Circular on Cyber Risks Associated with Generative Artificial Intelligence and Deepfakes

In light of rapidly evolving cyber threats and the recent surge in deepfake-related incidents globally, including impersonation scams and fraudulent activities, the Monetary Authority of Singapore ("**MAS**") has published two papers concerning cyber risks associated with generative artificial intelligence ("**GenAI**") and deepfakes. These papers aim to increase awareness by providing an overview of the cyber threats associated with GenAI and deepfakes, the risk implications and possible mitigation measures that could be taken to address the risks.

Lawyers should be cognisant of the evolving cyber developments and their risk implications, and are encouraged to review the two papers and – where applicable – implement the recommended (appropriate) risk mitigation measures as part of your internal controls, at the earliest opportunity.

Key Points from Paper on Cyber Risks Associated with GenAI

GenAI is now used by cyber threat actors to create (convincing) phishing emails, fake documents, and even realistic identities via synthetic media. Criminals may – amongst other things – abuse GenAI to circumvent customer due diligence ("**CDD**") / enhanced customer due diligence ("**ECDD**") measures. Lawyers should note the:

- **Emerging attack vectors** such as AI-generated scams and fraud risks (e.g. identify theft) affecting CDD/ECDD processes;
- **Risks identified** across various business aspects (i.e. people, process and technology) such as unauthorised access to client data, manipulation of transaction records, and injection of false identities or beneficial ownership information via AI-created (forged) documentation, data manipulation and bypassing of data system guardrails; and
- **Possible mitigation measures** such as the strengthening of data security and governance, enhancing your awareness of GenAI-enabled threats, implementing anomaly detection controls, and promptly reviewing transactional or client onboarding activity that are incongruent with standard client profiles.

Key Points from Paper on Cyber Risks Associated with Deepfakes

Deepfakes (e.g. digitally manipulated audio, video, or documents convincingly replicating a person's likeness or authority) are a growing vector that facilitate impersonation, falsified documents and fraudulent transactions. Lawyers with remote or cross-border transactions, for example, are at elevated risk of deepfake or AI-enabled compromise of your anti-money laundering, countering the financing of terrorism and countering proliferation financing ("**AML/CFT/CPF**") processes and measures. Lawyers should note that the:

- **Techniques** include AI-powered impersonation, fake instructions for payment or to access sensitive client information, and altered video or call content submitted for remote identification and verification of client's identity in response to CDD/ECDD checks;

- **Vulnerable areas** include non-face-to-face transactions and CDD/ECDD performed, transaction authorisations, and ongoing client verification – including those involving high-risk clients and/or clients outside of Singapore; and
- **Possible risk mitigation measures** include (where applicable) conducting robust documentary, call and/or video verification, implementing deepfake detection tools, strengthening processes and controls for high-risk transactions and educating staff on red flags and on deepfake and GenAI-enabled risks.

What can you do?

You should keep abreast of evolving cyber risks and threats, relevant cyber risk advisories and ensure that your risk mitigation measures, internal controls, staff training, and technological and system defenses are reviewed and enhanced where necessary. You are encouraged to review how cyber-enabled threats may intersect directly and/or impact your business in fulfilling AML/CFT/CPF obligations, such as CDD/ECDD measures when dealing with transactions and clients. You should regularly review your risk assessment and internal policies, procedures and controls in place to ensure that they remain updated and relevant, thereby ensuring that they (i) address risks posed by evolving technology – including but not limited to GenAI and deepfake technologies – and (ii) are in alignment with AML/CFT/CPF requirements.

Please disseminate the information in this circular to all other relevant personnel in your law practice.

Click **here** to access "MAS/TCRS/2024/05: Cyber Risks Associated with Generative Artificial Intelligence".
Click **here** to access "MAS/TCRS/2025/06: Cyber Risks Associated with Deepfakes".