Threat Assessment

NICB National Insurance Crime Bureau

Report Date:	September 6, 2024	Geographic Scope:	National
Report Title:	Artificial Intelligence Threat Assessment	Report Type:	General
Dissemination:	Member Companies and Law Enforcement	Analysis Period:	01/01/2022 – 09/01/2024

Executive Summary

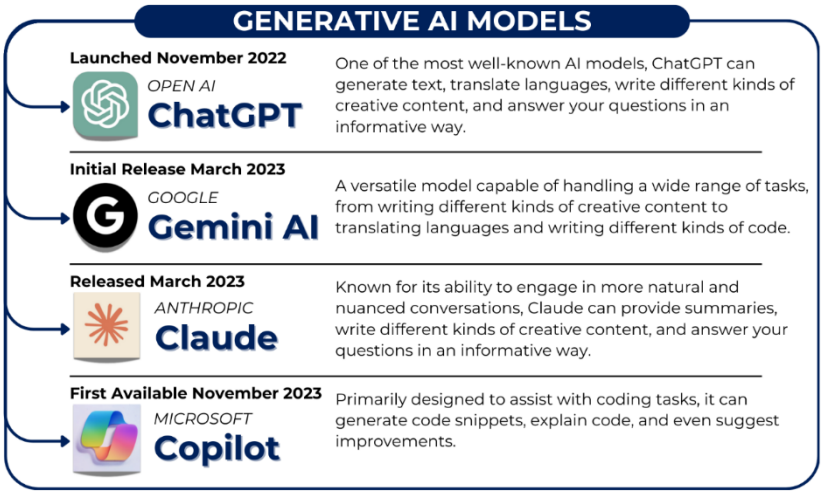
Artificial Intelligence (AI) is a rapidly growing technology with significant implications for the insurance industry. It offers vast potential for both legitimate applications and misuse. Insurance companies can leverage AI to enhance their defenses against fraud by strengthening policy and claim reviews, ensuring fraudulent claims are not paid out. The greatest risk lies in AI's ability to manipulate data and generate fake content, potentially leading to the creation of counterfeit VINs, fake cargo manifests, synthetic identities for insurance policies, and more. Every aspect of the insurance process is vulnerable to the misuse of AI and Generative AI. Therefore, it is crucial for insurance companies to consider integrating AI in their claims processes while remaining vigilant about its potential fraud and crime risks. Education and training can help investigators recognize signs of manipulation, while educating customers on safeguarding their personal information is equally important.

As AI technology continues to evolve, its applications and the tasks we ask of it will become increasingly sophisticated. This evolution brings both opportunities and challenges to the insurance industry. While AI can significantly enhance fraud prevention efforts, it also opens new avenues for fraudulent activities. Fraudsters may increasingly leverage AI to deceive insurers and exploit system vulnerabilities.

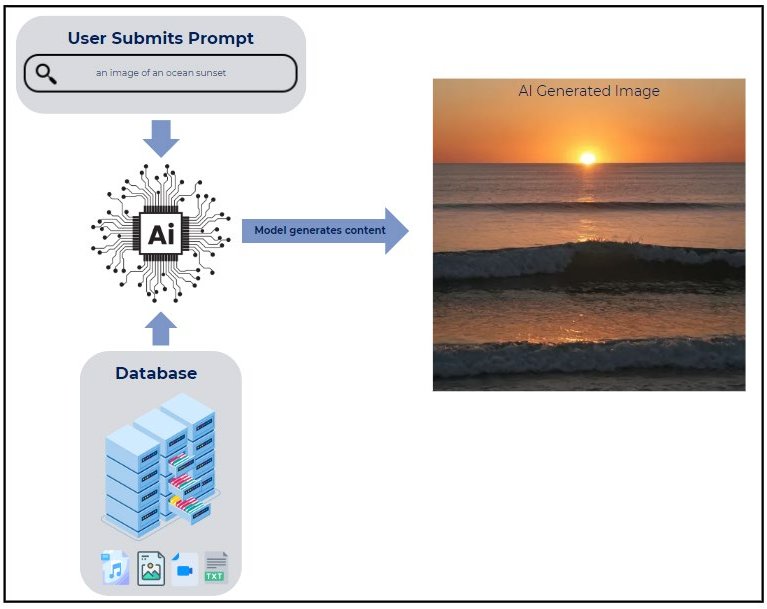
Contents

Section 1: What is Artificial Intelligence?

