RACONTEUR

Money Laundering: The AI Revolution

feedzai

feedzai

Feedzai is the market leader in fighting fraud with AI. We're coding the future of commerce with today's most advanced risk management platform powered by big data and machine learning. Founded and developed by data scientists and aerospace engineers, Feedzai has one mission: to make banking and commerce safe.

RACONTEUR

Publication sponsored by

feedzai

Publisher Michael Kershaw
Project manager Tom Andrews
Editorial consultant Gren Manuel
Editor Lindsay O'Hagan
Designer Sara Gelfgren, Harry Lewis-Irlam
Head of production Justyna O'Connell
Digital marketing manager Elise Ngobi

Contributors

Alison Coleman
Writer and editor, she has contributed to Forbes, The Guardian, Telegraph, Sunday Telegraph, Economia and Employee Benefits.

Mark Frary
A science, technology and business writer with eight published books, he was shortlisted in the British Journalism Awards for Specialist Media 2018.

Richard Harris
Senior vice president of international sales, Feedzai.

Oliver Pickup
Multi-award-winning journalist who has written for publications including The Times, Telegraph, Guardian, and FT Weekend.

Contents

In the fight against money laundering, technology is both friend and foe. This reports how breakthrough technologies mean financial institutions can achieve better results with fewer staff

How technology boosts the battle against illicit funds

Criminals are locked in a technological arms race with the authorities that want to detect the origins of their cash

ALISON COLEMAN

Technology is transforming the world of money. It is also transforming the world of money laundering – and the fight against it.

Innovations such as faster payments, artificial intelligence and open banking create both opportunities to launder money and new tools to detect it. As such, criminals who want to move money and disguise its origin are locked in a technological arms race with the banks, regulators and law enforcement agents that want to detect them.

The stakes are high. The United States ramped up its efforts against illicit financial movements within six weeks of the 9/11 terror attacks. It is using its status as the world's financial superpower, backed up by the threat of huge fines, to drive a global agenda of tighter surveillance of money flows, particularly in relation to the financing of terrorism or sanctions-busting.

Ismail Erturk, senior lecturer in banking at Alliance Manchester Business School, says: "In the 1960s and 1970s, for example, US banks were used as vehicles to assert US foreign policy in South America. Today, the US is firmly against money laundering and proactive in tackling financial crime, particularly activity that supports terrorism and flouts US sanctions against countries classed as risks to US national security."

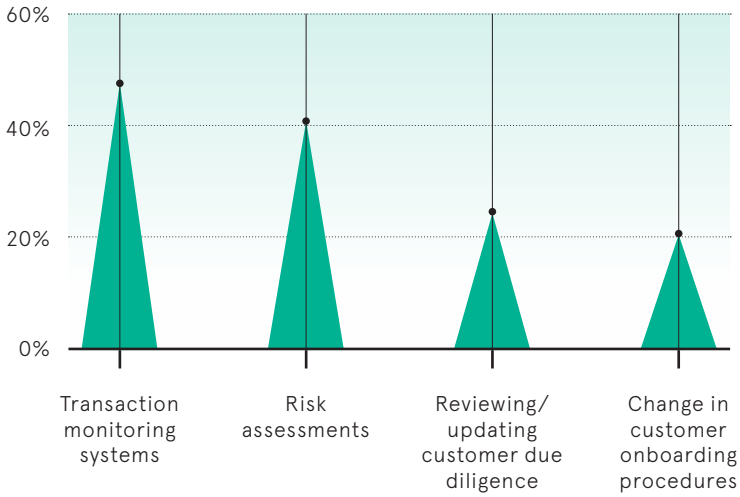
However, it is not just the US that is increasing the pressure. The EU is stepping up its campaign against dirty money in the wake of serious failings at Dutch bank ING and Denmark's Danske Bank. In September, the EU said it proposed to tackle money laundering more effectively across borders by strengthening the role of the European Banking Authority. Valdis Dombrovskis, the EU commission vice-president responsible for financial services policy, said: "Anti-money laundering supervision has failed all too often in the EU."

