FEATURE

Non Sequitur

EMERGING TECHNOLOGIES

Each month, these pages will feature our "bonus theme," that does not necessarily coincide with the overall themes of the issue.

ARTIFICIAL INTELLIGENCE
THE NEXT FRONTIER AND THE NEXT BIG THREAT

BY CHRISTINE MEADOR

Picture this scenario. You are the CEO of an organization and you have arrived home for the evening. You suddenly receive a call from your Treasurer. The Treasurer is confused by the email you supposedly sent him requesting a transfer from a popular online app. Immediately, you realize this was not your email. Alarming, well it should be, and this is only the tip of the iceberg. In fact, the bigger "reality check" is when you realize your email is likely one of thousands of emails sent out by a fraudster in a "single strike" from a remote and unidentified location.

How many of you have received a similar email like this? Did you act, verify, or respond? Whether it is an email or a robocall, these types of occurrences are happening more often and with the assistance of artificial intelligence (AI), they are being created with ease. What this tells us is we are entering a new frontier, where we often cannot trust what we see or hear. This is a monumental change to the world as we know it, in our private lives, in the business world, and especially in the area of crime.

How do we deal with this super advanced AI technology? In a world full of growing AI "chaos", dialing back to the basics of "common sense", constant vigilance, education, and outreach, is viewed as some of the best ways to protect businesses and the public at large. Let us take a deeper look at AI, the next frontier, and the next big threat.

Artificial Intelligence On The Horizon

To prepare for this article, I had the pleasure of speaking to two leading professionals dealing with AI, in the legal field and in the business sector, Brian McDonough, Assistant United States Attorney, White Collar Crime Unit / Elder Justice Coordinator, and Simon Marchand, VP of Product, Risk with GeoComply. In our discussions, both professionals agreed and confirmed that "AI is the next big threat."

We have seen technology grow in leaps and bounds; however, AI is now taking this technological growth to an entirely new level. So, what exactly is AI and how is it progressing into our everyday landscape? Interestingly, AI has been a term since the 1950s.

Artificial intelligence, as defined by Stanford University — Human-Centered Artificial Intelligence — is "a term coined by emeritus Stanford Professor John McCarthy in 1955, was defined by him as 'the science and engineering of making intelligent machines.' Much research has humans program machines to behave in a clever way, like playing chess, but, today, we emphasize machines that can learn, at least somewhat like human beings do." (https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf).

Another definition of AI is "a computer system or program with the ability to perform human related tasks that usually require human intelligence. A few examples include the ability of decision-making, translation, visual perception, and speech recognition." (https://www.oxfordreference.com/display/10.1093/oi/authority.20110803095426960;jsessionid=5C107E8E7CB161A6135F0E30C3CF91D7).

Today, we see AI integrated into our society in more ways than we may realize, such as map navigations, browsers, facial and voice recognition, fingerprint scanning, and much more. AI is visible everywhere, such as in schools where it is assisting teachers and students, in hospitals where AI is being introduced in monitoring and assisting patients, and even in the legal sector, as referenced in debates on legal writing, briefs and more. Artificial intelligence is on the rise, and it is going to affect everyone.

Why is AI a Game Changer and How is AI Affecting Businesses?

The advancement of artificial intelligence is a "game changer" in a few ways. Mr. Marchand, explains that "AI is creating a whole new discipline." The ease of use and the ability to access AI knowledge is what makes the new 'AI and programs' the next big threat. Organizations are using artificial intelligence for good, to protect and detect weaknesses; however, this is technology we do not have the means to protect. This can be a big threat in the hands of intruders and offenders.

A good example of an AI program, and one many readers will be familiar with, is ChatGPT, an AI program widely known as a "AI Chatbot" that can be used to "write" and more. This is one of many AI programs, which is widely accessible to all: private consumers, businesses, and unfortunately wrongdoers. Programs like this open the door to AI threats, as it puts technology in a place where we cannot control who is using it. As with "voice and video" fakes, it is clear, we are entering a new landscape where we cannot trust what we see or hear.

AI in Businesses and Fraud Prevention

AI is beneficial when leveraged by organizations to protect and detect weaknesses, as well as in detecting suspicious activities, transactions, or even robocallers.

In respect to the "anti-fraud programs," which is reflective across industries and as shown in the *2022 Anti-Fraud Technology Benchmarking Report by the ACFE and SAS,*

- "The use of artificial intelligence and machine learning in anti-fraud programs is expected to more than double over the next two years."
- In addition, "While only 17% of organizations' anti-fraud programs currently use artificial intelligence or machine learning analytics, these techniques are expected to experience the most growth, with 26% anticipating that their organizations will adopt this type of advanced analytics technology in the next two years."

(https://www.acfe.com/fraud-resources/anti-fraud-technology-benchmarking-report, 2022, p. 3, p. 7).

AI can be a great asset; however, it is critical not to replace the "human interaction" and oversight. As explained by Mr. Marchand, some organizations may rely on AI too much.

"There are organizations that utilize AI, for example, in the human resource process. The ease of using AI in handling a large employee volume may be seen as a benefit; however, the legal ramifications and dehumanization of key roles may lead to consequences in the event of hiring or firing employees. Organizations making the move to incorporate AI into key roles should be cautious on the regulatory standpoint, such as dealing with human resources and labor decisions."

In the Legal Field – Prosecution of Criminals and Litigation.

As we see, AI programs are utilizing information and images. It is clear we will again be moving into a new arena as the legal field becomes immersed in debates and litigation related to artificial intelligence.

- AI programs, creating or developing images or "works," may spark debates on copy rights, art, publications, and introduce new questions on ownership and more. As Mr. Marchand states, "Where do we draw the line."
- As with cybersecurity in the legal field, AI may be the next emerging legal discussion.
- When fraudsters or intruders are caught, the legal process walks "hand-in-hand" with the law, legal analysis, litigation, and prosecution.