It is safe to say, if you are reading these words chances are you have interacted with Artificial Intelligence (AI). In fact, you have been interacting with AI daily without even realizing it and for much longer than you might guess. If you have used Google Maps, posed a question to a Help Chat on a website, or have a streaming device that recommends content based on your use, AI has entered your life. In 2023, the reported number of users of AI tools more than doubled from 2022 with over 250 million users globally. It is predicted that this number will surpass 700 million by the end of the decade (Thormundsson, 2024). AI models are complex tools, however there are a growing amount of public facing Generative AI models that can be accessed by anyone with an internet connection.



In its simplest definition, "Artificial Intelligence is an attempt to make a computer, a robot, or other piece of technology 'think' and process data in the same way that humans do" (Microsoft). The advent of Generative AI in 2022 has once again thrust AI into the spotlight, and it will undoubtedly have a significant impact on day-to-day life. AI essentially involves making machines think and solve problems. While previous AI models were limited to making predictions based on specific datasets, Generative AI goes a step further, enabling the creation of content such as text, videos, photos, and audio.



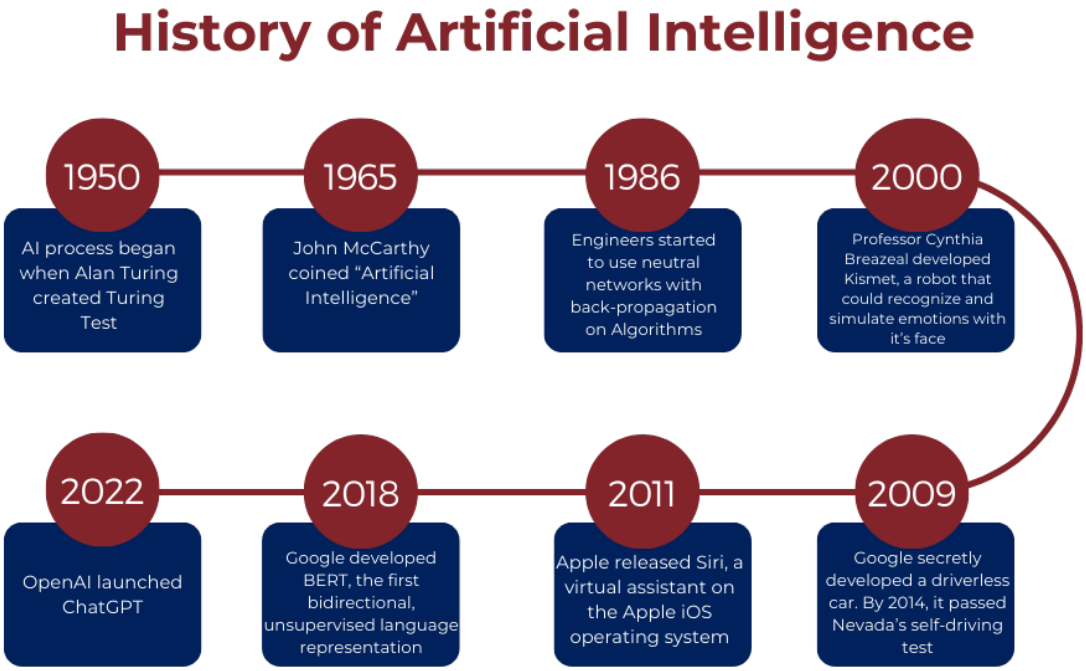
Generative AI relies on a database or **neural network** of information. This can be text, images sounds, etc. and is the basis for AI (Ghani, 2024). The model is rigorously "trained" on this data until a user can provide a prompt, or a description of desired content, which the model will attempt to create. Prompts can be words, numbers, or photos which are used to generate new examples based on the examples the model was trained on. These are then fed back into the model so it can continue to learn and increase its accuracy in achieving the desired prompt.

