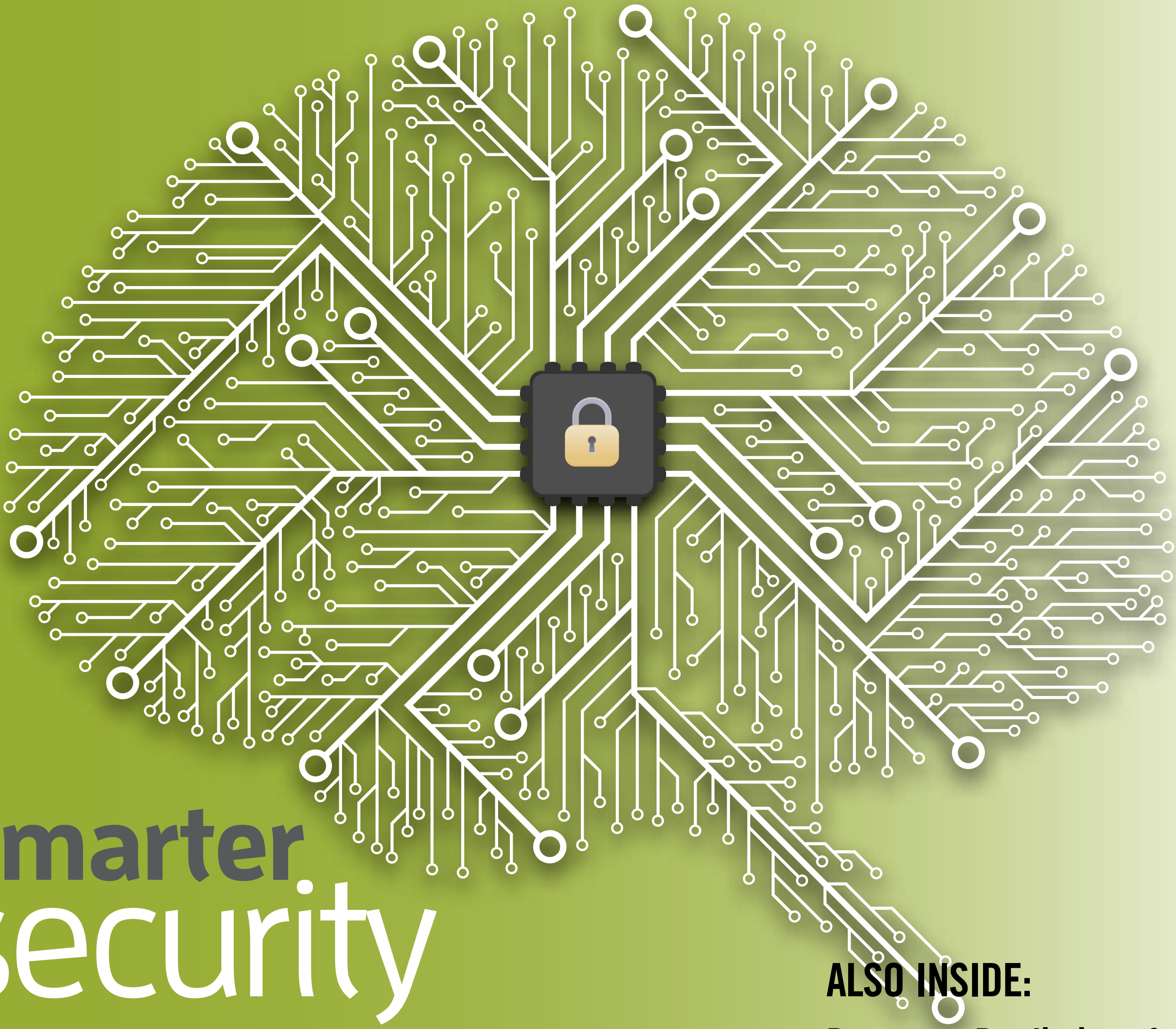
Exclusive: New Guidelines for Underwriting and Risk Monitoring PAGE 16

