Technology, Media & Telecommunications | Financial Institutions

Dealing with Digitally-Enabled Scams – MAS and IMDA Launch Consultations on Duties and Liability of Financial Institutions and Telcos

Introduction

As digital payments and transactions continue their rapid growth, so too has the risk posed by digitally-enabled scams, which have become increasingly more prevalent. The Singapore Police Force has reported that from January to June 2023 alone, the number of scam and cybercrime cases reached 24,525, with the total amount reported to have been cheated sitting at an estimated S$334.5 million.[1] The financial repercussions of such scams can be substantial, and amidst the pressing concerns, certain questions have arisen regarding the responsibility for preventing scams. Who should bear the liability for scam losses – is it the banks, the telecommunication operators ("**Telcos**"), or the consumers themselves? What should be the duties on the part of parties such as financial institutions ("**FIs**"), Telcos and individuals regarding scams?

The Singapore regulators have sought to implement greater certainty in this regard by introducing relevant frameworks and guidelines. The Monetary Authority of Singapore ("**MAS**") and the Infocomm Media Development Authority ("**IMDA**") are now looking to further these efforts by establishing specific measures to address the responsibilities, duties and liability of the relevant parties – in particular, FIs and Telcos. On 25 October 2023, the following consultations were launched:

- **Shared Responsibility Framework**: MAS and IMDA published a joint consultation paper proposing a Shared Responsibility Framework ("**SRF**") specifically dealing with phishing scams. The SRF sets out anti-scam duties for FIs and Telcos and proposes a "waterfall approach" for sharing losses. Under this approach, responsible FIs will bear the losses if they have breached their duties, followed by responsible Telcos, with consumers bearing the loss only if the FIs and Telcos have carried out their SRF duties.

- **E-Payments User Protection Guidelines**: MAS has also published a consultation paper on proposed enhancements to the E-Payments User Protection Guidelines ("**EUPG**"). The EUPG deals with unauthorised and erroneous transactions (and not just phishing scams), setting out the responsibilities of FIs and consumers and their liability for losses. The proposed enhancements seek to address digitally-enabled scams by including established anti-scam measures, enhancing the duties of responsible FIs to facilitate prompt detection of scams and a fairer dispute resolution process, and enhancing the duties of consumers to take necessary precautions.

[1] https://www.police.gov.sg/-/media/9B26F6C9613B4760AC78D15EBCDB4048.ashx

The proposed SRF and enhancements to the EUPG are important developments for FIs, Telcos and consumers alike. Parties may wish to provide feedback and comments in response to the relevant consultations, which close on 20 December 2023.

This Update highlights the key features of the proposed SRF and the proposed enhancements to the EUPG.

Consultation Paper on Proposed SRF

The proposed SRF assigns responsible FIs and Telcos with relevant duties to mitigate phishing scams, and requires payouts to affected scam victims where these duties are breached. FIs and Telcos should take note of the specific anti-scam duties that have been set out and be aware that under the proposed SRF, failure to comply with such duties may result in their liability for scam losses. MAS and IMDA are seeking comments from industry stakeholders and members of the public on the key areas of the SRF which will be implemented via a set of Guidelines.

The SRF and the EUPG are closely related, as the SRF leverages on some of the proposed enhanced anti-scam measures in the EUPG that responsible FIs are expected to implement, and holds FIs and Telcos directly accountable to consumers should they fail to implement the prescribed measures.

Scope of SRF

The SRF is expected to apply to the following entities:

- **Responsible FIs** – Banks and relevant payment service providers (i.e. major payment institutions providing account issuance services where the payment accounts issued can store e-money).

- **Responsible Telcos** – Mobile network operators under the Telecommunications Act 1999 which provide cellular mobile telephone services.

The SRF will focus on a defined scope of phishing scams:

- **Digital nexus** – The scam should involve the consumer being deceived into clicking on a phishing link and entering his credentials on a fake digital platform, allowing the scammer to perform unauthorised transactions.