As these models grow in sophistication metadata, or the data behind your data, has become increasingly important in measuring data's relevancy. An AI model that scrapes data from public websites for information can use metadata to determine how relevant a piece of information is. For example, a sentence from online forum 10 years ago is most likely not as useful or relevant as a comment on a more recent post. Metadata creates layers in data that can be further analyzed increasing accuracy, relevancy, and pattern recognition.

As powerful as AI is, it is not without limitations. AI is dependent on the data that is put into the model, including both base data and prompt data. This means a Generative AI model is incredibly susceptible to bias, much like humans. Essentially, this causes the model to potentially **hallucinate** or show nonexistent patterns (What are AI Hallucinations, 2023). It is important to keep this in mind when using Generative AI. Other limitations include a struggle to combine text and photos as well as creating realistic body parts such as hands and eyes (Gray, 2024). AI generated content is far from perfect; however, it is improving every day.

Brief History of Artificial Intelligence

The idea of thinking machines goes back to the ancient Greeks (Marr, 2024) with many leaps in progress on the way. The father of modern computer science, Alan Turing, speculated in 1950 on the possibility of creating a machine that could think. In 1997, AI beats the then World Chess Champion Garry Kasparov in a chess match and goes on to beat him again in a rematch (*Artificial Intelligence (AI) Guide: AI Timeline* 2024). These AI models and others like them are growing in ability and sophistication and are being used around the world.



Section 2: Emerging and Evolving Risks in Insurance Fraud

When it comes to insurance fraud, AI has the potential to not only heighten existing fraud schemes but make it more accessible for those who previously might not have otherwise participated in filing a false insurance claim. The potential ease and availability for AI to assist in committing fraud could entice those who would not have considered it before. From acquiring Personal Identifying Information (PII) to manipulating documentation to receive a fraudulent claim payout, all aspects of insurance fraud are possible with the misuse of AI. AI is already being used in both fraud schemes and fraud investigations, helping to both commit and prevent insurance fraud. It can be exploited to steal information and create fake documents, but it also analyzes claims data to identify risk indicators and patterns of fraud.

AI is user friendly and freely available, lowering the level of difficulty for even the average person to participate in insurance fraud. Seemingly legitimate supporting documents are simple to create using Generative AI. A user can type in a description of the photo they want such as vehicle and property damage which is generated by the AI model. Videos of vehicle crashes and weather events such as tornados can seem very real. Generative AI has also enhanced phishing schemes and is being used to trick recipients into divulging their PII. Stolen, leaked, or spilled PII is also used in the creation of fictitious identities, which can be used to take out fraudulent insurance policies and file fraudulent claims. Misused AI by sophisticated and organized criminal groups greatly amplifies the financial threat to insurance companies.

Document Forgery/Alteration/Creation

One of the most popular ways to use Generative AI to commit fraud is the creation of documents such as paystubs, insurance applications, finance applications, fake IDs, etc. Websites like Generator 3.0 can create up to 20,000 fake IDs per batch and sell them for starting at $5, including an identity background. AI also has the capability to clone and create voices that sound convincingly real. When used over the phone, one could easily trick an unsuspecting person into thinking they are talking to someone they know, even family members (FTC, 2024). When submitting a false claim, it is possible to impersonate or entirely create an individual and use voice manipulated AI to send voice messages or even take phone calls from insurance personnel. Additionally, Generative AI Chatbots like Dall-E and OpenArt can be instructed to create images of damaged vehicles and property for use in fraudulent claims.

