Artificial Intelligence and Economic Crime

06 September 2023

In today's digital age, where technology is advancing at an unprecedented pace, the rise of artificial intelligence (AI) has brought about both awe-inspiring possibilities and unprecedented threats in relation to economic crime.

While AI can be a powerful tool in combating economic crime, it can also be exploited by criminals to perpetrate sophisticated and elusive offences.

AI, with its ability to analyse vast amounts of data and identify patterns, has revolutionised the way we approach economic crime prevention. Machine learning algorithms can sift through mountains of financial transactions, detecting anomalies and flagging suspicious activities that might otherwise go unnoticed.

In June this year, to great fanfare, Google Cloud launched its AI-driven anti-money laundering tool. This marks a big departure from the traditional AI economic crime tools, as rather than starting with human determined rules to tell the AI where to look, Google’s tool does it all itself. This AI-first approach is proving successful at HSBC, which has reported that the Google tool has reduced alerts by 60% while increasing true hits by two to four times.

Such developments in AI will continue to drive down costs for financial institutions and allow the human experts to focus on the most serious cases. Ultimately, this should reduce economic crime and bolster the integrity of the financial system.

However, as AI evolves, so do the tactics employed by criminals. They are quick to adapt and exploit the very technology designed to thwart them. Cybercriminals are leveraging AI to develop sophisticated attacks, making it increasingly difficult for traditional security measures to keep up. AI-powered bots can mimic human behaviour, bypassing security protocols and infiltrating systems undetected. This has led to a surge in identity theft, phishing scams, and ransomware attacks, causing billions of dollars in losses annually.

One of the most concerning aspects of AI-driven economic crime is the potential for deepfakes. Deepfakes are manipulated videos or audios that convincingly depict someone saying or doing something they never did. Criminals can use this technology to impersonate high-ranking executives to authorise fraudulent transactions. The consequences of such deepfake attacks can be catastrophic, eroding trust in financial institutions and destabilising markets.

What’s clear is that the battle between AI and economic crime will continue for years to come. Criminals are continuously refining their techniques, exploiting AI's weaknesses and finding new ways to evade detection. As AI becomes more sophisticated, so do the criminals who seek to exploit it. This cat-and-mouse game requires constant innovation and collaboration between law enforcement agencies, financial institutions, cybersecurity experts, and AI developers.
In addition to this, the ethical implications of AI in economic crime prevention also have to be considered. Striking the right balance between privacy and security is a delicate task. AI algorithms need access to vast amounts of personal data to effectively detect and prevent economic crimes. However, this raises concerns about potential misuse of personal information and invasion of privacy. Stricter regulations across the globe are anticipated, but the criminals are unlikely to pay any attention to them and so could give the criminals an advantage in the ongoing battle with economic crime prevention.

TLT’s Economic Crime Compliance team has significant experience of advising clients on the design, implementation and operation of AI-led economic crime compliance programmes. Speak to us to discuss how you can use AI to streamline your compliance programme to enhance the efficiency and effectiveness and seek to gain the advantage over the economic criminals.

This publication is intended for general guidance and represents our understanding of the relevant law and practice as at September 2023. Specific advice should be sought for specific cases. For more information see our terms & conditions.