DEMYSTIFYING AI IN ANTI-FRAUD AND COMPLIANCE EFFORTS

Artificial intelligence and machine learning seem to be included in most technology discussions. But what do these potential technologies really mean for fraud examiners and compliance professionals?

COLUMNIST
VINCENT M. WALDEN, CFE, CPA
MANAGING DIRECTOR, DISPUTES AND INVESTIGATIONS PRACTICE
ALVAREZ & MARSAL

Michael is head of investigations at Ryan Ltd., a mid-sized, global manufacturing company. (All names and company references in this case example are fictional.) The company recently undertook an enterprise-wide digital transformation initiative that included various uses of artificial intelligence (AI). Michael's compliance and investigations team was no exception. So, he wasn't surprised when Tom, the company's global chief compliance officer, asked him to explore how his team could apply AI in their proactive fraud risk assessment and monitoring efforts plus their reactive investigations and legal department. But where does Michael start?

In the ACFE/SAS 2019 *Anti-Fraud Technology Benchmarking Report* (tinyurl.com/y56a57qq), 25% of companies surveyed said they expect to adopt AI and/or machine learning (a subset of AI) in the next one to two years. And many issues of *Fraud Magazine* contain technology advertisements touting AI or machine learning in some form to improve fraud detection. Every fraud, risk or compliance conference features at least one session on AI and the benefits it can provide a fraud risk management and compliance program.

Five years ago, the big corporate technology buzzword was "big data." Clearly, the buzzword today is AI. Yet, AI still is a vague concept. We hear about ways to improve decision-making with cognitive computing, natural language processing, deep learning, neural networks, self-driving cars, chat bots, smart contracts, robotics process automation and even automated medical diagnosis.

This column will attempt to demystify the subject and help accelerate innovation.

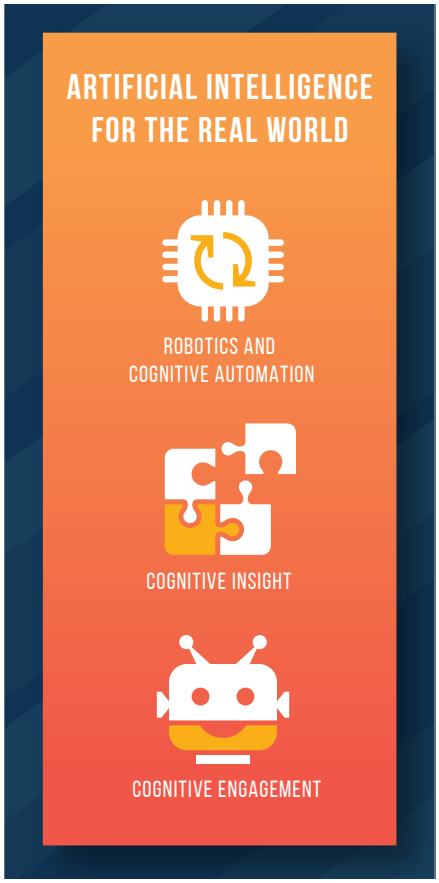
Defining AI — a spectrum of capabilities

Gartner Inc., a global research and advisory firm, suggests that AI means different things to different roles. CIOs (and all organizational professionals) must understand what business users and technologists expect when they talk about AI because this clarity will help maximize the value of their time, effort and money. (See "Define Artificial Intelligence for Your Organization to Streamline for Success," Garner, ID G00386440, tinyurl.com/y2u5tcdq.)

On a recent episode of my podcast, The Walden Pond (part of the Compliance Podcast Network), Lee Tiedrich, a partner with the law firm, Covington & Burling LLP, refers to AI rather broadly — yet succinctly — as "the capability of software together with data and computing to imitate intelligent human behavior. "... Machine learning, natural language processing, deep learning and neural networks are all applications of AI to automate cognitive tasks," Tiedrich says. (See tinyurl.com/vrgh8f4.)

In a 2018 *Harvard Business Review* article, "Artificial Intelligence for the Real World" (tinyurl.com/yapnma49), authors Thomas Davenport and Rajeev Ronaki studied more than 150 AI projects and observed three main categories based on levels of sophistication. On the lower end is *robotics and cognitive automation* in which robotic process automation technology, or RPA, automates typical back-office administrative and financial activities. Think of RPA as organizations developing large-scale MS Excel macros to accomplish routine tasks. But RPA technology doesn't limit us to the confines of just one software application. RPA tools, for example, allow the software to automatically open one application (such as a sales-tracking application), make an automated decision based on rules and then trigger an automated email in another application and/or post an entry into a separate financial accounting system.

The business return on investment from replacing human mouse clicks with RPA bots to improve efficiency is significant. Companies are launching many RPA initiatives to enhance functions like payroll, accounts payable, accounts receivable and data extraction or processing, among many other core business functions.



Davenport and Ronaki, in their *Harvard Business Review* article, describe the next category as *cognitive insight* or "analytics on steroids," which organizations use to detect patterns in large volumes of data and interpret their meanings.

We can leverage statistics more than algorithmic rules in cognitive insights to predict a particular customer's buying preferences, identify credit fraud in near or real time, and automate personalized targeting of digital ads. Much of machine learning and predictive modeling come from this category of AI, including deep learning, which attempts to mimic the activity in the human brain to recognize patterns. Davenport and Ronaki write that organizations typically use cognitive insight applications to improve performance on jobs only machines can do — not people.

The third category is *cognitive engagement*. Davenport and Ronaki observed in their study that projects engaging employees, vendors or customers who used natural language processing chatbots, intelligent agents and machine learning were the least common type of AI — accounting for only 16% of the total use cases.