Prompt: Toyota Corolla with a severely dented bumper in a driveway

Prompt: Badly damaged Toyota Corolla in a parking space

Generative AI Manipulation

Most public facing AI models have some degree of content control, but they can be "tricked" into making nefarious materials. This behavior is called **Prompt Injection**, where the user manipulates the AI system using disguised prompts to get a malicious outcome, such as influencing a Chatbot or LLM to steal private information, delete or send emails, etc. Generative AI can effortlessly create emails and texts for **phishing**, a scam to entice a user to click on malicious links, and **spoof** attacks, scammers disguising themselves as a legitimate source to gain a user's trust and commit further crimes with the information or access gained, that are incredibly believable (AI and fraud: Opportunities and challenges, 2023).

Synthetic Identities

Traditional identity theft involves the improper usage of an existing person's PII. A synthetic identity is the combination of PII (legitimate and faked) to fabricate a person or entity for personal or financial gain. Synthetic identities have been a growing problem for insurance companies and Generative AI is proving to exacerbate this issue. AI offers quick and believable ways to collect and create PII. For example, illegitimate credit repair companies trick individuals into supplying their social security numbers to acquire a Credit Privacy Number (CPN) with the promise of repairing their credit. AI helps these companies look legitimate though the creation of legitimate-looking forms and emails. Once a 'customer' provides their social security number and other identifying information, it is parsed out and used to create a fictitious identity. However an identity is created, it can then potentially be used to take out almost any kind of insurance policy and file fraudulent claims.

Section 3: How AI can Help Fight Insurance Fraud

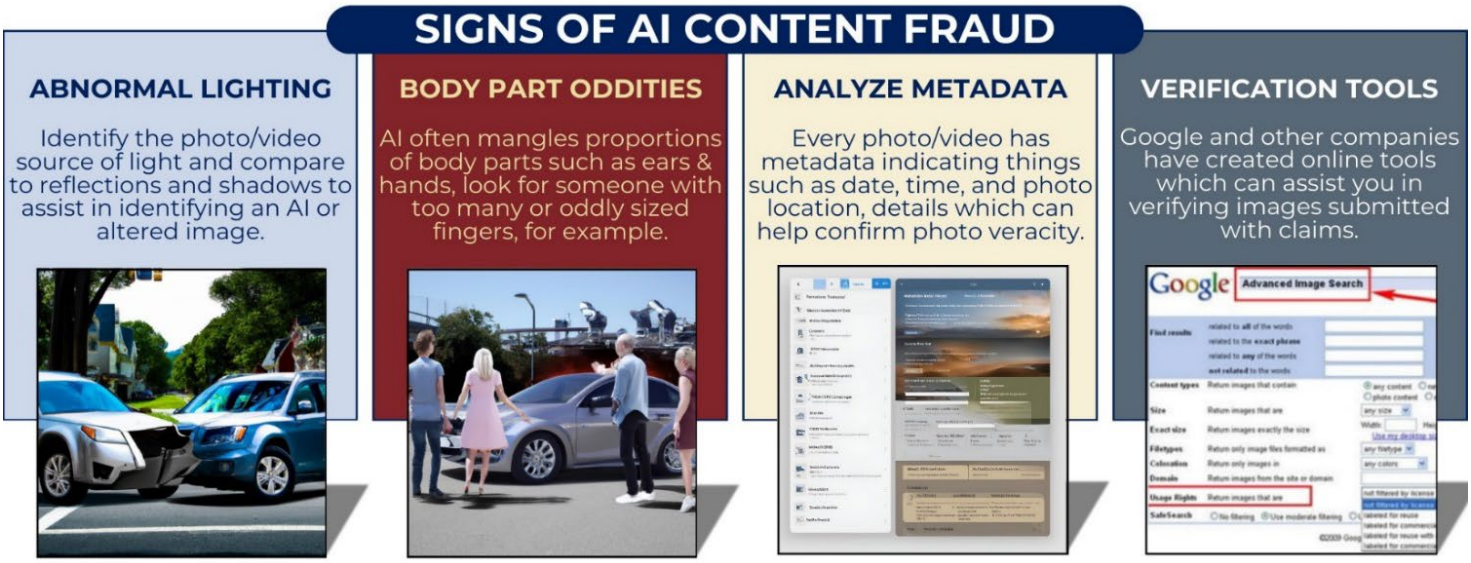
While AI can be used for illegitimate acts, there are many positives to using AI responsibly. Despite the looming threat of AI being used to perpetrate insurance fraud, fraud investigations stand to substantially grow in sophistication. AI models can pick up on and collate patterns faster than humans can. In many ways, AI can be embraced as a way to help analyze large amounts of data quickly, allowing investigators to dig deeper into their investigations and potentially be more effective.

