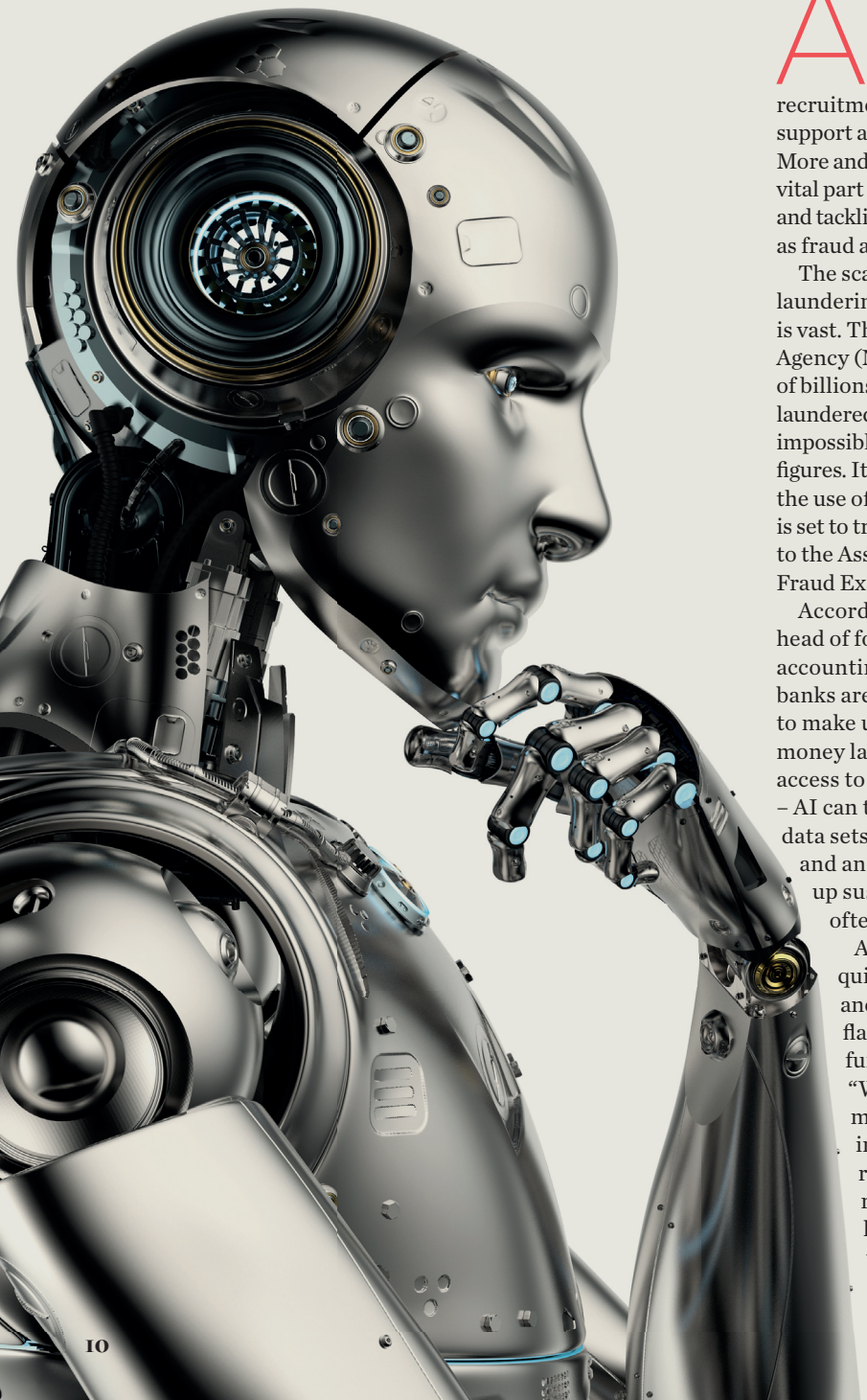
ARTIFICIAL INVESTIGATORS

AI is a powerful tool in fighting financial crime. But it also comes with risks



AI has the potential to revolutionise every aspect of daily life. Businesses use AI for recruitment, customer service support and sales, to name a few. More and more, it's become a vital part of security surveillance and tackling financial crime such as fraud and money laundering.

The scale of money laundering in the UK alone is vast. The National Crime Agency (NCA) believe hundreds of billions of pounds are laundered each year, but it's impossible to know the exact figures. It's no surprise then that the use of AI in fraud detection is set to triple by 2021, according to the Association of Certified Fraud Examiners (ACFE).

According to Jim Gee, head of forensic services at accounting firm Crowe, the big banks are in the best position to make use of AI to fight money laundering. They have access to vast volumes of data – AI can trawl through massive data sets to identify patterns and anomalies and flag up suspicious activity, often in real-time.

