Technology, Media & Telecommunications | Financial Institutions Group

Generative AI and Financial Institutions – MAS Provides Insight on Cyber Risks and Mitigation Measures

Introduction

Generative Artificial Intelligence ("**GenAI**") has proven an innovative and game-changing resource for businesses, while also presenting an array of thorny challenges. While GenAI has been adopted across a wide range of industries, its application to financial institutions ("**FIs**") raises some unique issues, both in terms of opportunities and attendant risks.

In light of this, the Monetary Authority of Singapore ("**MAS**") has published an information paper on "Cyber Risks Associated with GenAI" ("**GenAI Paper**"). The GenAI Paper aims to raise FIs' awareness by highlighting key cyber threats arising from GenAI, the risk implications, and the appropriate mitigation measures that FIs can take.

GenAI tools are already frequently used by FIs, and the associated cyber risks cannot be ignored. Similarly, it is vital for FIs to be aware of the risks arising from the use of GenAI by threat actors, and to take the necessary precautions. Failure to do so would open the FI up to cyber attacks, scams, and data leakage, which could impact the organisation both financially and reputationally, and may lead to potential regulatory repercussions.

In this regard, Rajah & Tann is able to assist FIs in understanding the risks that come with GenAI, as well as the mitigation measures that FIs may wish to implement. The relevant issues span across various areas of practice and should be looked at holistically to effectively deploy the necessary solutions. Rajah & Tann stands as a full-service firm with sectoral specialists that provide integrated and comprehensive advice, including our Technology, Media & Telecommunications Practice and our Financial Institutions Group.

Further, the topic of GenAI is necessarily a highly technical one, requiring expert technological input. Rajah & Tann Technologies and Rajah & Tann Cybersecurity are uniquely placed to assist FIs to protect, mitigate against cyber attacks, and minimise disruptions.

In this Update, we highlight the key features of the GenAI Paper and what it means for FIs. We also provide an overview of the solutions that Rajah & Tann Technologies and Rajah & Tann Cybersecurity can provide, mapped against the elements of the GenAI Paper.

Background

GenAI technology carries vast potential for FIs to make their business processes more productive, efficient and convenient. Some of the possible use cases include the automation of data extraction, acceleration of research, streamlining of operations, and enhancement of customer experience.

At the same time, there are many risks associated with the use of GenAI, particularly for FIs. These include:

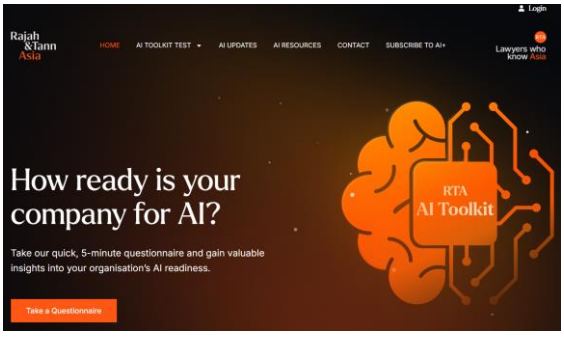
- Deepfakes and GenAI-enabled phishing;
- Malware generation and enhancement;
- Data leakage from GenAI deployment; and
- GenAI model and output manipulation.

The above risks have been highlighted by MAS in the GenAI Paper, setting out the scope of the threats, the relevant impact to the FI, and the appropriate countermeasures. In the next section, we summarise the guidance provided and set out the solutions that Rajah & Tann Technologies and Rajah & Tann Cybersecurity can provide, as mapped against MAS' GenAI Paper.

MAS has indicated that the GenAI Paper will be followed by an information paper on AI model risk management by the fourth quarter of 2024 or the first quarter of 2025. In the meantime, the full GenAI Paper is available here.

RTA AI Toolkit

In line with the industry focus on AI, Rajah & Tann Asia has unveiled the RTA AI Toolkit, an interactive AI portal designed to comprehensively evaluate your organisation's AI readiness across five Southeast Asian countries in just five minutes. Dive into the collection of AI resources, from latest news and guidelines to incisive publications on related trends and developments. Be at the forefront of AI integration and take your journey to the next level with us.



