ANALYTICS AND THE AML PARADIGM SHIFT

David Stewart of SAS on How to Separate Promise from Hype
As financial organizations deploy artificial intelligence and machine learning in the fight against financial crimes, David Stewart of SAS offers tips to help separate fact from market hype when reviewing new data analytics tools.

These emerging technologies and solutions certainly are not unique to financial services. But Stewart, a business director of security intelligence solutions within the SAS Security Intelligence Practice, sees particular interest and application in AML circles.

"There remain a good number of manual processes within financial crimes departments in financial institutions, and AI can help automate some of those rote tasks such as document review or alert triage," he says. "Due to investments in technology, there is a lower barrier of entry for midsized institutions.

"And finally, there's this anxiety over the unknown - those risks they are not able to detect, that may be hidden using traditional techniques - so they're hoping that more advanced, unsupervised learning techniques can be used to identify those edge cases or behaviors that are out of norm."

In an interview about analytics and the AML paradigm shift, Stewart discusses:

- The new industry intrigue with artificial intelligence and machine learning;
- How these emerging solutions can benefit financial institutions;
- The SAS approach of "crawl, walk run" when it comes to adopting new analytics tools.

Analytics and the Anti-Money Laundering Paradigm Shift

TOM FIELD: David, throughout the industry we're seeing a lot of hype, a lot of excitement over artificial intelligence, machine learning and analytics. Tie this back to anti-money laundering for me, and why do you find the industry to be so intrigued by these emerging technologies?

DAVID STEWART: Tom, I think there's probably three key reasons why AI is so intriguing for the industry, particularly within anti-money laundering compliance. First of all, there's frustration over the effectiveness of rules-based or typology-driven transaction monitoring strategies that have been deployed for the last 10, 15 years. The high false positive rates and subsequent staffing costs to review all of those work items has been so extreme that it's really no longer sustainable for many banks to continue that expenditure. There's this call from industry stakeholders to modernize the current AML/CFT regime, and they're looking for AI to assist with that.

Also, I think AI has become personal thanks to autonomous vehicles, Siri, Alexa or what have you. We're starting to experience AI firsthand. I think there'll remain a good number of manual processes within financial crimes departments of financial institutions, and AI can help automate some of those rote tasks like document review or alert triage, for example. Due to investments in technology, there's a lower barrier to entry for mid-size institutions. Finally, I think there's this anxiety over the unknown, those risks that they're not able to detect that may be hidden using traditional techniques where they're hoping that more advanced unsupervised learning techniques can be used to identify those edge cases or behaviors that are out of norm.

Key Regulatory Challenges

FIELD: David, over the past few years, payment card fraud cybercrimes have really gotten common in the headlines, but you and I both know that AML has remained an important component for financial institutions. What have you seen to be some of the key regulatory challenges that have emerged in recent years?
“Compliance departments and regulators aren’t necessarily known for their agility, so there’s going to be a tremendous amount of change in business process and cultural change... in the industry.”

STEWART: With respect to the adoption of analytics and particularly AI, I think one challenge is subjectivity. First of all, institutions have an obligation to file a SAR or an STR for potential suspicious activity. That’s a very subjective definition and may vary from one institution to another either depending upon risk appetite or geography. You don’t have that clear binary, yes/no delineation in AML the way you do in fraud, so that creates ambiguity. That in turn impacts the output that you derive from some of these self-learning analytical strategies. The subjectivity is a bit of a challenge in AML.

The other is transparency. Traditionally, AML departments want a clear explanation of why an alert fired, which transactions were associated with the alert, etc. It’s going to be incumbent upon auditors, examiners and regulators to become comfortable with some of these new methods where the output from the models may not be as easily explainable. I expect the model governance process will shift somewhat, perhaps where they validate models alongside investigators so the investigations units themselves trust the model output.