- **Singapore nexus** – The impersonated entities should be Singapore-based, or based overseas and offer their services to Singapore residents.

However, the SRF is not expected to cover the following types of scams:

- Malware-enabled scams;
- Scams where victims authorise payments to the scammer;
- Scams where a consumer was deceived into giving away his credentials to the scammer directly via text messages and non-digital means; and
- Other unauthorised transaction scam variants that do not involve phishing.

Waterfall approach

The question of which party will bear responsibility for scam losses under the SRF is based on a "waterfall approach", which operates as follows:

- **Step 1** – The responsible FI is placed first in line and is expected to bear the full losses if any of its duties under the SRF have been breached.

- **Step 2** – If (i) the FI has fulfilled all its SRF duties; and (ii) the Telco is assessed to have breached its SRF duties, the Telco is expected to bear the full losses.

- **Step 3** – If both the FI and Telco have carried out their SRF duties, the consumer bears the full scam losses. However, the consumer may still pursue further action through existing avenues of recourse, such as through Financial Industry Disputes Resolution Centre ("**FIDReC**").

This approach is intended to acknowledge the greater responsibility of FIs as custodians of consumers' money, and the secondary role of Telcos in fostering security of digital payments by facilitating SMS delivery.

Duties of FIs

The SRF sets out duties of responsible FIs, which are drawn from the duties under the EUPG. The duties are as follows:

- **Cooling off period** – Impose a 12-hour cooling off period upon activation of digital security token during which "high-risk" activities cannot be performed – this would contemplate activities that enable a scammer to quickly transfer out large sums of monies to a third party without triggering transaction notification alerts to a consumer. MAS stated that such activities would include (but not be limited to): (i) addition of new payees to the consumer's account; (ii) increasing transaction limits; (iii) disabling transaction notification alerts; and (iv) changes in contact information, specifically mobile number, email address and mailing address.

- **Notification for activation of tokens and high-risk activities** – Provide consumers with notification alerts on a real-time basis for the activation of digital security tokens and conduct of high-risk activities.

- **Notification for outgoing transactions** – Provide consumers with notification alerts for outgoing transactions on a real-time basis.

- **Reporting channel and kill-switch** – Provide a 24/7 reporting channel and self-service feature for consumers to report and block unauthorised access to their accounts.

Duties of Telcos

The SRF also sets out the duties of responsible Telcos, which are a specific subset of IMDA's directions to telcos under Section 31 of the Telecommunications Act 1999. The duties are as follows:

- **Connecting to authorised aggregators** – Connect only to authorised aggregators for delivery of Sender ID SMS to ensure these SMS originate from bona fide senders registered with the SMS Sender ID Registry.

- **Blocking SMS** – Block Sender ID SMS which are not from authorised aggregators to prevent delivery of Sender ID SMS originating from unauthorised SMS networks.

- **Anti-scam filter** – Implement an anti-scam filter over all SMS to block SMS with known phishing links.

Operational workflow for handling claims

The proposed SRF sets out the following four-stage workflow for handling consumer claims in respect of losses arising from covered phishing scams:

- **Claim Stage** – A responsible FI will be the first and overall point of contact with the consumer. It will assess if the claim falls within the SRF's scope, and inform a responsible Telco where applicable.

- **Investigation Stage** – A responsible FI, and responsible Telco where applicable, should conduct the investigation in a fair and timely manner. They should ensure, through appropriate governance structures, that there are independent processes for investigating consumer claims.

- **Outcome Stage** – A responsible FI should inform and explain the investigation outcome to the consumer.

- **Recourse Stage** – Where a consumer is dissatisfied with the outcome, they may pursue further action through avenues of recourse such as the FIDReC or IMDA. As currently only full banks are required to be members of FIDReC, MAS proposes to additionally require major payment institutions that provide account issuance services for payment accounts that store e-money to join FIDReC.

