution with its ability to process vast swathes of data, surface relevant insights, and present information to analysts in concise, human-readable formats.

The maturity level of gen AI has also sharply risen in the last year thanks to the popularization of publicly available tools such as OpenAI's ChatGPT. Many tech-savvy companies with skilled data scientists and analysts are capitalizing on this technology to articulate specialized learnings and tackle known challenges within their industries.

Early adoption of next-generation AI tools will allow financial institutions to position themselves for the future of combating financial crime. Driving significant productivity gains, improved efficiencies, high standards and deeper insights, gen AI can unlock unprecedented time savings and better decision-making in compliance functions.



No matter what, the subject of AIs will dominate the public discussion for the foreseeable future.

Bill Gates, March 2023

source: gatesnotes.com

Criminal exploitation of generative AI:

Curiosity in gen AI technology has everyone looking at its potential, include bad actors, criminals and fraudsters.

Gen AI is being exploited by criminals today.

Whether it be to devise malware or phishing attacks, deep fakes in the form of identity documents or voice prompts, or other generated artifacts to support increasingly complex scams and money laundering schemes, it is happening and it is hard to identify for the average institution.

Strides are being made however, following in the footsteps of "ChatGPT plagiarism" – where AI content checkers scan bodies of text to determine whether they've been produced by a chatbot or by a human. OpenAI's tool 'AI Text Classifier' does this now - it distinguishes between AI-generated text in Chat GPT and words that were written by a human. The same mechanics are now being explored in the financial crime space to detect the use of gen AI output in AML and fraud. Still in its infancy, it is expected this technology will accelerate in maturity in the coming year to be an essential add-on AI tool to modern AML compliance platforms.

\$10.5 trillion

Expected cost of cybercrime by 2025, an increase from \$8 trillion in 2023

source: [Cybersecurity Ventures](#)

Practical use cases of generative AI in anti financial crime (AFC)

Practical use cases of gen AI in AFC are abundant. Those which have proven the most practical and effective in terms of value, benefits, efficiencies and return on investment currently include:

- **Investigations:**
 - » **Data collection and analysis** – Collation of information from internal platforms, external datasets, and online searches eliminates manual data gathering efforts and facilitates thorough investigation of questionable entities.
 - » **Summarizing data and insights** – Digestible summaries of complex data patterns and meaningful insights aid efficient, comprehensive, and effective investigations of risk.
 - » **Intuitive interaction** – Natural language prompts and responses enable seamless interaction with minimal training needed for end-users.
 - » **Case records and reporting** – Automated narrative generation reduces manual effort while ensuring standardized, high-quality reports and case records.
- **Fraud detection:** Automatically analyze vast volumes of transaction data and identify intricate patterns indicative of fraudulent behavior, enabling quicker detection and mitigation of fraudulent activities while reducing reliance on manual analysis.
- **Sanctions screening:** Automate screening processes by cross-referencing transaction data with updated sanctions lists. Flag potential matches for further investigation, enhancing compliance with sanctions regulations.
- **Counter-terrorism financing:** Extend AI's capabilities from AML to counter-terrorism financing.
- **Anti-terrorism:** Dig into suspicious transactions that might appear as normal business activities, contributing to anti-terrorism efforts.
- **Regulatory reporting:** Generate case notes and regulatory reports, such as Suspicious Activity Reports (SARs).
- **BI reporting:** Analyze and generate business information reporting on KPIs, metrics, time spent resolving cases, volume of SARs raised, potential crime typologies operating in a country or region etc.

\$1.6 trillion

Amount lost to global money laundering each year

source: FACTI

[Learn more about the SymphonyAI Sensa-Net Reveal Solution](#)

Is all generative AI created equal?

Not necessarily. Thorough governance is essential for gen AI longevity and success and starts with gen AI providers and continues with banks/insurers to ensure ethical and reliable deployment of this technology. Institutions adopting gen AI should be cognizant of what 'good' looks like, especially for the model development processes, explainability mechanisms, and security measures.

- **Model development and training data:** Gen AI solutions require exposure to huge amounts of data to produce the results they achieve. The selection of datasets for the training and development of models is key, as it influences how susceptible to bias the models are, its reliability and accuracy, and may even impact the uses for which models are licensed. Comprehensive understanding of the datasets selected for training is key to selecting an appropriate and performative solution. Additionally, many gen AI solution providers may leverage foundational models, which they did not directly develop or train. As such, confirming which foundational models were used, whether they are privately licensed or open source, and understanding the development and training process is of paramount importance.

