Banks must rethink fraud controls as AI risks rise

THE recent Sessions Court ruling ordering a local bank to pay RM166,000 for failing to monitor anomalous transactions represents a critical inflection point for corporate governance in Malaysia.

By holding the institution liable for ignoring sudden, uncharacteristic account activity, the court effectively dismantled the legacy defence that merely having a secure system, such as sending automated SMS alerts, absolves an organisation of its duty of care.

The ruling sets a clear legal baseline: financial institutions cannot remain passive when faced with glaring transactional anomalies. It reinforces the expectation that financial compliance requires active, intelligent monitoring of escalation triggers, particularly when a transaction drastically deviates from established customer behaviour.

However, if our institutions are currently facing legal liability for missing traditional, rudimentary anomalies, they are alarmingly exposed to the incoming wave of AI-driven financial manipulation. What used to be neatly divided into IT risk versus finance risk is now one combined problem. Cybersecurity and financial compliance can no longer sit in separate rooms.

AI does not necessarily create new categories of fraud; it amplifies existing ones with devastating precision. The 2024 Arup incident, where a British engineering firm lost US$25mil after an employee transferred funds based on a deepfake video call with fabricated "senior management", serves as the global anchor case.

It proves an uncomfortable reality: we can no longer trust the channel. Relying on email authenticity or even live video confirmation is now an outdated assumption.

Furthermore, AI enables virtually undetectable fraud at scale. Instead of a single large, suspicious transfer, malicious actors can execute hundreds of micro transactions over time.

In this modern *One Cent Thief* (Malaysian television drama) scenario, each transaction sits comfortably below automated detection limits and approval thresholds but aggregates into significant corporate losses.

This is where our current regulatory frameworks face a critical gap. The Cybersecurity Act 2024 provides a strong foundation for strengthening system resilience and reporting breaches.

However, AI introduces a fundamentally different risk. It does not necessarily hack the system; rather, it manipulates how human decisions are made.

While current cybersecurity laws protect the infrastructure, they do not fully address the deception embedded within the financial workflow itself.

To survive this shift, corporate boards and audit committees must recognise that the answer is not simply telling employees to "be careful". Financial approval systems must be actively redesigned to withstand deception.

High-risk actions, such as large payments, urgent transfers or changes to vendor bank details, must trigger mandatory, independent, out-of-band verification using pre-approved contact channels.

Equally critical is the human factor. Fraud often succeeds not because a policy does not exist, but because an employee is pressured by urgency or perceived authority into bypassing it. Corporate culture must empower people to pause, question and escalate suspicious, time-sensitive instructions.

Crucially, no employee should ever be penalised for slowing down a transaction to exercise independent judgment.

The future of financial security is not just in building stronger firewalls; it is in disciplined human decision-making, better audit trails and structured verification built directly into financial processes.

As the recent court ruling demonstrates, the expectation of accountability is not new. The law is simply evolving to demand that our internal controls are robust enough to manage exactly how decisions are made and acted upon.

THULASY SUPPIAH
Kuala Lumpur