Singapore Management University

Institutional Knowledge at Singapore Management University

Research Collection School Of Computing and Information Systems | School of Computing and Information Systems

10-2020

The future of work now: AI-driven transaction surveillance at DBS Bank

Thomas H. DAVENPORT
Babson College

Steven M. MILLER
Singapore Management University, stevenmiller@smu.edu.sg

Follow this and additional works at: https://ink.library.smu.edu.sg/sis_research

 Part of the Artificial Intelligence and Robotics Commons, Asian Studies Commons, Databases and Information Systems Commons, Finance and Financial Management Commons, and the Strategic Management Policy Commons

Citation

DAVENPORT, Thomas H. and MILLER, Steven M.. The future of work now: AI-driven transaction surveillance at DBS Bank. (2020). *Forbes*. 1-5.
Available at: https://ink.library.smu.edu.sg/sis_research/5341

This Magazine Article is brought to you for free and open access by the School of Computing and Information Systems at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Research Collection School Of Computing and Information Systems by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email cherylds@smu.edu.sg.

The future of work now: AI-driven transaction surveillance at DBS Bank

Published in Forbes, 2020 October 23

Tom Davenport and Steven Miller

https://www.forbes.com/sites/tomdavenport/2020/10/23/the-future-of-work-now-ai-driven-transaction-surveillance-at-dbs-bank

One of the most frequently-used phrases at business events these days is "the future of work." It's increasingly clear that artificial intelligence and other new technologies will bring substantial changes in work tasks and business processes. But while these changes are predicted for the future, they're already present in many organizations for many different jobs. The job and incumbents described below are an example of this phenomenon. Steve Miller of Singapore Management University and I co-authored the story.

Since the passage of the Bank Secrecy Act in the U.S. in 1970, banks around the world have been held accountable by governments for preventing money laundering, suspicious cross-border flows of large amounts of money, and other types of financial crime. DBS Bank, the largest bank in Singapore and in Southeast Asia, has long had a focus on anti-money laundering (AML) and financial crime detection and prevention. According to a DBS executive,

"We want to make sure that we have tight internal controls within the bank so the perpetrators, money launderers, and sanctions evaders do not penetrate into the financial system, either through our bank, through our national system, or internationally."

Like other large banks, the area of DBS that focusses on these issues, called "Transaction Surveillance," has taken advantage of artificial intelligence for many years to do this type of work. The people in this function evaluate alerts that are raised by a rule-based system. The rules assess transaction data that come from many different systems across the bank including those for consumers, wealth management, institutional banking and their payments, and the various channels within each of these major areas. These transactions all flow through the rule-based system for screening, and the rules flag transactions that match conditions associated with an individual or entity doing suspicious transactions with the bank—those involving a potential money laundering event, or another type of financial fraud. Rule-based systems—in the past known as "expert systems"—are one of the oldest forms of AI, but they are still widely used in banking and insurance, as well as other industries.

At DBS and most other banks across the world, these types of rule-based financial transaction surveillance systems generate a large number of alerts every day. The primary shortcoming of rule-based surveillance systems is that most—up to 98%—of the alerts generated are "false positives." Some aspect of the transaction triggers a rule that leads it to be flagged on the alert list. However, after follow-on investigation by the human analyst, it turns out that the alerted transaction is actually not suspicious.

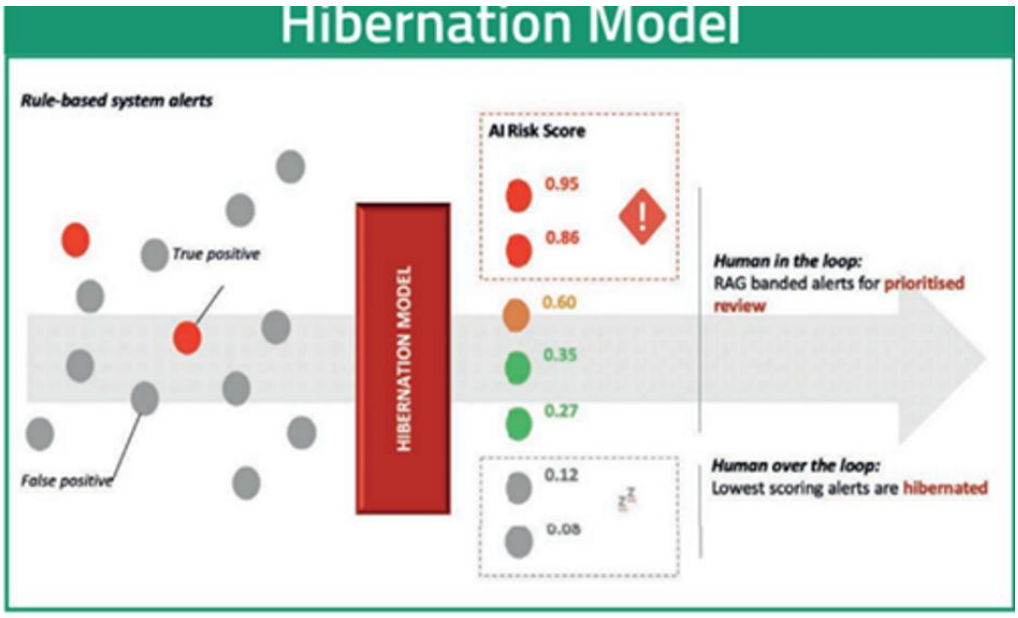
The transaction surveillance analysts have to follow up on each and every alert, looking at all the relevant transaction information. They also consider the profiles of the individuals involved with the transaction, their past financial behaviors, whatever they have declared in "Know Your Customer" and Customer Due Diligence documents, and anything else the bank might know about them. Following up on alerts is a time intensive process. Having an automated system that generates a large number of alerts, most of which turn out to be false positives, does not save human labor.

