BUILDING AN AI-FOCUSED ANTI-FRAUD COMPANY

Artificial intelligence (AI) is changing how businesses run – especially in anti-fraud and compliance. Here we describe how to build an AI-focused, anti-fraud technology company and what mindsets, strategies and tactics work well for organizations and entrepreneurs.

With billions of dollars stolen from U.S. pandemic relief programs, work has only just begun in tracking down the fraudsters who perpetrated such crimes and finding ways to prevent this kind of wrongdoing in future crises. Artificial intelligence (AI) is making that job easier and being adopted more and more by U.S. federal agencies and other organizations in their fight against fraud.

The Pandemic Response Accounting Committee (PRAC), a U.S. oversight agency for the emergency spending bills tied to the health crisis, has been using AI to pore over millions of records in search of fraud patterns. In one case, the technology reportedly helped PRAC track down a phone number of a Houston gas station that applied for 150 loans under the COVID programs, information PRAC quickly sent to federal agents. (See "'Biggest fraud in a generation': The looting of the Covid relief plan known as PPP," by Ken Dilanian and Laura Strickler, NBC News, Coronavirus, March 28, tinyurl.com/3x9wnm6s and "Using AI and machine learning to reduce government fraud," by Darrell M. West, The Brookings Institution, Sept. 10, 2021, tinyurl.com/4b3c2feh.)

TRADITIONAL TECHNOLOGY STARTUP	AI-DRIVEN STARTUP
Domain expertise and understanding the business problem (e.g., fraud prevention/ detection.)	
Develop product features.	Determine predictive model features.
Build a product.	Generate an accurate prediction.
Show a demo.	Show a report (with measurable results.)
Receive qualitative feedback.	Receive quantitative feedback.
Build more and more features.	Collect more data sources and samples.
Relaunch the product (version 2.0, 3.0, etc.)	Retrain the model.
Measure usage.	Measure accuracy.

Table 1

COLUMNIST
VINCENT M. WALDEN
CFE, CPA
CEO, KONA AI

Over the past 25 years, I've seen technology change a lot — and nothing has affected our profession as much as AI. In fact, the technological advances in AI inspired me to move from a consultant (who advises, then implements other people's technology) to recently becoming the CEO of a research-driven, AI-focused, anti-fraud prevention and detection software company.

Convergence of AI and anti-fraud

The ACFE's *Occupational Fraud 2022: A Report to the Nations* notes the median financial loss per case was $117,000, with over one in five cases having losses more than $1 million. (See ACFE.com/RTTN.) Half of those cases occurred because of a lack of internal controls or an override of existing controls. Clearly, there's an ROI case to be made for improving internal controls and increasing compliance monitoring. And in its most recent guidance, the U.S. Department of Justice (DOJ) expressed its support for machine learning and collaboration across

companies in a secure, data-sharing-type consortium.

The DOJ's "Evaluating of Corporate Compliance Programs" asks companies if they're incorporating lessons learned in their risk assessments with questions such as: "Does the company have a process for tracking and incorporating into its periodic risk assessment lessons learned either from the company's own prior issues or from those of other companies operating in the same industry and/or geographical region?" (See tinyurl.com/y6yyyaf8.)

Startups: What it means to be AI-focused

The goals of building a startup technology company versus an AI-focused one are notably different. An AI-focused startup is more than just a new company; it's geared toward completing a project, which I'll discuss in the next section. Instead of trying to get a product out the door, an AI-focused company is attempting to make its predictive model(s) accurate. Instead of having traditional product features as milestones, an AI-focused company has measurable model results. The output is a prediction (e.g., 25% likely to be a potentially improper payment) versus a mathematical calculation, or a rules-based test or query.

Table 1 on page 8 illustrates some of the mindset differences among the to-do lists for starting a technology company and an AI-driven company.