January/February 2016

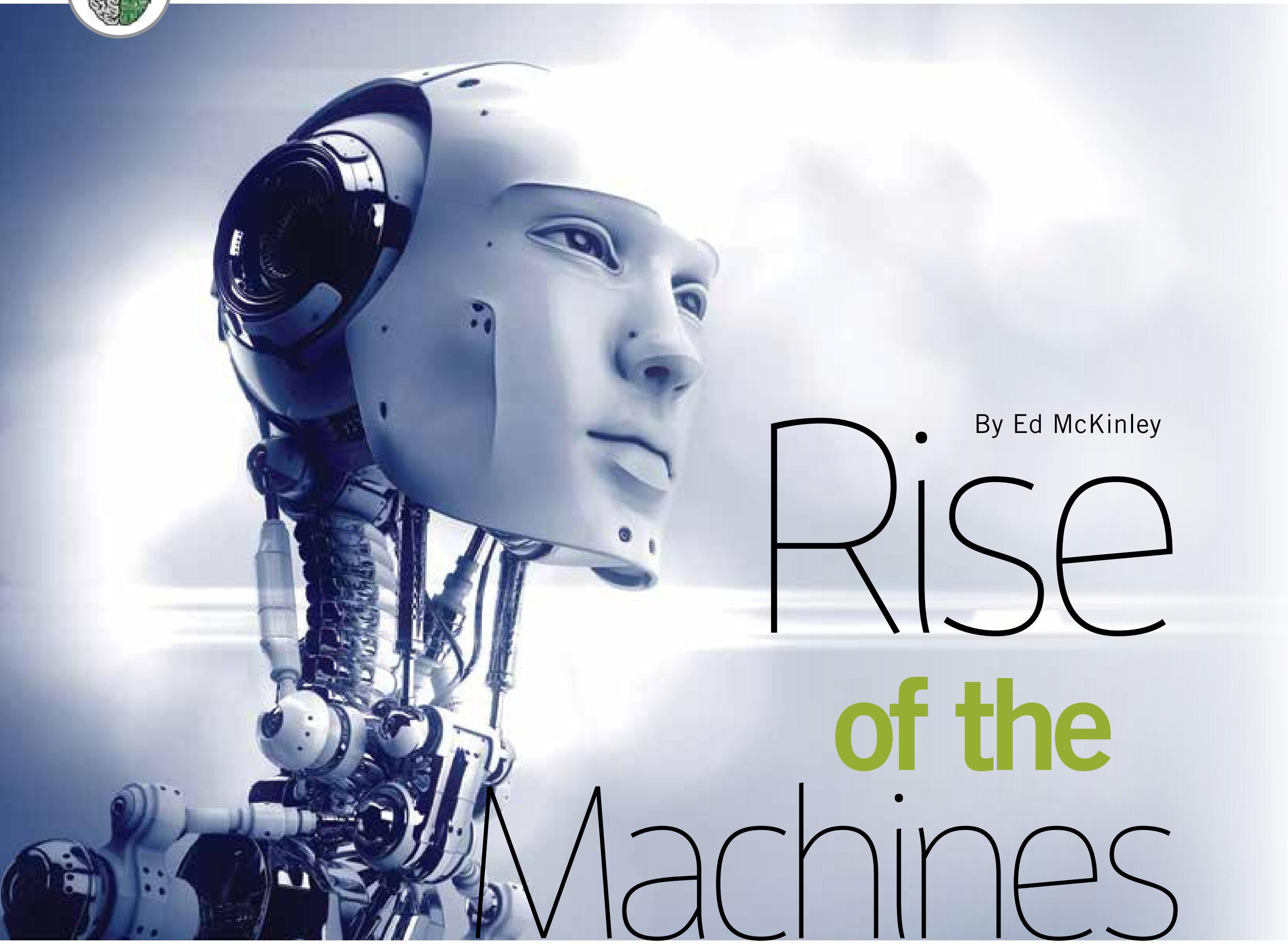
TRANSACTION trends

ETA THE OFFICIAL PUBLICATION OF THE ELECTRONIC TRANSACTIONS ASSOCIATION



Smarter security

Data protection reaches new levels of sophistication



By Ed McKinley

Rise of the Machines

As big banks and payments pros add AI to their IT systems, use cases emerge for security, merchant monitoring, and more

For generations of movie fans, the phrase "artificial intelligence" brings to mind the computer HAL 9000's unblinking red eye and chillingly calm voice in the film *2001: A Space Odyssey*. Others might think of actor Haley Joel Osment's portrayal of the robot child capable of love in the movie *A.I.* But yesterday's science fiction can become today's science, and the term "AI" is now entering the vocabulary of the payments business.

Still, opinions vary on what exactly AI means. For Rich L. Stuppy, chief operating officer of Kount, a fraud and risk-management vendor, AI came into being during the middle of the 20th century, when computers began following orders. But the public's definition of AI, he says, became a moving target, redefined as whatever lies just beyond the current state of computer technology. Julie Conroy, research director for Aite Group's retail banking practice, offers a different interpretation: "It's when you have computer technology that's able to learn on the fly from new inputs without having to go back and be retrained. 'Unsupervised model' is one of the buzz words."

Todd Clark, senior vice president for First Data Corp. and head of the STAR Network and Debit Processing Group, provides a helpful analogy: It's as broad and vague as saying "automobile" instead of "1957 Chevy Bel Air." In his last job, Clark served as senior vice president of worldwide sales for Feedzai, an AI vendor. He's more comfortable discussing the specific idea of "machine learning" than the larger concept of AI. Machine learning's underlying algorithms make it quicker to train, quicker to learn, and more able to handle a high volume of work than other forms of AI, he says.

