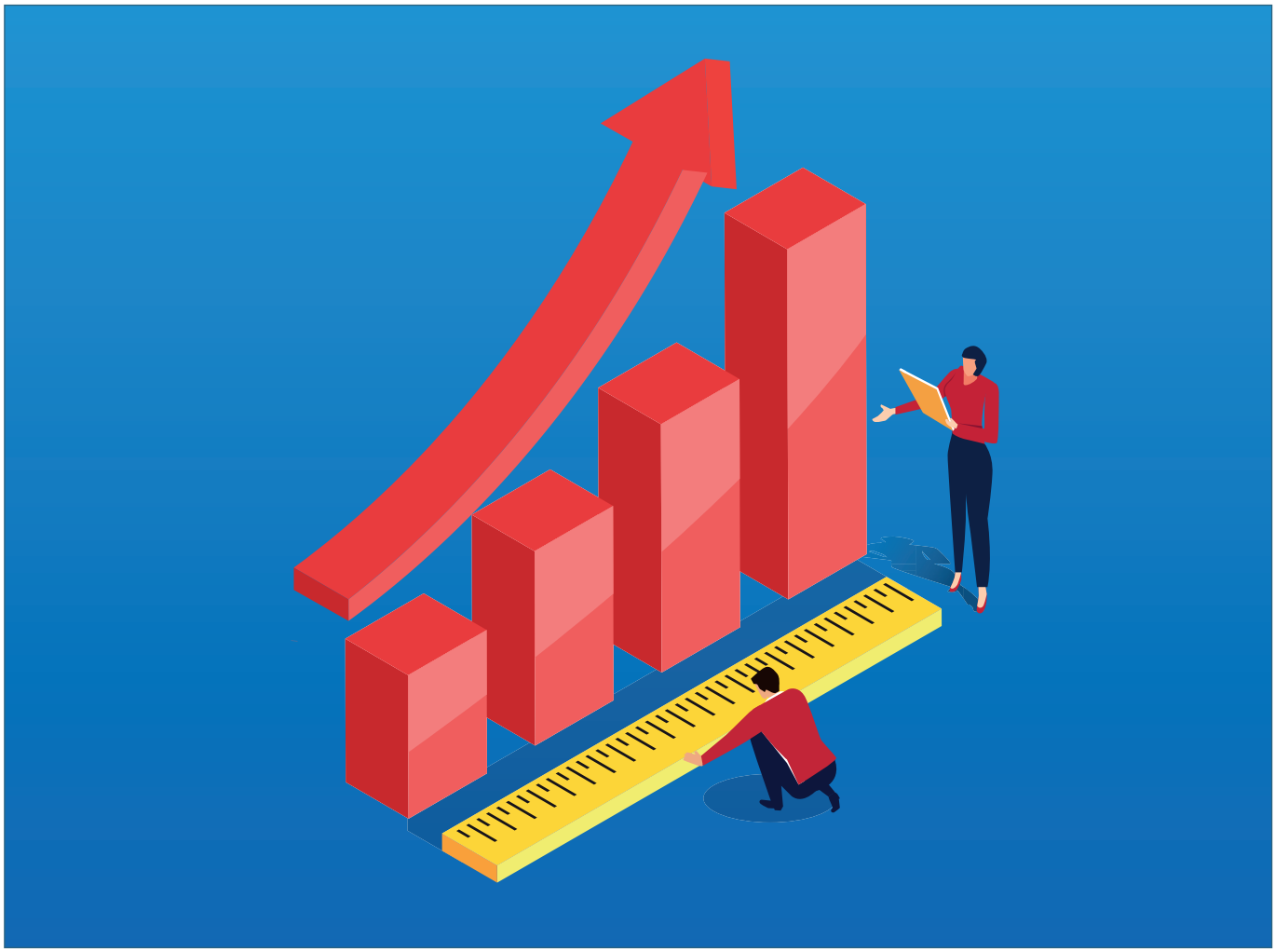
Taking the lead on financial crime regulatory compliance



Increased scrutiny of anti-money laundering and customer due-diligence procedures means banks must create more efficient and effective systems. A recent webinar convened by *Risk.net* and IBM discussed how leading banks are utilising artificial intelligence and cognitive technologies for financial crime prevention

Risk.net

IBM

Taking the lead on financial crime regulatory compliance

Increased scrutiny of anti-money laundering and customer due-diligence procedures means banks must create more efficient and effective systems. A recent webinar conducted by *Risk.net* and IBM discussed how leading banks are utilising artificial intelligence and cognitive technologies for financial crime prevention

Financial institutions today are subject to increasing scrutiny from regulators and growing pressure to improve compliance systems and processes to better detect suspicious activity and stop illegal activities more quickly. As a result, banks must invest significant time, money and resources in financial crime prevention that could be spent elsewhere in the business, according to expert panellists participating in a recent *Risk.net* webinar discussion commissioned by IBM.[1]

The discussion focused on how large financial institutions are managing the challenges of tackling financial crime in the current regulatory environment, drawing on evidence from a November 2018 *Risk.net*/IBM survey of 89 financial services professionals involved in financial crime investigation and analysis.