Building an AI-focused, rock-star team

So, here's the good news — as a fraud examiner, you've already completed the first checkbox and are on your way to building an AI-driven team. Looking at Table 2 on page 9, you'll note that building an AI-focused team doesn't start with software engineers. It starts with you, the anti-fraud professional with the expertise to ask the right risk questions. And you don't need to have all these individuals on your team from day one. In fact, the roles listed in Table 2 are in order of sequence. Bring on the data analyst first, then seek to add the data scientist and so forth as your number of recoveries and demand increase. One warning, however, as you move down the chart: Market demand (and hence, the cost) of these individuals goes up.

ROLE	BACKGROUND	ROLE EXAMPLES
Data analyst	Business/anti-fraud	Design anti-fraud tests, build dashboards, visualize data and interpret the results of the model.
Data scientist	Statistics	Set up and run experiments; e.g., hypothesis testing.
Data engineer	Databases	Identify data sources; extract, transform, load and clean data; create automated data pulls (internal and external to the organization); incorporate new data sources.
Machine-learning engineer	Computer science	Implement, train, monitor and fix machine-learning models.
Data-product manager	Product management	Incorporate data needs of a model with the business and usability intentions of the product design.
Data-infrastructure engineer	Distributed systems	Choose and set up correct databases, move data between databases, manage infrastructure, etc.
Machine-learning researcher	Machine learning	Set up and run experiments at a more senior, advanced level.
Software engineer	Computer science	Write the software code that delivers the model through an easy-to-use, intuitive interface; build application programing interfaces (APIs) to connect to other tools.
Designer	Graphics design	Design interfaces from an end-user experience perspective, including any interactive elements that seek feedback data from users and customers.

Table 2

Keep in mind that in today's market, the talent pool is scarce for these roles, and it'll take more than just money to bring good candidates on board. Generally speaking, professionals with these skill sets also want to be inspired. They want to use AI to solve real-world problems that matter — not just collect a paycheck. But what better, more exciting challenge than to build advanced algorithms to fight fraud, corruption and circumvention of controls?

AI tools to consider

Data scientists can't do much without the right tools. Giving them the resources to do great work helps inspire creativity. Technology tools are always changing, and people have their own personal preferences. However, Table 3 on page 10 is a summary example of the types of open-source and commercial tools by category to help get you started. Keep in mind your organization may already have access to these technologies, so be sure to ask around.

Machine-learning algorithms

As a baseline, there are five general categories of machine-learning (ML) algorithms: supervised, unsupervised, reinforcement, transfer and deep learning. The following are brief introductions to the categories. I encourage you to Google them because there's much more information available online.

Supervised learning is ideal when data is available, but the algorithm is unknown or missing. Supervised ML methods include random forest trees, decision trees, regression and neural networks. They're quite often used to find patterns or "profiles" of potentially improper transactions and risk-driving variables. (See "Understanding

SOFTWARE CATEGORY	EXAMPLES
Development environments	RStudio, PyCharm, Microsoft Visual Studio, JupyterLab, Jupyter Notebooks, Google Colaboratory, MathWorks, MATLAB.
Collaboration	Dataiku, Amazon SageMaker, Datarobot, Altyryx.
Frameworks	Open-source tools like Keras, Apache Spark, PyTorch, XGBoost, Google TensorFlow.
Cloud platforms	Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform, IBM Cloud and SAP Cloud.
Pre-trained models	Various open-source software tools are available online, as well as pre-built models in Google Cloud Platform, Amazon Rekognition and Microsoft Azure.
Machine learning	Google Cloud Platform, AutoML, AWS Comprehend & Rekognition, Microsoft AutoML, H2O.ai and DataRobot.
Visualizations	Tableau, Qlik, Spotfire, Domo, Microsoft PowerBI and Microsoft Excel.
Data preparation	Informatica, Trifacta, Alteryx, Paxata and Tamr.

Table 3

Random Forest," by Tony Yiu, Towards Data Science, June 12, 2019, tinyurl.com/3dabtvth and "A Walk-through of Regression Analysis Using Artificial Neural Networks in Tensorflow," by Srivignesh Rajan, Analytics, Vidhya, Aug. 16, 2021, tinyurl.com/wcskkw5b.)