Banks are implementing mechanisms to ensure compliance with money laundering and financial crime regulations. The problem is that many of the processes used to identify illicit transactions are inefficient and often rely on outdated technology – or lots of people.

This can make them expensive. Consultancy McKinsey said last year: "In the United States, anti-money laundering (AML) compliance staff have increased up to tenfold at major banks over the past five years or so."

Legislative disruption in the sector has added to the challenge. In January, new open

Where does the C-suite see the challenge?



Alix Partners global financial insitutions survey, 2017

banking regulations came into effect in the UK to give consumers greater control, choice and flexibility in terms of their finances. But this also increases risk by introducing more players and platforms that can process banking information and transactions in what is already a complex regulatory landscape.

"Open banking is also encouraging non-banking organisations to use payment systems and circulate money for lending and savings purposes," says Mr Erturk. "Therefore it is now possible for money launderers to set up their own financial institutions, payment products and cryptocurrencies to launder money or violate sanctions."

Regulators and central banks, however, are becoming increasingly vigilant in their supervision of financial institutions. David Gardner, partner at law firm TLT, suggests that open banking gives access to rich data streams that can be harnessed by service providers and banks to improve AML compliance. The adoption of new technologies will further speed up and enhance the effectiveness of AML processes.

"We are already seeing newly registered account information service providers offering AML services, utilising AI [artificial intelligence], machine learning and big data analytics," Mr Gardner says.

Machine learning has been shown to be effective in monitoring suspicious activity and transactions. For example, monitoring transactions generates a large number of alerts, which then have to be processed by operational teams. Machine learning can teach computers to detect and recognise suspicious behaviour and to classify alerts as being of high, medium or lower risk.

Andrew Garvey, chief commercial officer at fintech company Countingup, which provides banking services to small businesses, says: "There are so many international financial transactions being made these days, it is inevitable that technologies like AI and data analytics will increasingly be used to recognise patterns in data, identify illicit transactions and play a more significant role in AML."

$8.9bn

Record US penalty for BNP Paribas for AML failings

US Department of the Treasury, 2014

> **Anti-money laundering supervision has failed all too often in the EU**
>
> Valdis Dombrovskis

The scale of the problem

The United Nations Office on Drugs and Crime reckons that between $800 billion and $2 trillion is laundered each year. Estimating the size of a global and illicit trade is not easy, the UN agency admits, but "even the lower estimate underlines the seriousness of the problem governments have pledged to address". The UK's National Crime Agency estimates that "hundreds of billions of pounds" is laundered through UK banks and their subsidiaries annually.