“

In the context of financial crime investigations, human oversight and ultimate decisioning remains vital.

- **Model validation:** Intensive testing for bias and hallucinations is a key component of the development process before a gen AI solution is deployed. Even with comprehensive training data, model biases can occur, as can hallucinogenic or 'made-up' responses. Developers mitigate these risks with appropriate reinforced machine learning and embeddings. Human verification is also required in the testing and validation procedures, so no surprise results eventuate.
- **Transparency and interpretability:** Unlike simpler machine learning models which follow a clear path of 'if-then' logic, gen AI models analyze a myriad of parameters and datapoints to form complex conclusions and produce nuanced outputs. Ensuring transparency can therefore be challenging. Relevant explainability tools or models should be built into solutions to deliver insights into decision trees or feature importance in relation to a model's output. In the context of financial crime investigations, human oversight and ultimate decisioning remains vital. Practical Use Cases of Gen AI in Anti Financial Crime (AFC)
- **Security:** One unique feature of gen AI solutions is the ability to input natural language prompts, and to effectively converse with the solution to achieve desired results. Understanding if and how prompts and feedback might be used in the ongoing learning of the model is crucial, particularly in the AFC sector where highly sensitive information is at stake. Ensuring a privately deployed instance of a model is used within a secure, firewalled environment, and that prompts and inputs will not leak into the underlying foundational models should be top priorities.

Understanding the benefits

The benefits of gen AI are multifaceted and assessed by the value they bring in terms of efficiency, effectiveness and optimization. At the highest level, gen AI offers:

- **Greater access to knowledge**
- **Intelligent contextualization**
- **Automation of repetitive, time-consuming manual tasks**
- **Deals with large amounts of data quickly and accurately**
- **Personalization of content.**

For AML and fraud programs, some of the key benefits manifest in:

- **Accelerating investigations:** Gen AI can collect data from various sources, including internal systems and external sites to automate case due diligence activity. Time savings can amount up to 70% faster vs. manual gathering. Additionally, gen AI creates simple, human-like explanations for alerts and associated risks, with interaction via intuitive chat interfaces. These narratives can populate and draft investigator-friendly case logs and reports – saving time in both data digestion and building out reports.
- **Reliable and scalable processes:** Gen AI powered solutions offer consistent, high standard processes and composes reports in unambiguous, exact language. It also offers full auditability or explainability of what is gen AI content or not, so it is understood to process-owners and regulators. Lastly, the conversational nature of gen AI means little to no user training is required to use it once it is licensed. It is recommended staff continue to be trained on risk appetite, words/phases and language to be used in all case files, reports etc, that meet the institutions' risk tolerance and culture.
- **Accurate assessment of risk:** Context-aware gen AI 'understands' various types of investigations and where it sits in the overall process. This assists analysts and investigators, saves time and optimizes workflows and effort at each stage of the process. Further, intelligent enrichment of data helps focus on critical decisions and make more informed decisions.

60-70%

Percentage of work that employees currently undertake that could be automated by generative AI and other technologies today

source: 'The economic potential of generative AI: The next productivity frontier', McKinsey, June 2023