Matthew Parker, cofounder of a vendor called KYC SiteScan, agrees that it's preferable to focus discussion on machine learning instead of trying to pin down the vague notion of AI. "We have a lot of discussions internally about AI," he says of the semantics involved. "It's a layman's term. From a technical point of view, it doesn't exist."

Payments professionals often prefer to think of AI as machine learning or automated decision-making. By those definitions, it's already becoming a force in the industry's perennial struggle to maintain a technical advantage over data thieves. That's important because "when the merchant is either unwilling or unable to honor that chargeback, we stand in the shoes of the merchant and make that cardholder whole," notes Geoffrey Stocki, vice president of operations for acquirer and transaction processor North American Bancard.

AI can also foil bogus merchants. "The business case hinges on the need to understand your merchants' behaviors," Conroy says. "Is this merchant real, and is he really selling what he says he is?" Some industry players regard AI as the power behind the Know Your Customer (KYC) and Anti-Money Laundering (AML) processes. Both acronyms carry a "compliance connotation," and, as Conroy explains, they're becoming increasingly important to acquirers as concern about regulation intensifies.

Profit From the Statistics

Whichever term suits—the broad AI or the precise machine learning—the discussion soon proceeds beyond programming based on simple instructions, according to Sandeep Grover, senior vice president of global e-commerce at Feedzai. He says it's not just telling a computer that "if" a certain thing happens, it should "then" perform a specified task. To explain the complexity, Grover suggests thinking of self-driving cars.

Simply writing rules for a computer produces a few overly generic categories that cannot begin to take into account the vast number of cases that can become part of the model that results from the observations of machine learning, Grover continues. When changes occur in the market, machine learning adjusts immediately, as opposed to human-driven reaction that can take a long time, he maintains.

However one chooses to understand AI, the technology lived on the "bleeding edge" just a few years ago and now constitutes the "wave of the future," according to Clark. Setting up or modifying AI takes days instead of weeks or months, he says, and its workings are measured in milliseconds.

> "THE BUSINESS CASE HINGES ON THE NEED TO UNDERSTAND YOUR MERCHANTS' BEHAVIORS. IS THIS MERCHANT REAL, AND IS HE REALLY SELLING WHAT HE SAYS HE IS?"
>
> —JULIE CONROY, AITE GROUP

At First Data, the number of use cases for machine learning appears endless. It's useful anywhere the company has a lot of data. And AI makes the data practical because it shows the reasons for rejecting a particular file instead of merely saying it's rejected, he notes.

The company is using machine learning for merchant underwriting, Clark says. Instead of underwriting merchants when they sign on and then checking on them again once a year, machine learning allows the company to track every transaction. The security division also is using machine learning to assess companywide threats

Bonus Audio Content: Log in to listen to "Lessons from Implementing Machine Learning" from TRANSACT 15. Visit http://bit.ly/1sD7bzF.

to its own systems, he says.

First Data often comes up in industry discussions of AI or machine learning prowess, but the company's not alone at the forefront. Late last year, North American Bancard began testing a machine-learning tool that the company refers to as a custom risk-scoring model, says Stocki. He considers the system so "cutting edge" and such a great "competitive advantage" that he declines to name the vendor working on it.

The system monitors transactions and builds a statistical record of the ones that result in chargebacks, he says. By learning what characteristics indicate risk, the system becomes better at detecting potential problems, Stocki says. "Over time, the system refines the model," he maintains.

If, for example, someone is making $200 purchases in a coffee shop at 11 p.m., that merchant might be selling something other than coffee, he notes. In another example of suspicious behavior, a thief might repeatedly make significant purchases in a short time with the same card, indicating a merchant or customer is using stolen card information.

"MACHINE LEARNING ALLOWS US TO LOOK FOR ANOMALIES AND PATTERNS THAT ARE DOWN TO A FIELD OF ONE. THE RESULTS ARE EXTREMELY PROMISING."

—TODD CLARK, FIRST DATA CORP.

The relief isn't limited to the acquiring business. The STAR Network began using AI to monitor transactions internally last summer and started sharing the results with customers in January, Clark says. It can push all of its volume through, not just a subset of it. "It's kind of like that '95 Impala and a Tesla," he notes, continuing the automotive analogy. "Both cars—but very different."

The STAR Network doesn't view AI from a KYC or AML perspective because all it has to work with is a card number, not the cardholder's name or other information, Clark explains. So the company bases decisions on how and where the cardholder used the card in the past. "We're using Feedzai's engines to develop a profile of that card," he says.