The global response

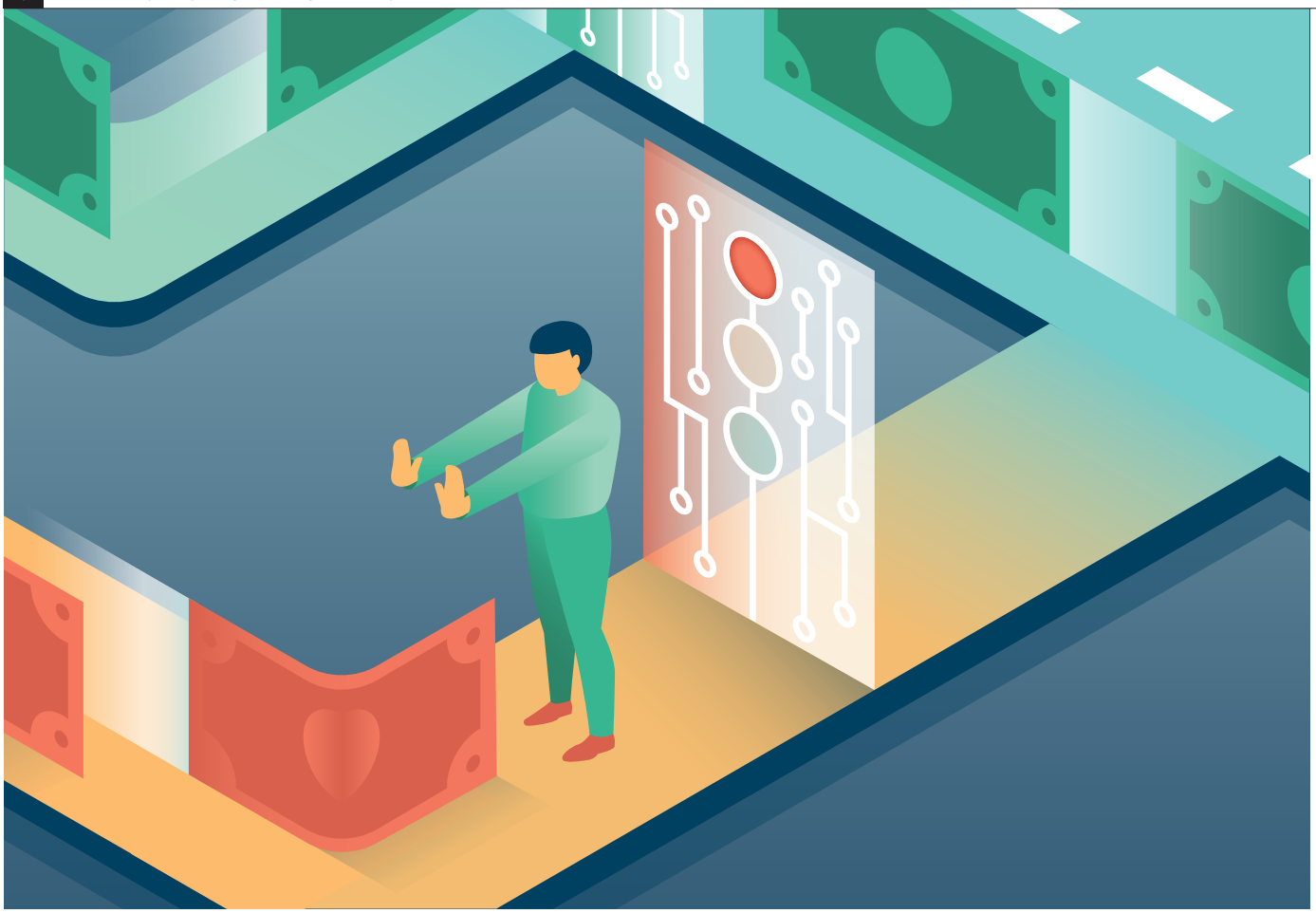
The war on money laundering is global, and requires cross-border co-operation to fight it effectively. Initiatives include the launch of the Financial Action Task Force on Money Laundering (FATF) in 1989. An intergovernmental organisation, FATF was founded on the initiative of the G7 to develop policies to combat money laundering. Since then other bodies, including the European Union and Organization of American States, have developed anti-money laundering standards for their member countries.

How it's done

The United Nations Office on Drugs and Crime identifies three distinct stages:

- Placement, moving the funds away from direct association with the crime.
- Layering, a potentially complex series of transactions that can hide the true origins of the funds.
- Integration, making the money available to the criminal with its original source now fully disguised.

The days of suitcases full of used notes are long gone. Increasingly, there is no cash involved – both the input and the output of the process are electronic.



Humans need machines to help tackle AML

AI can cut the time it takes to investigate a false positive from 30 minutes to 30 seconds

MARK FRARY

The €775 million (£687 million) penalty levied on Dutch bank ING at the beginning of September for failing to prevent clients from using their bank accounts for money laundering and other financial crimes contains in the small print a telling indication of the costs of AML for banks.

In ING's statement, the bank said that €100 million of the fine "represents the underspend by ING Netherlands over the period in scope on staffing for implementation and execution of financial economic crime customer due diligence policies and procedures".

Note that €100 million is just the underspend between 201 0 and 2016. And how is it preventing a recurrence? Ralph Hamers, chief executive of ING, said measures include tripling the size of the customer due diligence team in the Netherlands to 450 people.

This report has already highlighted the calculation by consultants McKinsey that in the United States, the number of compliance staff working in anti-money laundering (AML) has increased up to tenfold at major banks over the past five years. But the ING example brings home the sheer scale of the exercise.

