Applying analytics in financial institutions' fight against fraud

28 May 2017

For more information please contact:
Patricia.Garcia@quantumblack.com

QUANTUMBLACK
A MCKINSEY COMPANY

Defining the role of analytics in addressing the challenges of financial fraud
Continued

Forty years ago, banking fraud might have involved simply forging an account holder's signature on a withdrawal slip. Now the speed and intricacy of the schemes are mind boggling: a student bank account (with details obtained by a crime gang) receives a payment of £10,000. Within minutes, the funds have been cycled through dozens of accounts before being forwarded to an international account, where the trail suddenly goes cold. No alarm bells go off. No inquiries are made to the bank. The fraud is only discovered much later, at which point the money and the fraudsters are long gone.

Around the world, fraud is an ever-increasing risk for businesses of all stripes. The 2015/16 Global Fraud Report by Kroll and the Economist Intelligence Unit found that 75 percent of companies surveyed had been victims of fraud in the past year, an increase of 14 percentage points from three years earlier. And perhaps unsurprisingly, fraud is a particularly serious issue for financial institutions. The Association for Financial Professionals' 2016 Payments Fraud and Control Survey found that 73 percent of finance professionals reported an attempted payments fraud in 2015.

As prevalent as the fraud problem is for financial institutions, it can be difficult to address. Factors that contribute to the challenge include the sheer volume of transactions handled by most institutions versus the relatively small number of fraudulent transactions, the speed with which technology allows fraudsters to operate, poor or incomplete data, and the lack of information sharing among financial institutions. All too often, banks lack the technology and capabilities to implement the necessary safeguards, responding to a primarily digital problem in an analog way – for example, phone calls attempting to piece together the path of a rapid series of money transfers.

For financial institutions, data and analytics can speed the decision cycles used to observe, orient, decide, and act in fighting fraud. Since the best insights are often at the margins of where industries or data sets overlap, it's necessary to pose targeted questions and develop solutions from a variety of information sources. By combining proprietary data sets with industry benchmarks and government information, financial institutions can use artificial intelligence, machine learning, and analytics in the fight against financial fraud. Financial executives should move now to adopt appropriate processes, develop and acquire the necessary talent, and create the right culture to integrate analytics into their fraud detection efforts.

Defining the role of analytics in addressing the challenges of financial fraud

A vast amount of data flows through financial services organisations, so the ability to harness that data and analyse it effectively could transform the industry's fraud detection efforts and provide a host of other benefits. Coupling these rich data sets with appropriate analytical models provides a way to harvest the information needed to identify and prevent fraud more effectively. In some cases, an institution's data can be combined with other fraud markers necessary to provide a data set for training the analytics models used to detect possible incidents of fraud.

For financial institutions and government agencies looking to fight fraud, then, the goal should be to aggregate the existing data needed to support more timely detection and to couple that data with the expertise needed to create and apply the most effective fraud detection models. Doing so successfully can not only produce financial savings but also protect the company's reputation and maintain public confidence. A recent example demonstrates how applying analytics to fraud detection can provide immediate and significant benefits.

A new model detects an unprecedented volume of invoice redirection

Imagine receiving an e-mail from your CEO requesting an update to the payment details of a key supplier. Coming from a trusted source, you might carry out the task without question. But in doing so, you would become an unknowing accomplice to CEO fraud. In this crime, imposters gain access to business e-mail accounts and use them to convince unsuspecting employees to send funds to bogus accounts. CEO fraud has jumped 270 percent from 2015 through Q3 2016 and has led to losses of more than £2.3 billion over the past few years.

Most banks have manual fraud detection procedures or rules-based solutions, but their effectiveness is limited. The task is especially challenging for invoice redirection, where banks must spot bogus accounts that look very much like the real thing. It's truly like looking for fraud needles in the banking transaction haystack. In such cases, banks have no way of knowing whether they are paying a legitimate account.

Assembling the data needed to train an analytics model that can accurately identify potential invoice redirection can be a potent weapon in the fight against fraud. QuantumBlack worked with a major bank looking to reduce invoice redirection fraud — some tens of millions in value in such invoice redirections from 2010 to 2015— leveraging one of the country's largest data sets. The goal was to develop a tool that could provide daily reports of suspicious transactions and identify more than 80 percent of fraud cases in both value and incidence.