Until now, a company might have tracked American Express transactions, documenting, for example, that green card customers spend $300 a month and sometimes make late payments, gold card users spend $2,000 a month and pay on time, and platinum card shoppers spend $5,000 a month, Clark explains. "With machine learning, we're able to take it down to an individual card level," and know what constitutes usual behavior with a single card. That means if a customer who generally doesn't shop on weekdays and doesn't buy clothes walks into a Gap and buys $400 worth of jeans, something's possibly amiss.

That granular detail isn't possible with a rules-based approach because it would require humans to write so many rules. With machine learning, however, that level of detail becomes possible. "You don't have to have a thousand people sitting in a room poring over data," Clark observes. "Machine learning allows us to look for anomalies and patterns that are down to a field of one." The results are extremely promising, he says of what the company is achieving with AI. However, good results require a basis of good data, he asserts.

Consumers Cognition

It's also important to note, Clark insists, that machine learning can improve the customer experience by reducing the number of valid transactions that are rejected. Vitally, it can do that without slowing down the process, he asserts. "If we continue down this path, STAR will have the highest approval rate and the lowest fraud rate in the industry," he says. "That's our stated goal."

Elsewhere, North American Bancard finds other uses for the technology that's arguably akin to AI. It helps automate the work of evaluating, bringing onboard, and monitoring merchants. In the past, employees spent time researching prospective clients with computer searches, street maps, Yellow Pages listings, Better Business Bureau complaints, and government records of pending actions, says Stocki. Now, software from KYC SiteScan scans records automatically and produces a document with its findings, Stocki says. His company has added that capability to the automated, customized underwriting workflow process created with another vendor, ContractPal Inc. It entails writing rules that direct the program to notify humans when particular situations arise.

"If we get a hit on the CFPB [Consumer Financial Protection Bureau] site, for example, it kicks it out for an underwriter to review instead of sending it on to the next step," Stocki says. "So, we're spending our underwriters' time only where there's a problem that needs review." When problems don't arise, a less-skilled employee can handle the application without the help of a more-qualified underwriter, he says. Some applications receive approval without review by a credit analyst because they meet all of the criteria, Stocki explains. "We're able to give credit decisions in minutes instead of hours or days."

Matching what's on the application with what's available in public records has reduced the number of cases where criminals succeed in stealing a merchant's identity "tremendously," according to Stocki. Although it's hard to quantify, he suggests automation has reduced the number of fraudulent accounts boarded by at least 10 percent.

Automated onboarding has improved the customer experience by decreasing waiting time for merchants that don't require extensive review. For example, at nail salons, where the services have been rendered, chargebacks seldom occur, there's no forward delivery, and the cardholder is present for the transaction, Stocki says. "They can be processing with us the very next day," he notes.

Watchful Eyes

About 60 percent of merchant applications that acquirers process with KYC SiteScan meet the automated standards and don't require human review, says Parker. Acquirers shouldn't reject applications without having a human set of eyes on the file, he suggests. The human touch remains vital, agrees Clark. "Sometimes they do end up in the hands of humans," Clark says of cases that call for decisions. "This is not a matter of turning the machines loose to figure it all out."

The system flags possible problems but doesn't get the final say. "It doesn't remove the human element," Stocki says. "The fear is that the machines are going to take over, but there's no substitute for human judgment." The system merely flags inconsistencies for humans to review, he says. People judge the relevance of an anomaly and consider the circumstances surrounding it.

"If you had enough horsepower, you could probably program a machine to go through the variations of it, but, at this point in time, [the systems] aren't ready for that," Stocki says.

Even if they fall short of taking total responsibility for security, such systems could do a lot to keep merchants ahead of criminals bent on finding the newest ways to crack computer systems to steal card data, Stocki says. "We can save ourselves a lot of heartache," he observes.

By using AI to enhance security and avoid those heartaches, professionals in the payments industry believe such exemplary behavior could make state and federal regulators look upon them more favorably. Scrutiny by agencies like the Federal Trade Commission and the CFPB is forcing acquirers to maintain 24-7 vigilance, according to Barry Sloane, president, chairman, and CEO of Newtek Business Services Corp. The federal government's Operation Choke Point accused a Newtek subsidiary of wrongdoing in processing payments for a client engaged in illegal telemarketing schemes. The Feds obtained a monetary judgment against Newtek in federal court, but Sloane says the company has filed an appeal.

Sloane advocates combining technology like AI with human-powered diligence to avoid problems: "It would be great to have a solution where you run everything through a computer model, and it does everything for you. Unfortunately, the world doesn't work that way."

Regulation makes news, but Stocki claims he doesn't lose sleep over it because his company is campaigning to prevent losses to consumers and merchants. As he says, "If you're doing the right thing, you should have nothing to fear." ***TT***

Ed McKinley is a contributing writer for Transaction Trends. *Reach him at edmckinley773@yahoo.com.*