"Some Tier 1 organisations have more than 1,000 people in operations doing this type of work. Using technologies to help automate and improve the quality of that work is vital," says Patrick Craig, partner in EY's financial crime practice.

This is causing banks a huge headache, one that they hope to cure by using artificial intelligence and machine learning.

Speaking at an event on fintech innovation in AML at the end of 2017, Rob Gruppetta, head of the financial crime department at the Financial Conduct Authority, recognised the potential of such technologies. "Data analytics and machine learning are widely seen as the approaches with the greatest potential to improve current practices, particularly in the field of transaction monitoring," he said.

Existing transaction monitoring systems tend to be rules-based and are tuned to reflect specific risks. Using a rules-based system triggers alerts on many legitimate transactions; all have to be investigated and documented. That translates to people, or does it?

One of the reasons that AML measures need so many people is the high rate of false positives – transactions that look suspicious but are legitimate. This is because transaction-monitoring systems look for low-frequency events, a problem highlighted by McKinsey in early 2018.

The consultancy ran the math on a hypothetical system scanning transactions, of which one in a thousand meet the criteria as suspicious. If that system correctly classifies 95 per cent of transactions then it will have a false positive rate of over 98 per cent, with the tiny number of suspicious transactions drowned in a sea of acceptable transactions which have been wrongly flagged.

Michael Levi, professor of criminology at Cardiff University, says this is an area where AI could bring huge benefits.

"There are huge costs of human work in areas where the rate of false positives in alerts can be 95 per cent," he says. "AI can reduce the 20 to 30 minutes per human inspection of a false positive to 30 seconds."

58%

Institutions experiencing regulatory enforcement or inspection for AML in past two years

23%

Institutions who have done AML risk assessment past two years

PwC survey of banks, fund managers, brokers etc, 2018

HSBC, which paid a $1.92 billion fine to US regulators in 2012 for failure to tackle money laundering by drug cartels in Mexico, now employs some 6,000 staff in compliance areas.

Colin Bell, group head of financial crime risk at the bank, says: "Using machine learning, we hope to be able to investigate fewer, more meaningful alerts, allowing us to identify potentially suspicious activity with greater precision. If we get this right, we will find the more sophisticated actors and we will find them faster."

Mr Bell sees automation as a way "to augment humans, rather than replace them".

Tom Salmond, an associate partner in EY's financial crime practice, says tools that can get data out of siloed systems into one big data platform will be vital.

"We need to increase usage of these techniques, but also increasingly to apply them to help people in these investigations," he says.

The roll-out of AI in AML may not happen quickly and regulation may be the problem.

One stumbling block is that some AI systems cannot "explain" their decisions. Regulators are wrestling with the issue of whether to allow 'black box' technology that might make decisions that human investigators don't understand.

Dr Levi warns that AI will not be a magical pill that enables investigators to find every suspicious transaction. However, he believes AI will allow investigators to spend less time on monitoring which will enable them to introduce random checks to verify that machine judgments are broadly correct.

Other regulatory issues may be blocking quick implementation of AI tools.

EY's Patrick Craig says: "There is certainly a recognition of the ineffectiveness of the regulatory framework to allow institutions to do this in a cost-effective manner. A lot of the regulatory framework has been around for 20-30 years, but the world has moved on, so we need to update and innovate."

Mr Craig adds: "Financial institutions will be optimising their existing systems because they need to drive better efficiencies and [we] will also see them experimenting with advanced challenger-based models to show they can get better results, and that will be used to inform local and global legislation."

At the 2017 fintech event, the FCA's Rob Gruppetta, said: "Artificial intelligence has the capability to greatly amplify the effectiveness of the machine's human counterparts... [but] any bank hoping for a black box in the corner that will sniff out the launderers will be disappointed."

Why AI is vital in the fight against money laundering...

... but don't underestimate the power of people too

RICHARD HARRIS, FEEDZAI

A sea of change in anti-money laundering (AML) is happening in Europe, driven by real-time digital transactions, and the EU's revised Payment Service Directive (PSD2), which came into force in January.