AI, says Gee, learns very quickly what is normal and what isn't and can flag up anomalies for further investigation. "With technology used more effectively and innovatively, you can reduce manual and repetitive tasks, and humans can focus on the more material risks," he adds.

Limited capabilities

However, Adam Williamson, head of professional standards at AAT, says AI's ability to deal with big data is the "extent of its capabilities" right now. It hasn't got to a level where it can make complex decisions. It is excellent at data mining and helps accountants make connections and perform due diligence.

José Hernandez, forensic accountancy specialist, author of *Broken Business* and founder and CEO of Ortus Strategies has worked on some of the largest fraud, bribery and money laundering cases on record. He says it would "not have been possible" to gather relevant facts and evidence relating to the cases had it not been for AI.

"Each of the significant internal investigations we have been involved in has employed very sophisticated digital forensic tools. They used AI to organise, search and analyse vast quantities of data such as emails, chats, text messages, calendar entries and financial records," he says.

"These cases often involved a dark web of third-party intermediaries and offshore shell companies. Without such tools, we would not have been able to separate signal from noise and identify patterns quickly and efficiently."

Hidden criminals

As Hernandez explains, AI tools play a crucial role in helping organisations identify hard-to-detect forms of criminal activity.

AI can also help identify modern slavery practices and human trafficking, says Williamson. It comes into play when gang leaders bringing trafficked people into the UK open up multiple bank accounts in numerous branches (often on the same day).

"It's a smurfing technique, where small amounts of money are put into multiple accounts as a way of hiding large amounts of money," Williamson explains. "Someone might be paid £500 every week, or there might be regular, multiple payments to travel agencies and low-cost airlines. On their own, such transactions may not necessarily be suspicious, but together, they can point to trafficking and other unlawful activities."

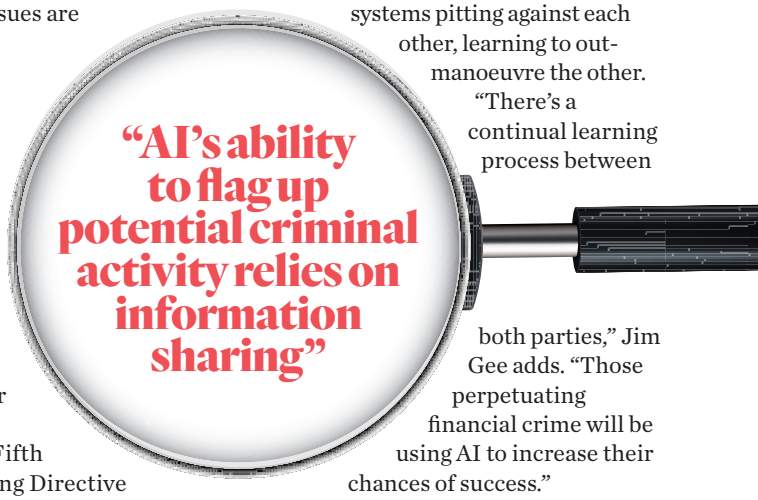
Often, AI's ability to flag up potential criminal activity relies on information sharing, particularly as gangs will open up accounts across different banks. Williamson says there is a general "market reluctance" to share information, not least because ethical and confidentiality issues are arising from data collection.

"If you have limited data to work with, the system can't make the connections and join the dots," he says. "Banks aren't always happy to give out customer information."

However, the Fifth Money Laundering Directive – due to come into force in January 2020 – focuses on transparency and direct access to information. It will require banks to hold registers of bank accounts, their owners and beneficiaries, so AI systems will hopefully have more access to vital information.

Unethical AI?

However, ethical issues are arising from AI to tackle this type of crime, and not just around data protection and information ownership.



Williamson warns there have been countless examples of inbuilt or learned bias from AI because it hasn't yet got the cognitive ability. Limited data sources and crude programming can result in discriminatory conclusions.

He uses the example of loan approvals, where people from a particular demographic or background may be turned down for loans despite meeting the criteria. It happens because the system has "learned" from previous process outcomes or is using limited data sources to determine risk. "AI will exacerbate any inbuilt or learned bias," he says.

There's also the issue of AI itself being used to commit crime. Williamson likens it to financial chess, with two systems pitting against each other, learning to out-manoeuvre the other.

"There's a continual learning process between both parties," Jim Gee adds. "Those perpetuating financial crime will be using AI to increase their chances of success."

The most significant impact on fraud and financial crime, he says, has come from changing the balance of human behaviour: mobilising and growing the "honest majority" and deterring and shrinking the "dishonest minority".

Gee insists that the future of AI lies in identifying weaknesses of criminal systems – for every flaw removed is another financial crime stopped. "Ultimately though," he says, "AI needs to prevent crime, not just detect it."