AI can also be used to accumulate data from either public-facing sites or fed data, making it an incredible search engine. It can collectively analyze data and assist in policy evaluation and risk analysis, potentially protecting insurance companies from fraudulent claims before they are paid out. Proactive use of AI can critically review documentation before policy inception, effectively fighting fraud on both fronts.

Currently, AI is not the most accurate when trying to detect itself; however, this could change in the future as the technology develops. AI is a tool insurance companies can use to their advantage throughout the entire claims process.

Section 4: Recommendations

The number one threat of Generative AI is the ability to make realistic looking content that is used to commit illegal acts. One of the first lines of defense is recognizing altered content. AI is not able to successfully create realistic content all the time. Things like hands, eyes, and the sound of crying or genuine emotion is still something not perfected by AI. In claim reviews, taking steps such as asking for multiple photos using different angles of damaged property can help distinguish real from AI faked damage photos. Looking for signs like odd cuts in videos and disfigured body parts can indicate the efficacy of content. Today, it is more important than ever to question the truth of what the screen is telling the user. When examining documents to support insurance claims, it is important to take measures such as training investigators on what to look for when examining potentially AI influenced content.



Section 5: Conclusion

AI is a transformative technology with the potential to revolutionize various aspects of society and industry. It brings a range of opportunities and challenges that are worth considering:

Opportunities:

- *Automation and Efficiency:* AI can automate routine tasks, leading to increased efficiency and productivity.
- *Enhanced Decision-Making:* AI algorithms can analyze vast amounts of data more quickly and accurately than humans, providing insights that lead to better decision-making.
- *Innovation:* AI is driving innovation opening new frontiers for technological development.
- *Accessibility:* AI-powered tools can make technology more accessible to people with disabilities, such as voice recognition software for those with mobility impairments or visual recognition tools for the visually impaired.

Challenges:

- *Ethical Concerns:* AI raises ethical questions, including concerns about bias in algorithms, privacy issues, and the potential for AI to be used in harmful ways, such as deepfakes or autonomous weapons.
- *Job Displacement:* The automation of jobs by AI could lead to job displacement in certain industries, particularly in roles involving routine, repetitive tasks.
- *Security Risks:* AI can be exploited for malicious purposes, such as creating convincing phishing schemes, hacking, or generating false information that can deceive people on a large scale.
- *Dependency and Trust:* As AI becomes more integrated into daily life, there is a risk of over-reliance on AI systems, which may lead to reduced human oversight and potential errors if the AI fails or is compromised.

As AI continues to grow in sophistication so will the tasks we ask of it. It "has the potential to transform various industries, from finance and education to transportation and healthcare" (Ghani, 2024). The insurance industry and the industry of fraud are no exemption. Fraud actors will use and develop AI for the purpose of fooling others and gaining money and services they are not owed. Special Investigation Units can utilize AI to help bolster policy and claim review to help prevent the issuing of fraudulent policies and catch fraudulent claims before they are paid out.

AI is a powerful tool that, if used responsibly, can bring about significant positive changes. However, it also requires careful consideration of its ethical, social, and security implications to ensure that its benefits are maximized while minimizing potential harms. Balancing innovation with responsibility is key to harnessing the full potential of AI.