To keep pace with changing regulations and customer demands, business leaders must act urgently to fortify traditional methods of defence – slow, manual work, done by lots of humans and based on previous experiences – with a layer of artificial intelligence (AI), or face monumental fines from regulators.

Adding to the complexity and scale of AML is the "aggressive rollout of real-time/instant payments initiatives in 51 countries", according to US-based payments infrastructure firm The Clearing House. As payments move to real-time and involve transferring from different entities across the world, the old-fashioned checks have become outmoded. Traditional systems might detect that money laundering has taken place, but by the time this happens the money has long gone.

57%

Executives having transaction monitoring as a top three AML priority

Alix Partners global financial institutions survey, 2017

Organisations don't want to have to explain to regulators that they know money laundering is taking place but are powerless to stop it. If the end-to-end audit trail is not visible, the authorities will mete out stinging penalties.

Regulators in the United States and Europe have imposed $342 billion (£262 billion) of fines on financial institutions since 2009 for misconduct, including violation of AML rules, a report by consulting firm Quinlan & Associates found in September 2017. This figure is forecast to exceed $400 billion by 2020.

In 2012, HSBC was fined £1.4 billion for helping drug cartels launder money in Mexico, among other contraventions. In early 2017, Deutsche Bank was hit for more than £500 million by British and American authorities, including a record £163 million fine from the UK's Financial Conduct Authority, for what the FCA said was

Three things to know

False positives are the enemy:
It is essential to use systems that can work at a granular level. The explosion in data means this is not going to get any easier, and the answer is not to hire hundreds more people, because AI can ably assist now.

Transparency is vital:
If you are going to work with AI in AML, choose a system that enables you to see how a decision was made. Transparency is critical, particularly from a regulatory point of view.

Regulatory requirements are the minimum:
AML should be a major investment because you want to be at the front of the pack, and therefore not vulnerable to regulatory fines. The expense of doing it right in the first place far outweighs the cost of being penalised and catching up.

an "inadequate AML control framework". And in June 2018, Australia's Commonwealth Bank had to pay $700 million (£400 million) – the largest civil penalty in the country's corporate history – after the late filing of 53,506 reports of transactions over $10,000 because they did not have the right controls in place.

The people behind money laundering are determined, well-coordinated criminals who fund global terrorism, human trafficking, and narcotics distribution. The money launderers are using sophisticated AI that can automate opening accounts. Earlier this summer, for example, one of our clients, a large global merchant, detected more than £2.3 million of fraudulent transactions in the course of 48 hours, having been attacked by a specific dataset with more than 50,000 entities.

