How Advanced Technologies Are Reshaping the Banking Sector's Tools in Confronting Risks

Dr. Maher Al-Mahrouq
General Director of the
Association of Banks in Jordan

Financial fraud is no longer merely a technical threat that can be contained through traditional regulatory tools; it has evolved into a complex ecosystem reflecting profound transformations in the nature of the global digital economy. As technological innovation accelerates, fraud methods evolve in parallel at an even faster pace, driven using artificial intelligence, digital business models, and cross-border organized networks. This makes the greatest challenge today the protection not only of systems, but also of the very logic of decision making within financial institutions, in a digital environment where reality and forgery intertwine to an unprecedented degree.

Within this framework, the Association of Banks in Jordan continues to play its role as a unifying and active platform for enhancing the readiness of the banking sector. The Association held its first quarterly briefing session of 2026 at a particularly critical juncture, with the aim of shedding light on the most significant transformations in the field of combating financial fraud, and of looking ahead to the future tools and technologies capable of confronting these escalating challenges.

The discussions held during the session demonstrated that the nature of financial fraud is no longer what it once was. Whereas fraudulent operations were previously based, for the most part, on limited individual practices, today they rely on interconnected systems that operate across multiple channels and harness advanced digital technologies to construct synthetic identities, reinforce false credibility, and adapt dynamically to oversight systems. Consequently, the challenge is no longer confined to detecting suspicious transactions; it has become tied to the capacity of institutions to understand complex behavioral patterns, analyze the relationships among data, and detect attempts to influence decisions before the fraudulent operation is completed.

Among the most prominent conceptual shifts that have emerged in this field is the transition from traditional models based on the analysis of individual transactions to more advanced models that rely on what is known as Hypothesis Generation. These models allow for the simultaneous exploration of multiple scenarios and the linking of data received from various sources, including financial institutions, regulatory bodies, and financial intelligence units. This approach represents a qualitative leap in the way risks are addressed; however, it simultaneously raises challenges related to data governance, accessibility, and ensuring that data is used within clear regulatory frameworks.

In this context, artificial intelligence is assuming a growing role as one of the principal drivers in advancing detection and analysis capabilities. It is now being used to link events within broader contexts, build predictive models, and analyze multiple scenarios in real time.

The development of explainable artificial intelligence models has likewise gained increasing importance, as it bolsters the confidence of regulatory authorities, ensures the responsible use of these technologies, and enhances the capacity of financial institutions to continuously develop their capabilities and maintain their defensive edge.

Within this context, a number of advanced technologies have emerged that are reshaping the landscape of combating financial fraud. Foremost among these are machine learning and deep learning technologies, alongside advanced data analytics tools. Together, they represent a practical extension of the shift toward more intelligent and integrated risk management models, in response to threats that are no longer traditional but have likewise become driven by artificial intelligence and capable of continuous adaptation and evolution.

These technologies enable a transition from traditional approaches based on fixed rules and after-the-fact verification toward dynamic models capable of continuous learning, the analysis of vast volumes of data in real time, and the discovery of hidden patterns that are difficult to identify through conventional means. This includes tracking behavior across multiple channels and understanding the full context of an interaction, rather than focusing solely on the financial transaction itself.

The importance of anomaly detection systems is likewise becoming evident as a pivotal tool for proactively identifying unusual behaviors, even in the absence of previously known fraud indicators. The most recent advancement, however, lies in the move toward models capable of analyzing "decision-making behavior" itself and detecting attempts to influence users through fake digital identities or misleading interactions, particularly considering the growing use of deepfake technologies and AI-powered fraud.

This shift constitutes a qualitative transformation in working methodologies. The focus is no longer limited to analyzing individual transactions; it now extends to building advanced predictive models that link data with various contexts, thereby contributing to the enhanced effectiveness of oversight systems.

This in turn calls for strengthening data governance frameworks, ensuring data quality, and developing explainable models that support compliance requirements and reinforce the confidence of regulatory authorities, all within an environment that requires real-time response and a higher degree of integration among the various risk management systems.

It is also impossible to overlook the future trajectories associated with quantum computing, which carries unprecedented potential for processing complex data while simultaneously raising fundamental challenges related to information security and encryption systems. This calls upon financial institutions to prepare early and to build resilient capabilities capable of adapting to these transformations.

Considering these accelerating developments, cooperation among the various parties has become more important than ever. Confronting financial fraud is no longer the responsibility of a single entity; it requires the coordination of efforts among banks, regulatory authorities, and security agencies, as well as the strengthening of information sharing mechanisms and the adoption of joint approaches grounded in international best practices.

From this standpoint, the Jordanian banking sector, with the support of the Central Bank of Jordan, continues to enhance its readiness to confront these challenges. It draws upon a robust regulatory framework, an advanced level of compliance, and growing investment in digital transformation and modern technologies. This reflects its commitment to preserving the soundness of the financial system, reinforcing the trust of customers, and ensuring the continuity of operations with both efficiency and resilience.

In a world where technologies advance at the same pace as risks, progress in the tools used to combat fraud is no longer an operational option but a strategic necessity. The capacity to adapt to these transformations, to anticipate threats, and to build more intelligent and integrated systems will remain the decisive factor in protecting financial institutions and safeguarding the trust that constitutes the fundamental pillar of the banking sector's sustainability.