The benefits of gen AI are multifaceted

Navigating the potential pitfalls

Potential pitfall	Mitigation
Not researching the gen AI provider properly Not understanding providers' methodology and approach to building and training AI models or reviewing evidence of proven results.	Research and meet with gen AI providers for AML and fraud to perform due diligence and assess their practices, design methodology, investment in ongoing innovation, support capability and heritage in the fincrime space. Ensure a thorough understanding of any foundational models and training datasets used.
Cleanliness of internal data Not understanding how clean or dirty existing internal financial crime and fraud data is, and whether it has bias built in already for certain factors. Once large language models are implemented, they will continue to train and learn from your institutions' data.	Assess the cleanliness of internal AML and fraud data. If needed, be ready to either cleanse or remediate where it is warranted. Independent reviews of datasets for potential sources of bias can be helpful. Consider which datasets should be incorporated into gen AI solutions based on the target use case(s).
Data privacy Using public or opensource gen AI solutions brings additional risk of sensitive data being leaked outside the institution.	Protecting sensitive data is important and controls should be in place to ensure data leakage does not occur. Perform adequate due diligence on gen AI providers' approach to data privacy, adherence to data protection regulations and guidelines during the analysis process. Confirm if and how prompt data will be used to reinforce and train models. Only deploy private instances of models and solutions to avoid sensitive data leaking into underlying foundational models. Adequately train staff on the risks of sensitive data leakage.
AI Interpretability The outputs generated by AI models, particularly those based on complex algorithms like Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs), can be difficult to interpret. This black box nature of AI systems can create a barrier to acceptance, as users may be skeptical of outputs they do not fully understand.	Confirm the gen AI provider has designed transparency and interpretability in the models. Explainable AI (XAI) techniques are leveraged to make the decision-making process of AI models transparent and understandable. Consider how to implement robust validation and oversight of AI models within business operations.
Accuracy of Information Gen AI models run the risk of generating misleading or inaccurate information. Given the serious implications of AML investigations, it is crucial that the data generated by AI systems is accurate, reliable, and trustworthy.	Robust mechanisms for data verification and investigation guardrails must be in place to allow for cross-validation techniques, anomaly detection systems to identify outliers, and the continual training and testing of models to ensure their accuracy. Solutions designed with embeddings to point gen AI solutions to specific datasets and evidence can mitigate hallucinations. Appropriate oversight of model outputs is also crucial.

The way forward

The gen AI wave of momentum is here to stay in AML and fraud. Taking control of the impacts of gen AI is the dual responsibility of providers developing it and those adopting the technology.

With the use cases growing and continuing to prove successful and effective results in detecting and preventing financial crime every month, the maturity of this tech in this industry will advance and become a built-in component of AML and fraud programs going forward.

By understanding what best-practice AI model development and learning looks like, what value and benefit gen AI brings in modernizing existing AML and fraud programs to keep pace with emerging crimes methods, and in knowing that pitfalls have mitigations that will be become easier and easier to remedy, confidence is gained in this new technology evolution.



Customers rate Sensa-NetReveal a perfect 5 across functionality, technology, and service and support.

Neil Katkov, Director, Celent

Meet Sensa Investigation Hub – powered by generative AI.

- A single, enterprise-wide solution for all your investigative needs Sensa Investigation Hub is detection agnostic and configurable to any use case, business unit, or asset class. Generative AI-powered investigation using the built-in Sensa Copilot, accelerating investigations by ~70%
- Seamlessly working alongside your existing solutions to deliver enhanced efficiency and accuracy
- Enterprise-wide risk management, consolidating the risk and compliance tech stack with a single SaaS-led platform
- Entity-centric investigation offering a complete view of a subject's risk profile across anti-money laundering, sanctions, know your customer (KYC), customer due diligence (CDD), and fraud.
- Auditable decisioning and reporting via end-to-end transparency aligned with organizational processes, policies, and regulations, ensuring consistency
- To find out how Sensa Investigation Hub can transform your investigations, [click here to book in a demo.](#)

Awards and accreditations



SymphonyAI Sensa-NetReveal named Category Leader in Chartis RiskTech® Quadrant for Payment Risk Solutions (overall), 2023



SymphonyAI Sensa-NetReveal named as a Luminary in XCelent Awards for Financial Crime Compliance Technology: AML Transaction Monitoring Edition 2023



SymphonyAI Sensa-NetReveal named as a Technology Leader for KYC Solutions by Quadrant Knowledge Solutions, 2023



A significant new addition to the compliance technology ecosystem.

Sidhartha Dash, Research Director, Chartis

About SymphonyAI Sensa-NetReveal

SymphonyAI Sensa-NetReveal, a division of SymphonyAI, provides leading AI-based financial crime detection software.

Contact us to learn how SymphonyAI Sensa-NetReveal can help drive more effective financial crime detection and prevention in your company.



UK Location

Notcutt House,
36 Southwark Bridge Rd.
London, SE1 9EU



Spain Location

Paseo de la
Castellana n. 141,
5 planta, Madrid



France Location

19 Bd Malesherbes
75008 Paris



Germany Location

Mainzer Landstraße
50/6th floor, 60325
Frankfurt am Main