The other key regulatory challenge is going to be from a workforce perspective. There’s going to be an impact on existing workforce across the board, especially for regulators, bank examiners and auditors. Are we going to have a workforce that’s capable and comfortable with this new regime, etc? Compliance departments and regulators aren’t necessarily known for their agility, so there’s going to be a tremendous amount of change in business process and cultural change, I think, in the industry. Those would be some of the key challenges I think you’d expect to see.

Tangible Opportunities in AML Compliance

FIELD: Okay, so if we turn that around, talk about opportunities, what are some of the tangible opportunities that you see in AML compliance?

STEWART: We use that term horizon scanning. I think, first of all, there are a lot of proven analytical strategies that have been deployed in fraud and credit risk, and other types of risk management practices that are proven, and tangible, and have legs. It’s funny, back in 2002, we delivered a principal components analysis, PCA, model to an AML development partner, and they told us to, “Put that away. We just need rules. We don’t need that stuff.” It’s funny now, PCA is very much en vogue as a dimension reduction technique. Since about 2009, we’ve been using some fairly advanced analytics with what I call innovators, or early adopters in the AML community. First of all, segmentation, using unsupervised clustering techniques, for example, to build tighter segments which then can be used for anomaly detection. We’ve seen in some of these practices, we’ve seen 4x to 6x improvement in SAR conversion rates just doing more analytical segmentation.

A very popular technique is something called an auto referral, or hibernation model. It’s something we’ve been doing since about 2008 or ’09. Basically, you deploy learning models that learn from past case decisions, and you create groups of productive and non-productive investigations. Then we deploy predictive ensemble models that determine whether alerts should lie in a wait state or hibernate, or if it scores high enough, promote it for further
investigation. This approach can eliminate unnecessary work by 50 percent, [which] is what we've seen in the real world.

Another area where we've been doing some interesting research is we've been testing cognitive computing capabilities for character recognition. In a pilot with a major bank, our models were able to accurately identify handwritten trade finance documents with about a 99 percent accuracy. To do this process for the mound of the documents that we ran through the process, it would've taken a human several weeks to review all of those documents. Generally, humans review documents when fairly fatigued at less than ~95% percent accuracy. We reduced that process from several weeks to 26 seconds in an automated process. Those kind of results get you pretty excited about the possibilities.

Another area is scenario authoring. We developed a product that used decision trees to author AML scenarios, and it received a lot of interest and curiosity. Instead of creating typical floors and ceilings of parameter values, we took more of a laser approach and we would use specific leaves of a population of data, if you will, for scenario parameter values. You could deploy a dozen challenger rules in a few minutes using in-memory technology that would've traditionally run overnight in batch. That's just a handful of tangible examples of where we've applied machine learning or advanced analytics, and in the case of cognitive computing, really AI, that have tangible applications within AML compliance.

“Another area where we've been doing some interesting research is we've been testing cognitive computing capabilities for character recognition. In a pilot with a major bank, our models were able to accurately identify handwritten trade finance documents with about a 99 percent accuracy.”

Where is the AML Industry Going and How Can SAS Help?

FIELD: David, those are great examples, and they hammer home the point that SAS is no newcomer to analytics. From your perspective, when you look at artificial intelligence, machine learning, analytics, where do you see this industry going, and how is SAS helping its customers to get there?

STEWART: At SAS, we’re excited that financial crimes risk management practices are embracing AI because analytics is our wheelhouse. There’s a lot of debate in the industry on how much will be automated by machines in the future. If you have read some of the comments by Elon Musk, he paints a very apprehensive picture. In the UK, the regulators are suggesting that AI could reduce ambiguity, especially in securities and trade activity. What’s unique about SAS and how we’re helping customers get there is we have the advantage of not only providing analytical tools, but we also have over 15 years of experience in operationalizing fraud and AML solutions. We understand the balance the industry needs to take between human intelligence and artificial intelligence. In our mind, this is more of an evolution, not a revolution.