Unsupervised learning, on the other hand, is ideal when there's less information about the risks, but you want the data to help define itself by grouping like events (or transactions) together. This can be particularly helpful in fraud detection when you're looking for anomalies or patterns in data without applying any preset rules.Techniques that can be used in unsupervised learning include K-means clustering and Apriori algorithms. (See "Apriori Algorithm," GeeksforGeeks, updated January 13, tinyurl.com/2w9rwkm5, and "K-Means Clustering, What Does K-Means Clustering Mean?" techopedia.com, dictionary, tinyurl.com/m8mmj8rx.)

Reinforcement allows a user to decide the best action based on the current state and learned behaviors that maximize the rewards. This approach is often used in robotics where the computer trains itself continually using trial and error. The machine learns from experience and tries to capture the best possible knowledge to make accurate business decisions. In fraud detection, reinforcement techniques can be helpful with some of the necessary data extraction and cleanup required to prepare data for analysis, for example.

Transfer learning focuses on storing knowledge gained while solving one problem and applying it to a different, but related, problem. For example, knowledge gained while learning to recognize cars could apply when trying to recognize trucks. Transfer learning is good when problems are similar, the time to train a model is limited and results are needed fast. Bayesian networks and Markov logic networks are effective transfer learning methods. In an anti-fraud context, transfer learning can help uncover conflicts of interest by finding hidden patterns and relationships, such as in an unauthorized employee and vendor relationship. (See "A friendly introduction to Bayes' Theorem and Hidden Markov Models," by Luis Serrano, Udacity, YouTube, March 27, 2018, tinyurl.com/2p84p6je.)

Finally, there's *deep learning*. According to IBM, deep learning attempts to mimic the human brain — albeit far from matching its ability — enabling systems to cluster data and make predictions with incredible accuracy. Deep learning is ideal when there's lots of unstructured time series data or data that's not independent. Deep learning drives many AI applications and services that improve automation, performing analytical and physical tasks without human intervention. Deep-learning technology lies behind everyday products and services, such as digital assistants, voice-enabled TV remotes and credit card fraud detection, as well as emerging technologies, such as self-driving cars.

As you think about the potential for your own business, I encourage you to consider building an AI-focused, anti-fraud program in your organization by applying some of these concepts. While I embark on my new journey in the AI business, I'm excited about the possibilities for using it to measurably prevent and detect more corruption, fraud, waste and abuse — and when you see how AI tools and strategies can successfully increase your anti-fraud results, I think you will be, too. ■ FM

Vincent M. Walden, CFE, CPA, is the CEO of Kona.AI, an AI-driven anti-fraud and compliance technology company providing research-driven, proven AI models around corruption, fraud prevention and detection. He welcomes your feedback and ideas. Contact Walden at vwalden@kona.ai. Walden acknowledges Ash Fontana, author of "The AI-First Company: How to Compete and Win with Artificial Intelligence," for many of the AI concepts discussed in this column.

INVEST IN THE FUTURE

of the Anti-Fraud Profession

The ACFE Foundation funds research critical to advancing our knowledge of how to prevent and detect fraud through the ACFE Research Institute (ARI) — a multidisciplinary research center that works with academics and industry experts worldwide to generate research projects.

The Foundation also encourages students to pursue careers in fraud examination and supports the education of the next generation of CFEs through the Ritchie-Jennings Memorial Scholarship Fund. Since 1996, nearly $1 million has been distributed to more than 600 students in scholarships.

With the help of your contributions, the ACFE Foundation can continue to increase the body of anti-fraud knowledge and support future anti-fraud professionals worldwide.

The ACFE Foundation is a 501(c)(3), tax-exempt organization. Contributions to the ACFE Foundation are tax-deductible to the extent allowed by law.

ACFE FOUNDATION