Maintaining high standards for anti-money laundering (AML) and customer due-diligence (CDD) systems and processes is crucial for banks now and in the future, but questions have begun to arise about whether resources are being funnelled into this area in the most efficient way. According to the survey, many market participants do not think so. Asked to rate the existing investigation process at their organisation, only 9% of these professionals gave top ratings for effectiveness, and less than 5% for efficiency.

This result highlights a pressing need for improvement of the AML and CDD systems large banks currently use to prevent financial crime. As some firms are already starting to discover, greater use of automation and innovative tools such as artificial intelligence (AI) and cognitive learning could significantly increase effectiveness and efficiency in this area. This would enable banks to tackle financial crime, comply with increasingly onerous regulations and direct some of the resources currently given to this area to other parts of the business to improve customer experience or enable growth.

Identifying the challenges

The webinar participants acknowledged that similar challenges plague many banks when it comes to satisfying AML and CDD requirements. For example, discussing current controls used to identify riskier customers or activities, panellist Christopher Sidler, managing director at Promontory Financial Group, said: "We [in the financial industry] are still using old, outdated measures to quantify and evaluate what risk quantum actually is for those customers." As a result, non-risky customers may be unnecessarily caught up in refresh cycles. Dismissing such false alerts takes time and effort by financial crime analysts, resulting in a negative impact on customer relationships.