Aspect	Threats	Impact	Countermeasures	Solutions from Rajah & Tann Technologies & Rajah & Tann Cybersecurity
2.1 Deepfakes and GenAI-Enabled Phishing				
People	• Deepfakes can make impersonation more convincing, posing significant risks for organisations	• Business e-mail compromise (BEC) • Loss of personally identifiable information ("**PII**") or FI confidential data • Financial loss	• Conduct deepfake awareness campaigns • Reconfirm identity with another factor • Leverage new technologies to detect deepfakes and AI-generated content	• Automated AI powered phishing protection • Vishing Protection: Deepfake video/image generation and identification services to bolster defences • Extensive online eLearning library of deepfake and cybersecurity awareness courses • Phishing or cybersecurity table-top exercises with AI-generated deepfake videos/images • Deepfake identification services
Process	• Threat actors can leverage GenAI to create realistic images, videos, speech, and personas for fraud and deception	• Financial loss • Identity theft • Data exposure	• Implement additional user verification for high-risk transactions and high-risk roles by different means such as challenge questions, email etc.	• Re-design or update existing procedures to deter deepfake scams • User verification procedures and business processes

Aspect	Threats	Impact	Countermeasures	Solutions from Rajah & Tann Technologies & Rajah & Tann Cybersecurity
Technology	• New account creation fraud, and bypassing existing authentication mechanisms with fake identities • Spread of fake news with botnets (with possibility of market manipulation)	• Fraud risk • Security compromised • Money laundering schemes • Evading security protocol • Market manipulation	• Implement deepfake detection tools • Implement additional • verification for high-risk transactions	• Zero trust authentication and permissions management solutions for client systems and key, highly sensitive business processes
2.2. Malware Generation and Enhancement				
People	• Malware sent through phishing links	• Financial loss • Loss of PII	• Conduct user awareness campaigns • Maintain basic cyber hygiene	• Regular MAS Cyber Hygiene audits for enterprises • Vishing Protection: Deepfake video/image generation and identification services to bolster defences • Extensive online eLearning library of malware and cybersecurity awareness courses • Phishing or cybersecurity table-top exercises with AI-generated deepfake videos/images • Deepfake identification services

Aspect	Threats	Impact	Countermeasures	Solutions from Rajah & Tann Technologies & Rajah & Tann Cybersecurity
Process	• Inability to detect new malware	• Delayed detection of threats • Delayed containment of malware	• Adopt a multi-layered cyber defence strategy • Incorporate solutions that leverage machine learning and heuristics-based behavioural detection to stop both legacy and new malware threats	• Automated AI powered phishing protection • Review security architecture to identify weaknesses against AI threats • AI-powered endpoint detection and response solution, which uses machine learning and heuristics • Human risk-centric approach towards cultural and attitudinal change required to protect against malware threats
Technology	• Polymorphic AI malware which evades detection • Outdated enterprise systems which are unable to detect malware	• Bypass of security measures leading to loss of sensitive information, financial loss and reputation damage	• Implement AI-powered tools to detect polymorphic malware • Incorporate AI and integrate threat intelligence into log monitoring to better identify anomalies and suspicious activities	• Deploy AI-powered Endpoint Detection and Response (EDR) solution to detect new polymorphic malware • Ongoing technology consulting and advice • Automated AI powered phishing protection