£2.3bn

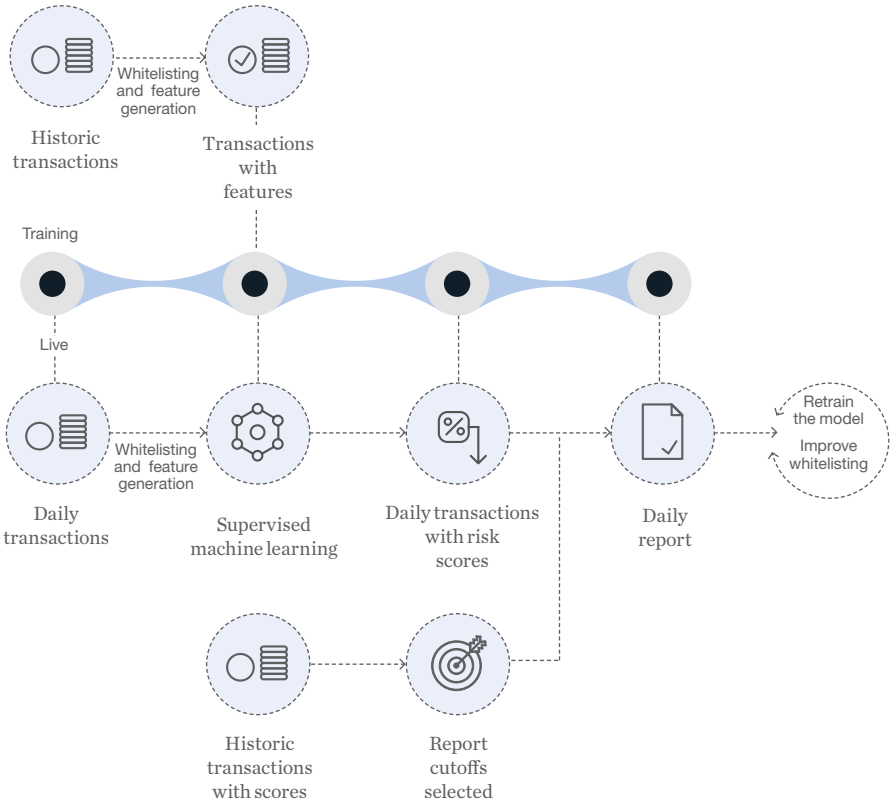
Of losses over the last few years

To score every one of the millions of daily transactions for fraud risk, QuantumBlack built a supervised machine learning model. But while the model needed a sufficiently large data set to learn to detect fraud, the number of potentially fraudulent transactions on any given day is so small that waiting for the natural operational work flow to generate the needed number would have taken too long. In response, the QuantumBlack team decoupled the training process from the day-to-day operation and created a partially synthetic data set to train the model.

Our team worked closely with the client's data engineering team to ensure computational performance, database best practices, and legal compliance. The curated data sets successfully trained the model to determine which transactions are safe and which are potentially fraudulent.

In actual use, most daily transactions can be immediately categorised as non-fraudulent. The remaining few thousand transactions are run through the machine learning model, which provides a risk score indicating which transactions are most suspicious and which can be assumed safe. By using analytics to combine the value and risk probability of each transaction, the model can instantly rank transactions by risk score. The risk score is computed taking into consideration two different transaction patterns, one between the source and the destination account and the relationships established at the destination account.

Figure 1 – An overview of the model



The result is that the bank now has a tool that significantly improved its high-value fraudulent transactions detection capability. The live product now notifies the bank of an average of 35 high-risk transactions a day out of the several million processed, allowing the bank's fraud team to focus on the transactions that truly demand closer investigation. The investigation results are then used to continue training the machine learning model on both new fraudulent cases as well as new relationships validated as safe.

The predictive model identifies more than 85 percent of fraud cases in value and incidents on the day the transaction is processed, allowing the bank to halt transactions before close of business and recover the funds. Within the first few weeks of live-scoring transactions, the model detected approximately $100,000 in fraudulent transactions. Other banks have expressed interest in the product, which is just the first step of applying analytics and modeling to the financial fraud detection space.

35

High-risk transactions a day out

$100,000

Fraudelent transactions detected within the few weeks of live scoring

Figure 2 – The screen below is a presentation of the capability provided to the bank

Working together to craft practical solutions

These use cases reinforce the opportunities for financial institutions to wield analytics to implement real solutions to fraud. The projects often involve bringing multiple players to the table to assemble the data needed to train the models that will identify fraud—but those combined efforts are handsomely rewarded through a significant reduction in fraud losses and increased public confidence in financial institutions.

To benefit from the opportunities that data analytics present to fight fraud, financial institution executives could implement a framework centered on four key areas:

/ Empower the organisation with targeted tools and capabilities: On top of advanced analytics solutions, ensure that people can get results out of analytics by providing the training needed to help them understand the results and the markers of fraud. A key element will be creating a culture of vigilance and data-driven decisions. In some cases, it will be necessary to bring in new talent.

/ Redesign processes for speed and efficiency: Determine how the organisation will apply or alter its processes to improve fraud detection, possibly involving changes to the information that's reported or using new tools to obtain better information. An audit to identify data sources and measure data quality could be part of this phase.

/ Mobilise the entire enterprise through effective communications: Craft a story around the fraud detection effort and the new advanced analytics capabilities, how they will be deployed, and their expected benefits. More importantly make clear how each individual member of the organisation has to change the way he or she operates to deploy those capabilities in day-to-day tasks. Use internal channels to share the story across the organisation.

/ Activate the C-suite: Drive change from the top down. Executives should be involved in analytics initiatives and be vocal advocates for integrating data-driven decision making into all facets of the organisation.

Finally, institutions should determine whether to build their own internal data science capability or work with an outside organisation to close any gaps in analytics skills.

Using analytics to fight fraud

Fraud is a significant problem for all types of financial institutions, but analytics offer the potential to identify fraud cases more quickly and frequently, sometimes even before the fraudulent act occurs. Fortunately, financial institutions already collect a tremendous amount of data which can be used to help fight fraud. The data sets don't have to be perfect to be useful, but a good first step for most organisations is to assess existing data and its quality and determine what other useful data might be collected.

To benefit from the fraud-fighting potential of data analytics, financial institutions must commit to developing the necessary skills and creating the appropriate culture. But given the potentially sizable rewards of reduced fraud losses and maintaining public trust, that commitment should be one all organisations are willing to make.

Thank you

Jacomo Corbo is the chief data scientist at QuantumBlack, Chris Wigley is the chief commercial officer at QuantumBlack and a partner in McKinsey's London office, and Carlo Giovine is a manager at QuantumBlack and in McKinsey's London office.

QuantumBlack.com