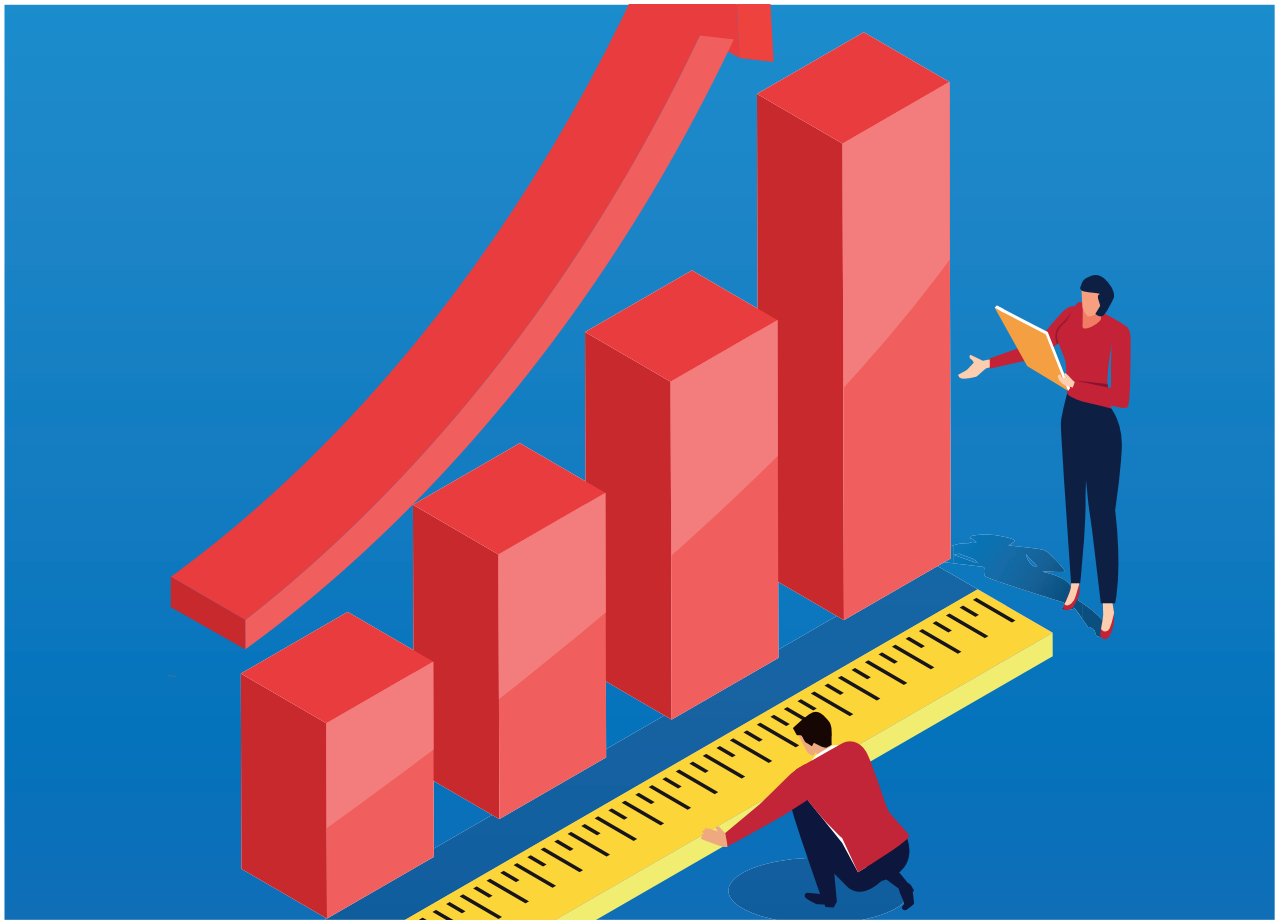
THE PANEL

Marc Andrews, Vice-president, Financial crimes and conduct risk, Watson Financial Services Solutions, IBM
Christopher Sidler, Managing director, Promontory Financial Group
Moderator: Joel Clark, Contributing editor, *Risk.net*

> "If we can learn over time which [behaviours] correlate with people involved in money laundering, we will have an opportunity to dramatically impact the false-positive rate that banks are dealing with today"
>
> Marc Andrews, IBM

Some organisations in this space are already starting to embrace automation, AI and machine learning to address these issues. According to the survey results discussed in the webinar, and explored in full in the IBM white paper *Smarter thinking about financial crime prevention*,[2] one-third of financial firms polled are already incorporating such techniques into their risk and compliance programmes, including AML and CDD activities, while a further one in six are using them for other areas of risk but not yet financial crime prevention.

While banks are evidently 'dipping a toe in the water', some firms' experimentation with AI and cognitive technology is very much ahead of the curve. "The ability to start clustering and segmenting customers more dynamically based on their behaviours [is] one of the areas where we have seen [banks] start to get some positive results," said Marc Andrews, vice-president, Watson Financial Services Solutions at IBM. This involves identifying specific behaviours displayed by customers



that are symptomatic or causative of financial crimes, rather than following the traditional approach of using a static scorecard of characteristics to gauge risk. "If we can learn over time which [behaviours] correlate with people involved in money laundering, we will have an opportunity to dramatically impact the false-positive rate that banks are dealing with today," he said, also citing industry accounts of banks being inundated with alerts, of which only one or two out of 100 resulted in a suspicious activity or suspicious transaction report.

What's next?

Pilots conducted by some of the leading financial institutions have already shown impressive results to date, according to Andrews. "One bank was able to segment a certain set of customers, out of which one-third initially identified as high risk were actually not generating any alerts, and were likely entities that could be considered low risk," he said. When it comes to tackling false positives, Andrews has seen initial trials identify 25–35% of generated alerts as false, and in one case as many as 65%, with backtesting demonstrating no need for suspicious activity reports within the population.

The next steps for such innovation is likely to be the automatic disposition of alerts, according to both the survey respondents and the webinar panellists. Using automation here would reduce the valuable time spent by analysts researching and dismissing false positives, and then documenting the process for compliance purposes.

While such advances – for which regulatory backing has only recently emerged[3] – remain a way off, some banks have already been hard at work exploring this option. Those already experimenting with these techniques will be ahead of the competition in terms of developing and benefiting from the most efficient AML and CDD systems. "We are seeing banks start to push that envelope already," Andrews said. "And it is likely to be here before [other] banks even realise it."

Learn more

The *Risk.net* and IBM webinar *AML benchmarking: How does your approach measure up?* is available on demand at *www.risk.net/6205061*

A white paper based on the full survey results, *Smarter thinking around financial crime prevention*, is available at *www.risk.net/6265151*

[1] *Risk.net, IBM,* AML benchmarking: How does your approach measure up?, *December 2018, www.risk.net/6205061*

[2] *Risk.net, IBM,* Smarter thinking around financial crime prevention, *December 2018, www.risk.net/6265151*

[3] *Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency,* Joint statement on innovative efforts to combat money laundering and terrorist financing, *December 2018, https://bit.ly/2BTDu62*

Risk.net

PRODUCED IN
COLLABORATION WITH

IBM®