If the analyst confirms that a transaction is justifiably suspicious or verified as fraud, the bank has a legal obligation to issue a “Suspicious Activity Report” (SAR) to the appropriate authorities. This is a high-stakes decision so it is important for the analyst to get it right: if incorrect, law-abiding bank customers could be incorrectly notified that they are being investigated for financial crimes. On the other side, if a “bad actor” is not detected and reported, it leads to problems related to money laundering and other financial crimes.

For now at least, the rule-based systems can’t be eliminated because the national regulatory authorities in most countries still require them. But DBS executives realized there are many additional sources of internal and external information available to them that, if used correctly, could be used to automatically evaluate each alert from the rule-based system. This could be done using machine learning (ML), which can deal with more complex patterns and make more accurate predictions than rule-based systems.

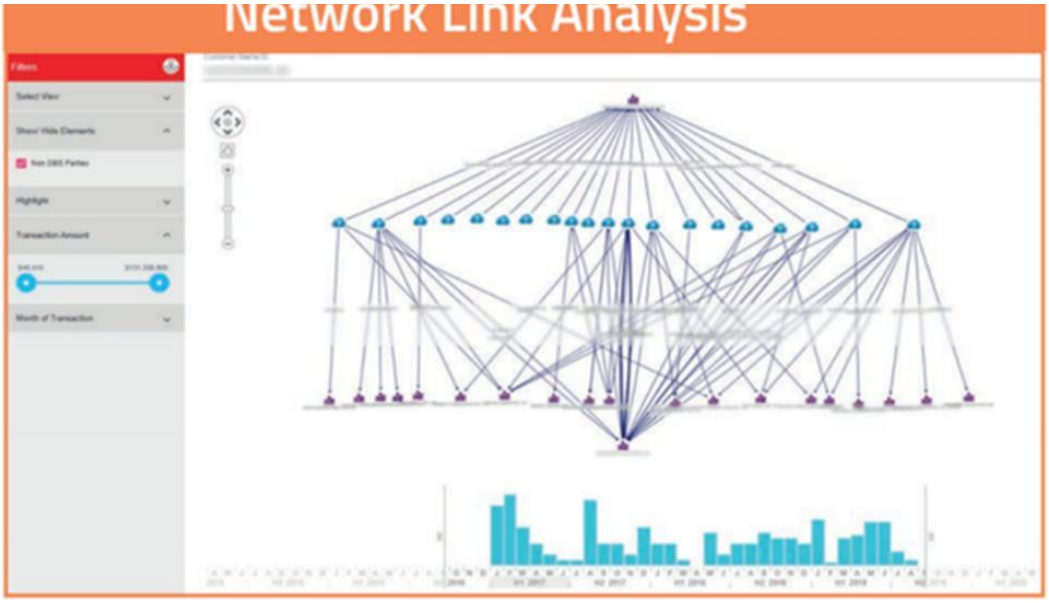
A few years back, DBS set out on a project to apply the new generation of AI/ML capabilities in combination with the existing rule-based screening system. The combination would enable the bank to prioritize all of the alerts generated by the rule-based system according to a numerically calculated probability score indicating the level of suspicion. The ML system was trained to recognize suspicious and fraudulent situations from recent and historical data and outcomes.

The new ML based filtering system (see figure below) has been in use for just over one year. It reviews all of the alerts generated by the rule-based system, assigns each alert a risk score, and also categorizes each alert into higher, medium, and lower risk categories. This type of “post-processing” of the rule-based alerts enables the analyst to decipher which ones to immediately prioritize (those in the higher and medium risk categories) and which ones can wait (those in the lowest risk category). An important capability of this ML system is that it has an explainer that shows the analyst the evidence used in making the automated assessment of the probability of being a suspicious transaction. The explanation and guided navigation given by the AI/ML model helps the analyst make the right risk decision.



Model to recommend "hibernation" of the AML alert - DBS

DBS also developed other new capabilities to support the investigation of alerted transactions, including a “Network Link Analytics” system (Fig.2) for detecting suspicious relationships and transactions across multiple parties.