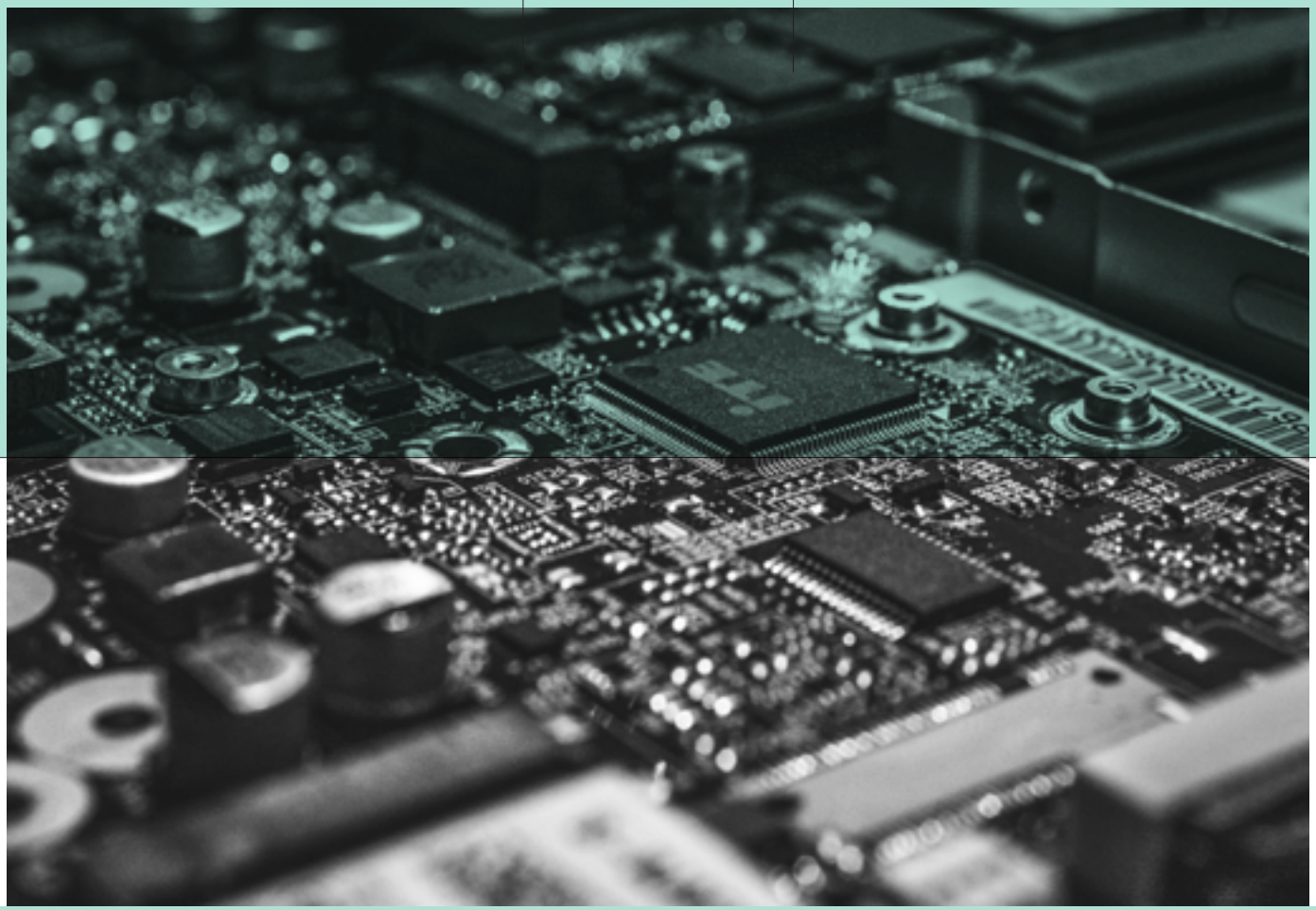
Consumer data is so cheaply available that at any particular moment thousands of accounts are being created, and this contributes to the rapidly growing scale of this issue. Criminals are investing heavily to find the weak points and can deploy a new strategy within minutes. AML has become a live battle that is changing every second.

The organisational burden is another pain point of AML. Financial institutions might employ upwards of 5,000 employees in sanction screening alone. As transaction volume keeps growing, so do alerts, false positives, and compliance teams, all at unsustainable rates.

Automating these processes is a must. Feedzai uses machine learning and advanced data science automation to replace the manually tedious parts of AML processes with insights that are specific to money laundering. The promise of this AI-enabled technology is that financial institutions can shift from mere compliance to total risk management, identify serious risk signals amid the noise, and ensure that manual investigation resources are intelligently applied using a validated risk-based approach.

Even with advances in technology, it remains critical to keep humans in the loop. For example, all AI systems need to be trained and validated by human practitioners. The benefit is that people and machine learning working together will increase accuracy and granularity, thereby rapidly reducing the number of false positives – which is what AML investigators spend 99 per cent of their time on.

Machines are not replacing humans, but augmenting them. Indeed, a multi-layered approach, using technology with built-in transparency, controllability and explainability is critical to bolstering AML defences. This winning combination will help keep regulators satisfied and criminals at bay, in 2018 and beyond.



The hunt for talent

Higher skills, fewer staff: the way ahead for teams fighting money laundering

DAVID BENADY

The recipe for combatting money laundering is not new: premium technology plus skilled people. Unfortunately, that second ingredient is in short supply.