Applications of cognitive engagement in the study included intelligent agents (such as chatbots) that offer 24/7 customer service addressing a broad array of simple issues, such as password requests to technical support questions — all in the customer's natural language. Other examples included internal company sites for answering employee questions on topics, such as IT, employee benefits or HR policy, and product or service recommendation systems for retailers to increase personalization, engagement and sales.

Practical use cases in legal, compliance and investigations

Now, let's revisit our opening (fictitious but indicative) case with Michael in the context of what we now know about AI

and the three general categories. From a robotics and cognitive automation perspective, Michael can use AI to automate certain data refresh tasks as part of his company's compliance monitoring and audit analytics initiatives.

Traditionally, the data-gathering and validation aspects of any forensic data analytics project could consume up to 80% or more of the budgeted time, which leaves little room for the most value-added component — analysis and interpretation. But RPA can now automate manual and tedious data-gathering components.

Next is cognitive insight. Michael could recommend machine learning to improve fraud prevention and detection in high-risk transactions that his "rules-based" (e.g., matching, sorting, querying and filtering) anti-fraud and compliance analytics tools weren't providing.

For example, one consumer products company virtually eliminated a fake customer scheme with machine learning by simply profiling the key attributes of known fake customers obtained from previous investigations. When certain attributes were present, such as cash-only customers, lack of in-store product displays, discrepancies in the actual versus recommended product purchases and high amounts of customer returns — among several other variables — the model predicted fake customers with a 96% confidence rate.

The company, when it applied the model across its portfolio of customer transactions, identified many fake customers, plus the small group of employees who were creating them to meet bonus targets and divert marketing funds.

Companies have also used similar predictive models to identify high-risk payments to third parties as part of anti-bribery and corruption compliance programs. They analyzed known bribe payments to build profiles of high-risk vendors that fraudsters were paying with potentially improper company funds.

Finally, Michael can impress his management team by recommending cognitive engagement technologies. This is where compliance and anti-fraud efforts can get exciting. Fraud examiners and investigators conducting monitoring efforts can look beyond simple exception reports and engage employees directly using targeted communications or training guidance based on factual observations in the data.

Organizations are using more compliance chatbots for common questions and training purposes. Employees often feel more comfortable talking to a chatbot or submitting anonymous questions via compliance applications on their mobile phones. In one large telecommunications company, the compliance department noticed more than 1,000 inquiries in the chatbot asking, "What is a conflict of interest?" This helped the compliance team improve training and communications, and mitigate possibly hundreds, if not thousands, of potential policy violations.

I'm excited about what I like to call "Compliance 2.0" or "The Compliance Vision of the Future," in which fraud examiners and legal, risk and compliance professionals expand their training, policy guidance, reporting and investigation responsibilities to develop automated systems based on risk alerts from multiple data sources. For example, General Electric's compliance team incorporated all three categories of AI — automation, insight and engagement — to proactively build effective training and compliance guidance to high-risk employees who met "risk triggers" based on their historic travel and entertainment expenses, training histories, information on business sales opportunities and other factors. GE then would communicate friendly reminders to these high-risk employees to comply and hopefully prevent violations. (See the January/February 2018 "Innovation Update" column, tinyurl.com/y2bnp4h3.)

> We can leverage statistics more than algorithmic rules in cognitive insights to predict a particular customer's buying preferences, identify credit fraud in near or real time, and automate personalized targeting of digital ads.

Let's not create The Terminator

Michael also should consider the data privacy and regulatory aspects of AI when he presents his recommendations to management. Countries, including France, UAE, China, Germany, India and Singapore, have formed AI ethics committees to monitor the development of AI technologies.

In the U.S., on Feb. 11, 2019, the president signed an Executive Order on Maintaining American Leadership in Artificial Intelligence (tinyurl.com/y2fljv72). The U.S. House of Representatives introduced the Artificial Intelligence Job Opportunities and Background Summary Act of 2019 (known as the AI JOBS Act) on Jan. 28, 2019 (tinyurl.com/yxb2n9dr); the resolution, "Supporting the development of

guidelines for ethical development of artificial intelligence" on Feb. 27, 2019 (tinyurl.com/y5k6quux); and referred the Algorithmic Accountability Act to the House Committee on Energy and Commerce (tinyurl.com/yy2dapfj) on March 10, 2019.

Perhaps the Organization for Economic Cooperation and Development (OECD) best summarized the ethical considerations in its May 2019 AI policy guidelines, which the 36 member countries, including the U.S., signed and adopted. (Six non-member countries also signed the OECD guidelines: Argentina, Brazil, Colombia, Costa Rica, Peru and Romania.)

The guidelines identify five complementary values-based principles for the responsible stewardship of trustworthy AI:

- AI should benefit people and the planet by driving inclusive growth, sustainable development and well-being.
- AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards — for example, enabling human intervention where necessary — to ensure a fair and just society.
- There should be transparency and responsible disclosure around AI systems to ensure that people understand AI-based outcomes and can challenge them.
- AI systems must function in a robust, secure and safe way throughout their life cycles and potential risks should be continually assessed and managed.
- Organizations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles. (See tinyurl.com/y56epg4f.)

Regardless of the AI tools we incorporate, it's not a wise strategy for us to think that digital transformation with AI won't affect legal, compliance and anti-fraud functions of our organizations.

Doing nothing is no longer an option. We've gained too much — in dollar savings, business integrity and organizational culture — to not integrate advanced analytics, such as AI, into our fraud risk management programs. ■ FM

Vincent M. Walden, CFE, CPA, is a managing director with Alvarez & Marsal's Disputes and Investigations Practice. Walden welcomes your feedback. Contact him at vwalden@alvarezandmarsal.com.