Analysis of the networks among DBS accounts - DBS

In parallel, DBS has also replaced a labor-intensive approach to investigation workflow with a new platform that automates for the analyst much of the support for surveillance-related investigation and case management called CRUISE that integrates the outputs of the rule-based engine, the ML filter model, and the network link system. Additionally, the CRUISE system provides the analyst with easy and integrated access to the relevant data from across the bank needed to follow up on the transactions they are investigating. Within this CRUISE environment, the bank also captures all the feedback related to the analyst's work on the case, and this feedback helps to further improve DBS's systems and processes.

Impact on the Analyst

Of course, this all makes analysts much more efficient in reviewing alerts. Few years ago, it was not uncommon for a DBS transaction surveillance analyst to spend two or more hours looking into an alert. This included the front end preparation time to fetch data from multiple systems and to manually collate relevant past transactions, and the actual analysis time to evaluate the evidence, look for patterns, and make the final judgement as to whether the alert seemed to actually be a suspicious transaction or not.

After implementation of multiple tools including CRUISE, Network Link Analytics, and the ML based filter model, analysts are able to do about a third more cases in the same amount of time. Also, for the high-risk cases that are identified using these tools, DBS is able to catch the "bad actors" faster than before.

Commenting on how this differs from traditional surveillance approaches, a senior DBS manager shared:

"In traditional transaction surveillance settings, it is very challenging for an analyst to get all of the information they needed across the various parts of the bank in order to follow up on alerts because of the abundance and variety of data involved. An analyst has to close out a review within a certain specified time period. Within this time, there is only so much data the analyst can acquire across the bank and make sense of, but the analyst just has to make a decision on the alert within that time period. Sometimes that decision is right. Sometimes it is wrong. But that is the best that could be done under the circumstances.

Today at DBS, our machines are able to gather the necessary support data from various sources across the bank and present it on the screen of our analyst. Now the analyst can easily see the relevant supporting information for each alert and make the right decision. The analyst does not have to search through 60 different systems to get the supporting data. The machines now do this for the analyst much faster than a human can. It makes the life of the analysts easier and their decisions a lot sharper.

In the past, due to practical limitations, transaction surveillance analysts were only able to collect and use a small fraction of the data within the bank that was relevant to reviewing the alert. Today at DBS, with our new tools and processes, the analyst is able to make decisions based on instant, automatic access to nearly all the relevant data within the bank about the transaction. They see this data, nicely organized in a condensed manner on their screen, with a risk score and with the help of an explainer that guides them through the evidence that led to the output of the model."

DBS invested in a skill set "uplift" across the staff who were involved in creating and using these new surveillance systems. This included the transaction surveillance analysts who had expertise in detecting financial crimes and were trained in using the new technology platform and in relevant data analytics skillsets. Staff from these teams were cross-trained in the other two areas (product specialists and technology specialists) so they could more effectively work with their counterparts in those areas. These teams helped to design the new systems, beginning with the front-end work to identify risk typologies. They also provided inputs to identify the data that made most sense to use, and where automated data analytics and ML capabilities could be most helpful to them.

When asked how the systems would affect human transaction analysts in the future, a DBS executive said:

"Efficiency is always important, and we must always strive for higher levels of it. We want to handle the transaction-based aspects of our current and future surveillance workload with fewer people, and then reinvest the freed-up capacity into new areas of surveillance and fraud prevention. There will always be unknown and new dimensions of bad financial behavior and bad actors, and we need to invest more time and more people into these types of areas. To the extent that we can, we will do this through reinvesting the efficiency gains we achieve within our more standard transaction surveillance efforts."

The Next Phase of Transaction Surveillance

The bank's overall aspiration for AML transaction surveillance is to become more integrated as well as more proactive. Rather than just relying on alerts generated from the rule-based engine, executives want to make use of multiple levels of Integrated Risk Surveillance which enables the bank to monitor holistically from 'transaction to account to customer to network to macro' levels. This combination would help the bank to find more bad actors, and to do so more effectively and efficiently.

A DBS senior manager elaborated:

"It is important to note that money launderers and sanctions evaders are always finding new ways of doing things. Our people need to work with our technology and data analytics capabilities to stay ahead of these emerging threats. We want to free up the time our people have been spending on the tedious, manual aspects of reviewing alerts, and use that time to keep pace with the emerging threats."

Human analysts will continue to play an important role in AML transaction surveillance, though the way they use their time and their human expertise will continue to evolve.

The senior manager at DBS also shared a perspective on AI:

"It's really augmented intelligence, rather than automated artificial intelligence in risk surveillance. We do not think we can remove human judgement from the final decisions because there will always be a subjective element to evaluations of what is and is not suspicious in the context of money laundering and other financial crimes. We cannot eliminate this subjective element, but we can minimize the manual work that the human analyst does as part of reviewing and evaluating the alerts."