Aspect	Threats	Impact	Countermeasures	Solutions from Rajah & Tann Technologies & Rajah & Tann Cybersecurity
3.1. Data Leakage from GenAI Deployment				
People	• Intentional or unintentional data leaks by employees to public GenAI models	• Loss of customer data/ PII and FI secrets • Regulatory consequences and reputational damage	• Conduct awareness campaigns • Implement data classification for data which can be entered into GenAI models	• AI generated cyber risk awareness campaigns • Online and in-person training on effective GenAI prompting • Extensive online eLearning library of GenAI awareness courses including the risks associated with using these tools
Process	• Vulnerabilities or security weaknesses in in-house developed GenAI models • Risks of supply chain attack arising from the use of third party or open-source GenAI models	• Data leakage leading to loss of sensitive information • Backdoors and in-built vulnerabilities	• Adopt security best practices while developing GenAI models • Conduct third-party provided or open-source GenAI model risk assessment	• Conduct GenAI model risk assessments • Advise on security best practices to adopt when developing inhouse GenAI models • Integrated AI development and orchestration platform to enforce AI security and governance policies
Technology	• Inability to detect unusual user inputs • Bypass of GenAI model guardrails	• Loss of sensitive information • Data leak of PII • Reputational damage	• Implement Data Loss Prevention (DLP) tools and firewalls for GenAI models to mitigate loss of confidential data to GenAI models • Introduce controls while developing and using the GenAI models	• Conduct GenAI model risk assessments • Vulnerability assessments and adversarial testing on inhouse GenAI models • Red teaming • DLP protection in the use of internal GenAI services

Aspect	Threats	Impact	Countermeasures	Solutions from Rajah & Tann Technologies & Rajah & Tann Cybersecurity
			• Conduct vulnerability assessments and security testing on GenAI models	
3.2. GenAI Model and Output Manipulation				
People	• Insider threats • Access to foundation model and training data is not limited	• Unauthorised data access and loss of data integrity	• Implement maker-checker function to edit data in foundation models • Implement human-in-the-loop to verify that the output is as expected	• Review and design access controls for Foundation Models • Re-design or update client's procedures to implement human validators in acceptance testing of new in-house GenAI models • We offer an integrated AI development and orchestration platform to allow organisations to develop and enforce AI security and governance policies across multiple business problem statements. The solution supports multiple AI models as they are tailored for each business application across the enterprise.

Aspect	Threats	Impact	Countermeasures	Solutions from Rajah & Tann Technologies & Rajah & Tann Cybersecurity
Process	• Lack of proper access control to GenAI model data • Improper data governance for data used to train GenAI models if the data is not sanitised and verified • Lack of contingency measures for GenAI solutions	• Unauthorised data access • Poisoning of foundation model data • Impact to business operations due to disruptions to GenAI solutions	• Ensure robust access controls to the GenAI training data and foundation model • Establish proper GenAI model and data governance • Include contingency measures for GenAI solutions into business continuity plan • Conduct information sharing on issues and challenges faced during GenAI model deployment	• Permissions management solutions to control who has access to AI models • Audit of access approval processes • Develop client's AI Security and Governance checklist, based on industry standards • BCP planning for continual access to inhouse / commercial GenAI solutions
Technology	• Inability to monitor model performance, model drift, or unexpected behaviours • Inability to detect unusual model outputs	• Incorrect information provided to users • Reputational damage • Regulatory consequences	• Implement tools to log and monitor output of GenAI models	• Integrated AI development and orchestration platform to enforce AI security and governance policies • Assessment of adequacy of logging of GenAI services • GenAI model testing for unusual outputs

Contacts

Technology, Media & Telecommunications

Rajesh Sreenivasan
Head, Technology, Media & Telecommunications

T +65 6232 0751

rajesh@rajahtann.com

Steve Tan
Deputy Head, Technology, Media & Telecommunications

T +65 6232 0786

steve.tan@rajahtann.com

Benjamin Cheong
Deputy Head, Technology, Media & Telecommunications

T +65 6232 0738

benjamin.cheong@rajahtann.com

Click **here** for our Partners in Technology, Media and Telecommunications Practice.

Financial Institutions

Regina Liew
Head, Financial Institutions Group

T +65 6232 0456

regina.liew@rajahtann.com

Larry Lim
Deputy Head, Financial Institutions Group

T +65 6232 0482

larry.lim@rajahtann.com

Click **here** for our Partners in Financial Institutions Group.