Appendix: Related Terms

Algorithm: a set of rules or instructions that tell a machine what to do with the data input into the system

Deep Learning: a method of machine learning that lets computers learn in a way that mimics a human brain, by analyzing lots of information and classifying that information into categories. Deep learning relies on a neural network.

Neural Network: a deep learning technique that loosely mimics the structure of a human brain. Just as the brain has interconnected neurons, a neural network has tiny interconnected nodes that work together to process information. Neural networks improve with feedback and training.

Machine Learning (ML): a type of artificial intelligence that uses algorithms which allow machines to learn and adapt from evidence (often historical data), without being explicitly programmed to learn that particular thing.

Large Language Model (LLM): a computer program that has been trained on massive amounts of text data such as books, articles, website content, etc. LLMs use natural language processing (NLP) techniques to learn to recognize patterns and identify relationships between words. Understanding those relationships helps LLMs generate responses that sound human—it's the type of model that powers AI chatbots such as ChatGPT.

Natural Language Processing (NLP): the ability of machines to use algorithms to analyze large quantities of text, allowing the machines to simulate human conversation and to understand and work with human language.

AI Hallucination: a phenomenon wherein a large language model (LLM)—often a generative AI chatbot or computer vision tool—perceives patterns or objects that are nonexistent or imperceptible to human observers, creating outputs that are nonsensical or altogether inaccurate.

Prompt Injection: When an attacker manipulates a large language model (LLM) through crafted inputs, causing the LLM to unknowingly execute the attacker's intentions. This can be done directly by "jailbreaking" the system prompt or indirectly through manipulated external inputs, potentially leading to data exfiltration, social engineering, and other issues.

Synthetic Identity: combination of Personal Identifying Information (legitimate and faked) to fabricate a person or entity to commit a dishonest act for personal or financial gain. They key to this type of identity theft is the use of fictitious data.

Metadata: data behind data such as GPS location, date/time, etc

Spoof attack: scammers disguising themselves as a legitimate source to gain a user's trust and commit further crimes with the information or access gained

Phishing: a scam to entice a user to click on malicious links

References

FTC submits comment to FCC on work to protect consumers from potential harmful effects of ai. Federal Trade Commission. (2024, July 31). https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-submits-comment-fcc-work-protect-consumers-potential-harmful-effects-ai

Ghani, R. (2024). Artificial Intelligence, Explained. Carnegie Mellon University's Heinz College. https://www.heinz.cmu.edu/media/2023/July/artificial-intelligence-explained

Gray, R. (2024, March 18). *How to spot a manipulated image*. BBC News. https://www.bbc.com/future/article/20240311-how-to-spot-a-manipulated-image

LexisNexis Risk Solutions. (2023, September 22). AI and fraud: Opportunities and challenges. https://risk.lexisnexis.com/global/en/insights-resources/article/ai-and-online-fraud

Libguides: Artificial Intelligence (AI) guide: Ai timeline. AI Timeline - Artificial Intelligence (AI) Guide - LibGuides at University of Texas Southwestern Medical Center. (2024, May 31). https://utsouthwestern.libguides.com/artificial-intelligence/ai-timeline

Marr, B. (2024, July 2). Artificial Intelligence 101: Its evolution, implications and possibilities. Forbes. https://www.forbes.com/sites/bernardmarr/2024/02/08/understanding-ai-in-2023-its-definition-role-and-impact/

Microsoft. Fundamentals of Artificial Intelligence. Student-Guide-Module-1-Fundamentals-of-AI.pdf (microsoft.com)

Thormundsson, B. (2024, February 13). *Worldwide AI tool users 2030*. Statista. https://www.statista.com/forecasts/1449844/ai-tool-users-worldwide#:~:text=People%20using%20AI%20tools%20globally,the%20end%20of%20the%20decade.

Social Engineering Scams. INTERPOL. https://www.interpol.int/en/Crimes/Financial-crime/Social-engineering-scams

What are ai hallucinations?. IBM. (2023, September 1). https://www.ibm.com/topics/ai-hallucinations