In the near term, you’ll continue to see process automation in the investigative processes, things like case enrichment or what’s commonly called RPA - robotics process automation. Investigators won’t have to manually search subjects or go to source systems or green screens. All of the necessary information will be automatically presented to speed up the decision process. All of our new interfaces use REST APIs to make it easier to interact with other data and processes. With respect to unstructured data, whether those are images, voice or text from a web app, natural language processing and cognitive computing will be used to automate manual processes. It will also raise the sophistication of authentication on mobile devices, and I think make it harder for fraudsters to compromise our accounts.

For the innovators in the industry, the early adopters, they’re already piloting the use of modeling techniques like gradient boosting, support vector machines and random forests to identify suspicious activity or fraud that may fly under the radar of simple Boolean logic. I call them the false negative hunters. I would expect over the next few years for certain types of risks, those techniques will replace traditional rules. If we look farther out, the advancements in chips, particularly GPUs, or graphical processing units, will enable deep learning and enable many more layers, hidden layers to be used in

Analytics and the AML Paradigm Shift
“Despite the hype around AI, you have to admit that there are opportunities right in front of us to improve processes and automate manual tasks so you can allocate your investigative resources on the serious risks that threaten your reputation.”

neural networks where we're actually trying to simulate human reasoning and solve complex problems. That work today is primarily being done in academia. I would expect to see this over the next three to five years being deployed in industry.

Pragmatic Recommendations

FIELD: David, before we sat down for this recording, you and I talked a little bit and you shared with me your philosophy about when it comes to analytics, one first must crawl, then walk, and then run. With that as our backdrop, what are your pragmatic recommendations to organizations regarding analytics in this methodology, crawl, walk, run?

STEWART: Tom, despite the hype around AI, you have to admit that there are opportunities right in front of us to improve processes and automate manual tasks so you can allocate your investigative resources on the serious risks that threaten your reputation. At SAS, we always recommend a hybrid approach. By a hybrid approach, what we mean is improve and optimize your existing systems so you can go out and play and have fun, and do more innovative things over time. We would say first, everything begins with data. Beginning with data quality, do you have a single view of [the] customer? We’re doing entity resolution projects right now with a number of pretty sophisticated clients to help them identify counterparty exposure in correspondent banking, for example. Get your data tight, improve the quality of your data.

There's also, generally speaking, an opportunity to review your segmentation strategies and move beyond those business-defined segments to more of a behavioral segment or behavioral profiles based upon actual activity. We've talked about the 4x, 6x improvements that these segmentation strategies can derive. Then tune what you have. Tune your scenario thresholds of your scenarios that perform reasonably well to improve your coverage and conversion rates. Not all rules are inherently bad, especially for known risks like cash or PEPs, for example.

Automate where it makes sense, particularly your alert to case decisions, to eliminate repetitive work. Don't just automate, but aggregate. In other words, make your case decisions at a customer or party level as opposed to transaction or account level. Those aggregation strategies reap huge productivity gains and really provide a truer picture of client risk. Another thing you can do is extend your visualization capabilities beyond typical operational dashboards and use some of the geospatial analysis and entity link analysis to analyze funnel account activity, flow of funds, and just identify trends that may be early warning signs of risks at a portfolio or book of business level.

Finally, establish a sandbox for innovation, once you've tightened up everything else, taking advantage of big data architectures so that we can deploy these technologies against very large datasets and rapidly simulate various monitoring or fraud prevention strategies against data that's more representative of your production environment. What this does is it allows you to more accurately assess your operational impact to deploy new analytics and to compare results of models compared to the alert output of your traditional rules. You would typically compare some of the more innovative techniques alongside of your BAU environments so that you could over time roll off some of your incumbent processes, and again, be a bit more innovative. For 99 percent of the institutions we deal with, we could create order of magnitude gains in efficiency and effectiveness just by tightening up each of these functional areas. Once these areas are optimal, you now free up resources so that you can invest in data scientists to run with AI. That's how we plan to help our customers evolve.

Listen to the full interview: http://www.bankinfosecurity.com/interviews/analytics-aml-paradigm-shift-i-3651
About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io