The market for all staff with strong digital skills is getting tighter. A joint research report by Capgemini and LinkedIn, published last October, laid bare the extent of the issue: in summary, a high majority of the organisations surveyed "acknowledged that the digital gap is widening". Uncertainty about the ability to import skilled staff post-Brexit doesn't help.

Try to recruit staff with good knowledge of artificial intelligence, or skills in anti-money laundering – or tougher yet, both – and the problems intensify. Less than eight per cent of developers work specifically in data science or machine learning, according to research by Stack Overflow, a website for developers, earlier this year.

Dean Curtis, managing director at LexisNexis Risk Solutions, says the skills shortage in AML is driving up recruitment costs and salaries, but it is a necessary expense. "Real-life input remains key, as only by combining human talent and technology expertise will the best outcomes be achieved," he says.

45%

Executives having training as a top three AML priority

Alix Partners global financial institutions survey, 2017

Peter Bebbington, chief technology officer of Brainpool, a worldwide expert network for AI and machine learning, says the market in the UK for all staff with AI expertise is being made tighter by a "hiring frenzy". He points to a study by job search website indeed.com that shows the number of jobs in AI in the UK grew by 485 per cent from 2014 to November 2017.

"AML is probably one of the biggest opportunities in the financial and regulation services," Dr Bebbington says. "We have seen this first-hand from our clients, and the demand is high for such a skill set."

The skills shortage is concerning for C-suite executives. They are desperate for AI experts in general, and those with AML expertise are particularly thin on the ground.

As a result of this shortage of talent, top AML-focused developers, who can understand, strategise and apply their expertise come at a premium price – anywhere between £60,000 and £300,000 a year, suggests Dr Bebbington.

Thankfully, there is a path that doesn't involve hiring key staff at a salary up to twice that of the Prime Minister. One part of that could be helping an organisation's existing developers become comfortable dealing with AI and big data. Among the tools is a site named Kaggle which offers graded exercises and competitions that help developers hone (and show off) their data science skills.

An organisation building a team might find that the expert in data science doesn't have in-depth AML knowledge, says Dr Bebbington, and indeed Kaggle competitions about anti-money laundering can be won by data scientists without specific AML knowledge.

"If one can define a target and understand your data's features then a data scientist has all they need. Being a subject matter expert becomes secondary and referenced [for future jobs] when results are generated."

David Divitt, vice-president, product management, fraud and AML at payment systems provider Vocalink, says bringing in data scientists and developers from outside the narrow field can sometimes be beneficial.

"This can actually support the recruitment process and also be highly productive as those individuals bring in a different view of the problem and often aren't clouded by the traditional ways of devising a solution," he says.

"We have been very successful bringing in these varied skill sets from disciplines such as astrophysics in order to broaden our experience base."

The team's skills don't need to be fully advanced before starting to make progress. Tim Tully, senior vice-president and chief technology officer of San Francisco-based big data company Splunk, believes developers should "jump straight in" using existing software libraries and then developing more bespoke software as their skills develop.

Mr Tully says: "We see more organisations using out-of-the-box, tailored tools as the fastest way to get rolling on AML while their talent continues to train."

Wherever the staff comes from, it is clear that a new way of thinking is taking hold. As Mr Divitt notes, the traditional path to insuring against AML for financial institutions has been the quantity of staff, rather than quality.

"AML has traditionally been an industry where throwing more staff at an issue was the typical way of dealing with problems," he says. "For this reason, many companies may employ lots of less trained staff instead of a fewer number of very skilled people.

"In order to deal with some of the newer and more sophisticated money laundering occurring today, the industry needs to focus on highly modern technology with skilled staff who are able to fully use it to its full potential."

Mr Curtis of LexisNexis says companies need to manage the transition carefully. "Ultimately, there is a fine balancing act: whenever technology advances there is always a risk of a skills gap emerging, either because individuals need a greater level of training, or because technologies replace certain roles, making expertise in that area more uncommon."

However, Thomas Webb, director of the fraud and white collar crime team at law firm Burges Salmon, says AML teams "will not succeed in isolation".

He adds: "They can only operate successfully within an institution that has an embedded culture of propriety, transparency and compliance, the responsibility for which remains with the institution's senior management."