AI Threats in Real Time

AI can be an asset to organizations; however, by the same token, it is a tool that can be used for both good and evil. The most recent AI threat, mentioned by both of our leading professionals, is the deepfakes or "deep voice fakes" which fraudsters are creating with the use of AI programs. This act of stealing voice clips from popular social media apps is occurring in scams, such as the Grandparent Scams.

In addition, AI is being used in aggravated identity theft which involves impersonating federal law enforcement, FBI, IRS, or local police, as well as scenarios like the CEO fraud, as presented in the above introduction. As stated by Brian McDonough, "We are at a vector point in crime," where we cannot trust voice, face, or audio.

Threats like these are becoming a reality due to ease of use and just as AI technology is evolving, fraudsters are also becoming more sophisticated in their fraud schemes. AI makes fraud easy and more accessible. Fraudsters can use AI to develop fraud programs and AI can intrude into corporate networks, as well as in fraud scams, affecting the general public from undisclosed locations, both local and abroad.

Recommendations in Regard to AI Threats

There is no doubt, the best way to prevent against any threat is to prepare. The most obvious "tip" from these leaders is to understand AI is a real threat. It is important to understand the threat exists and educate. This is especially important for those most vulnerable, such as the elderly.

Business Sector Recommendations

Simon Marchand, VP of Product, Risk with GeoComply, leads fraud prevention professionals, trainings, and is a leading presenter in regard to fraud, identity, biometrics, fraud prevention, and artificial intelligence. Simon shared the following recommendations:

- From an organizational standpoint, incorporate policies and procedures to protect yourself against risks of external attacks and refined CEO fraud, but also policies on the responsible use of AI within the organization.
- Understand the threats you are under. As fraud experts, managers, executives, it is essential to understand what AI means, what new technologies do and how they work. Disregarding the latest technology poses a

significant risk to be exposed to new threats that you are not properly protected against, and that can mean fraud threat, but also PR threat. Your organization's reputation is on the line.

- As a consumer, always be aware of the information you share online, and understand: the more you share, the more you expose yourself to potential attacks that could leverage AI.
- As a consumer, be critical of information you are exposed to. Fraudsters can use AI to trick you, and they will.
- Big organizations and governments have the responsibility to educate and communicate on the risks of new technologies.
- As individuals, if we understand those risks, we must communicate them with the most vulnerable. The elderly are particularly vulnerable to the use of low-sophistication deepfakes or deep voices.

Fraud Prevention Recommendations

As with any organization, having a *Response Plan in place is key to protecting. Additionally, as new threats evolve, such as artificial intelligence, be sure to update your organizations policies and procedures, and your Response Plan.* (https://www.medicacpa.com/~medica/files/Nov19BarJournalMeador.pdf).

- **Response Plan** – The best way to prepare in advance is to develop a good Response Plan.
- **Insurance policies** – In relation to insurance policies, it is critical to know your policy in advance and to understand where cyber or artificial intelligence threats fall under the insurance umbrella.
- **Educate your 'in-house' team** – As with organizational trainings on topics such as ethics, it would be beneficial to offer trainings on cybersecurity and new evolving artificial intelligence threats.

Legal Field Recommendations – Elder Fraud and Scams – Increased AI Threats

Assistant United States Attorney, Brian McDonough, White Collar Crime Unit and Elder Justice Coordinator, shares the best way to protect against "scams" is to practice "constant vigilance." This can be achieved through education, outreach, and staying engaged with the public. Additional recommendations are listed below:

- Constant vigilance, education, and outreach. Stay engaged with folks. This is important for those most vulnerable, such as the elderly.
- Key to all of the scams is the ingredient of EMERGENCY and the need for funds. Take this EMERGENCY as a red flag and take time to confirm.
- Hang up if: Caller threatens you with arrest or property seizure, claims to be a grandchild or loved one in trouble with the law, asks you to wire money, mail cash, or pay with gift cards, or a repair person calls out of the blue and wants to fix your computer.
- Never open suspicious email links or unsolicited text messages.
- Report "AI" crime to www.ic3.gov.

Conclusion

As artificial intelligence programs filter into the world as we know it, we are noticing the benefits and detriments that can arise. In short, AI allows users access to AI programs which deliver countless capabilities, and this can be used for good or evil. We can look back throughout history and it is a fact, change comes with "growing pains." The benefits of AI technology will no doubt prove beneficial to businesses and the public; however, we know this too will benefit individuals seeking to do harm.

The key to success in dealing with this AI advancement is to be responsible and understand AI is here. The public should be proactive, educate, and protect. It is important to understand the capability of AI, to the best of our ability, in the field and in our daily lives. People will need to be responsible and observe constant vigilance. Leading professionals in the field urge people and businesses to educate. In fact, the theme of "educating" is a constant between all three sectors presented in the article: business, legal and fraud prevention. Training and education is viewed as one of the best ways to protect yourself and your organization.

Christine M. Meador is a CFE, forensic accountant and affiliate member of Medica, LLC. She focuses on assisting organizations with fraud prevention, detection, forensic investigations, and a variety of management needs. Christine is the President of the Northeast Ohio Chapter of the Association of Certified Fraud Examiners and is a nonprofit and for-profit management consultant with CMM Consulting Services, LLC. CMBA Member since 2017. She can be reached at (216) 513-0687 or cmeador@medicacpa.com.

A special thanks to Brian M. McDonough, Assistant United States Attorney, White Collar Crimes Unit / Elder Justice Coordinator, for contributions with AI recommendations, and Simon Marchand, CFE. C.Admin., VP of Product, Risk with GeoComply, for contributions with AI recommendations.