Rajah & Tann Technologies

Raymond Lum
Chief Executive Officer
Rajah & Tann Technologies

T +65 6988 4903

raymond.lum@rttechlaw.com

Rajah & Tann Cybersecurity

Wong Onn Chee
Chief Executive Officer
Rajah & Tann Cybersecurity

T +65 6996 0404

onnchee@rtcyber.com

Please feel free to also contact Knowledge Management at eOASIS@rajahtann.com

Our Regional Contacts

RAJAH & TANN SOK & HENG | *Cambodia*
Rajah & Tann Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*
Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*
Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*
Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN | *Myanmar*
Rajah & Tann Myanmar Company Limited
T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

RAJAH & TANN | *Singapore*
Rajah & Tann Singapore LLP
T +65 6535 3600
sg.rajahtannasia.com

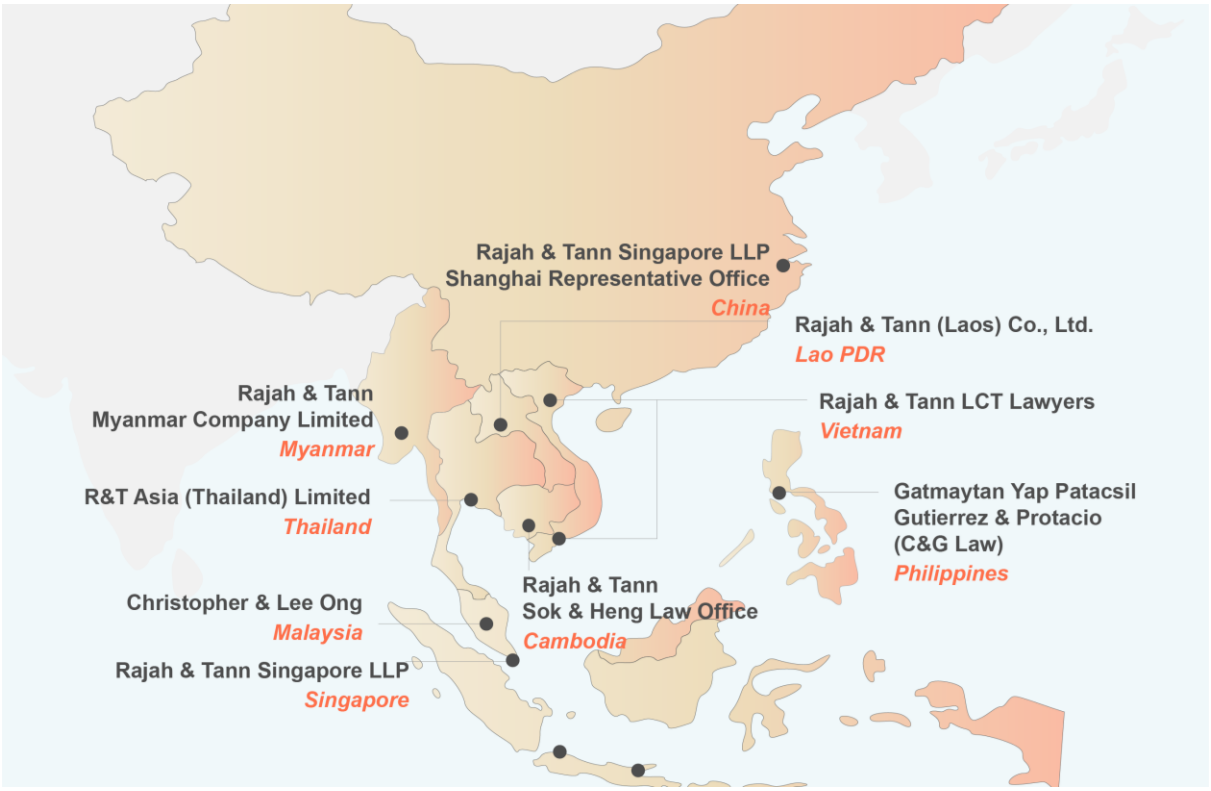
RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Our Regional Presence



Rajah & Tann Singapore LLP is one of the largest full-service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.