"We see more organisations using out-of-the-box, tailored tools as the fastest way to get rolling on AML while their talent continues to train

Five new technologies on the front line

Cloud and big data have already helped transform AML. What's next?

1

OLIVER PICKUP

Take a wide view

"A 360° solution can transform enterprise decision-making regarding anti-money laundering (AML) by providing the most comprehensive, accurate, real-time and actionable customer engagement insights across millions of data points spread over multiple channels," says Jai Ganesh, senior vice-president and head of Next Labs at Mphasis, an Indian IT services organisation. Increasingly, organisations are looking for a 360° view of their customers, and investing accordingly. Dr Ganesh adds: "Such solutions can offer feature-rich business intelligence and actionable insights by bridging the gap between enterprise data and external and third-party data, such as social media, credit scores, open data and other multimedia datasets."

2

Artificial intelligence

A computer can quickly scan transactions to find those that aren't normal. But what happens when the definition of "normal" changes? This is one of the benefits of moving to an AI-based system – it can adjust its reasoning when a person or institution changes its behaviour, avoiding a blizzard of false alerts. But "normal" can also change when those seeking to disguise transactions switch tactics – which they frequently do. The best AI implementations can not only detect new types of anomaly in real time, but they can also explain their reasoning, providing vital intelligence on threats and attacks.

Data visualisation

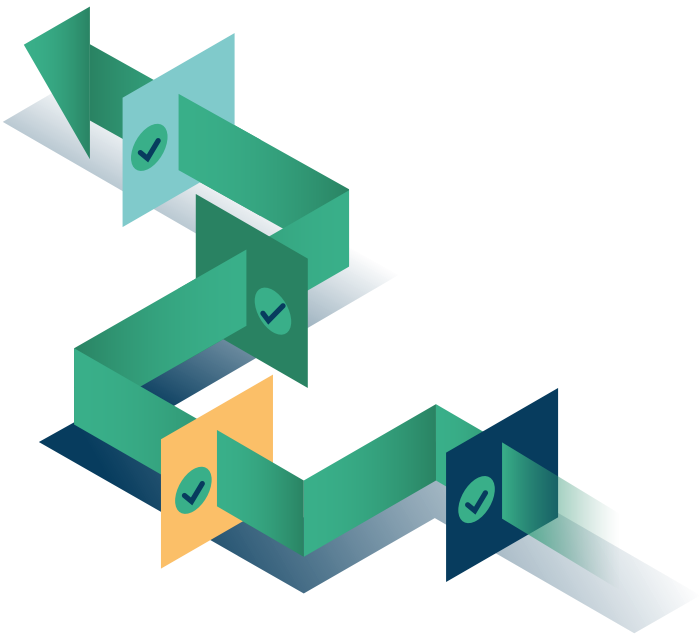
The partnership between people and technology can only work if the there is clear communication between them – and sophisticated data visualisation is an essential part of that. This is much more than a traditional dashboard-type display, where the AI or other software is reporting its activities. Real data visualisation allows a deep dive into specific activities, real-time insights, sophisticated prioritisation of alerts, and more generally helps create the digital space in which humans and machines interact to pursue their common goal.

Natural language processing

A report prepared in 2017 for the Financial Conduct Authority (FCA) highlighted natural language processing as having great potential, particularly when used in combination with other technologies such as machine learning. Some of the tasks currently being performed by staff could be automated using this technology, it reckoned, not only reducing costs but allowing more consistency. It would also help solve a problem that appears simple but causes a profound difficulty in rooting out money laundering: that a person may have multiple variations of their name, making it harder to track their activity.

Blockchain

The same FCA report reported very mixed views on the use of blockchain technology, which employs advanced cryptography to create a public, distributed database and has been touted as a way of improving the transparency of financial systems generally. The report concluded: "In practice, the most common view espoused [from both technology and regulated firms] was that truly compelling blockchain use cases had yet to be articulated in AML compliance, restricting the pace of adoption." One key issue was that staff who truly understand the technology are in very short supply, not only in financial institutions but also at regulators.



RACONTEUR

feedzai