

Interview by Business
Time Azerbaijan with
Sabuhi Abilhasanli,
Audit Director at
KPMG in Azerbaijan.

WHEN FALSE LOOKS REAL: AI AND THE CHANGING FACE OF FRAUD

– **Sabuhi, how would you define what is actually changing with AI in the context of fraud and audit?**

– What is changing is the nature of trust in business information. AI has changed not only the tools of fraud but also the reliability of what businesses assume is genuine. Documents, identities, messages, and even voice or video interactions can now be fabricated convincingly and at scale. For audit, this means fraud is no longer limited to manipulating real documents or real systems. It can now be created from scratch and still appear legitimate.

This is why AI-related fraud is such an important shift. It challenges a basic assumption in business and in audit that evidence can be trusted simply because it looks authentic. KPMG's global research shows how serious this has already become: 81 percent of surveyed organizations reported attempted or successful AI-powered fraud over the previous 12 months.

This shift also has important implications for audit. While external auditors are not responsible for detecting all fraud, they are required to obtain reasonable assurance that the financial statements are free from material misstatement, whether caused by fraud or error.

– **If we now move to practical impact – how is this AI-driven fraud landscape affecting companies in Azerbaijan?**

– In Azerbaijan, the exposure is increasing as more companies rely on digital workflows, remote approvals, electronic documentation, and faster onboarding of counterparties.

Sectors with higher transaction volumes, remote communication, digital onboarding, or complex procurement processes are likely to face greater exposure. This may include financial services, energy, infrastructure, logistics, and procurement heavy businesses. In these environments, AI can be used to imitate identities, create convincing supporting documents, or simulate legitimate counterparties.

The main challenge is that fraud is becoming harder to identify through traditional warning signs. In many cases, the issue is no longer whether something looks suspicious. The issue is whether something that looks normal is actually real.

– **Deepfakes and synthetic identities are often discussed. Why are they such a concern for audit and internal controls?**

– Because they weaken one of the most basic assumptions in business: that what we see and hear can be trusted.

Deepfake technology can now imitate voice, video, and written communication with a high level of realism. This creates practical risks for companies: fake executive instructions, impersonation of suppliers or business partners, manipulation of verification calls, and false identities used in digital onboarding.

KPMG's deepfake research highlights exactly this problem: many traditional control environments still rely on visual, verbal, or document-based confirmation. In an AI-driven environment, those signals are no longer enough on their own.

– **Why are traditional internal control systems struggling to respond to this shift?**

– Because they were designed for a different risk environment. Traditional controls assume that fraud is usually carried out by humans, that it leaves inconsistencies, and that verifica-

tion through documents, signatures, calls, or video is generally reliable. AI challenges all of these assumptions at the same time.

A document can now be fully synthetic. A voice can be cloned. A video call can be manipulated. And all of it can appear internally consistent enough to pass routine checks.

That is why the question today is not only how to detect fraud. It is how to validate authenticity when false authenticity can be manufactured at scale. KPMG describes this as a shift from detecting suspicious anomalies to dealing with fraud that increasingly looks like normal activity.

– **How is the audit profession changing in response to these developments?**

– We are seeing a clear shift from periodic audit toward continuous, data-driven assurance.

KPMG's global audit transformation approach emphasizes how technology, automation, and AI are being used to strengthen audit quality, expand data analysis, and help auditors focus more effectively on areas of higher risk. This allows audit teams to move beyond routine manual work and spend more time applying professional judgment where it matters most.

For a market like Azerbaijan, where many industries are becoming more digital and transaction-heavy, this evolution is especially relevant. The role of audit is therefore evolving from retrospective validation to ongoing risk intelligence.

– **Can AI also help detect fraud, or is it purely a risk driver?**

– It is both, and this duality is central to the current environment. The same technology that helps fraudsters generate convincing deception can also help organizations detect unusual patterns, anomalies, and hidden risk signals. KPMG's global research point to the growing use of AI and machine learning in identifying anomalies and suspicious patterns in financial data and audit processes.

However, there is still a readiness gap. Many organizations understand that AI-related fraud is increasing faster than their ability to detect it. So, the issue is not only whether AI can help. It is whether companies are adopting the right capabilities quickly enough.

– **Finally, how does KPMG position itself in helping organizations in Azerbaijan address these challenges?**

– KPMG's role is evolving from traditional assurance toward technology-enabled audit and risk insight. This includes embedding AI and data analytics into audit methodologies, identifying emerging fraud typologies such as deepfakes and synthetic identities, supporting governance frameworks for responsible AI usage, and strengthening internal control environments across increasingly digital ecosystems.

Ultimately, the objective is to help organizations maintain trust in systems that are becoming more automated and complex. Audit is no longer only about verifying financial accuracy; it is about ensuring confidence in the integrity of digital business environments.

Leyla Akhundova