Consultation Paper on Enhancements to EUPG

The EUPG, introduced in 2018, underscores the importance of collective efforts by responsible FIs[2] and consumers to mitigate the risk of unauthorised transactions. MAS is proposing enhancements to the EUPG targeted at unauthorised transactions arising from prevalent scam typologies in Singapore, such as phishing and malware-enabled scams.

The proposed enhancements: (i) align industry practice across responsible FIs by including in the EUPG the suite of anti-scam measures announced by MAS and the Association of Banks in Singapore on 19 January 2022 and 2 June 2022; (ii) further enhance the duties of responsible FIs to facilitate the prompt detection of scams by consumers and a fairer dispute resolution process; and (iii) enhance the duties of consumers to take necessary precautions against scams.

Key aspects of the proposed enhancements, including where a FI's duty under the proposed SRF is drawn from a EUPG measure, are summarised in the table below.

Enhancements to align industry practice across responsible FIs	**Further enhancements to the duties of responsible FIs**	**Enhancements to consumers' duties**
Preventive measures		
		Cyber hygiene practices - Consumers should, among others, only download the FI's mobile application from official sources for Singapore users and use strong authentication methods.
Sending clickable links and phone numbers - Do not send clickable links/phone numbers unless the consumer is expecting it, the link does		**Clickable links and phone number** - Consumers should not click on links in SMS or emails, unless these are informational links that they

[2] Responsible FIs refers to all banks, finance companies, non-bank credit card issuers and relevant payment service providers issuing e-wallets, which provide accounts to individuals or sole proprietors.

Enhancements to align industry practice across responsible FIs	Further enhancements to the duties of responsible FIs	Enhancements to consumers' duties
not require the consumer to perform a transaction and it does not lead to a platform that requires the downloading of applications.		are expecting to receive from the FI.
Measures prior to performing high-risk activities - Require further authentication from consumers and have pop-up risk-warning messages.		**Measures prior to performing high-risk activities** - Read the pop-up risk warning messages sent by the FI and check that the action was intended.
		Measures prior to authenticating transactions - Read the FI's messages containing the authorisation access codes and ensure the stated recipient is the intended recipient.
Cooling off period - Impose a minimum 12-hour cooling off period after activation of a digital security token, where high-risk activities cannot be performed. Send a notification alert to the consumer's registered contact. Also applicable under the proposed SRF.		
Detective measures		
	Information to enable consumers to validate their intended recipient - Access codes should be accompanied with sufficient information to enable the consumer to confirm	

Enhancements to align industry practice across responsible FIs	Further enhancements to the duties of responsible FIs	Enhancements to consumers' duties
	the validity of the transaction before authenticating it.	
Outgoing transaction notification alerts - Send consumers transaction notifications on a real-time basis for all outgoing transactions, in accordance with the transaction notification threshold. Also applicable under the proposed SRF.		
	Notification alerts when high-risk activities are performed - Send consumers notifications to alert them to any high-risk activities being performed. Also applicable under the proposed SRF.	
Remedial measures		
		Reporting unauthorised activities - Report any unauthorised account activity to the FI as soon as practicable, and no later than 30 calendar days after receipt of a notification alert.
Self-service feature - Provide consumers with a kill switch that is available through a channel other than the FI's mobile or internet banking channels. Also applicable under the proposed SRF.		**Activating kill switch** - Activate the kill switch as soon as practicable after notification of any unauthorised transaction or they have reason to believe their account is compromised.

Enhancements to align industry practice across responsible FIs	Further enhancements to the duties of responsible FIs	Enhancements to consumers' duties
24/7 reporting channel - Have a reporting channel that is always available for consumers. Also applicable under the proposed SRF.		
		Lodging police reports - Also make a police report if they suspect a scam or fraud, cooperate with the Police and furnish the police report to the FI within three calendar days of notifying the FI of such transaction.
Measures to ensure a fair dispute resolution process		
	Expectations of responsible FIs' dispute resolution process - FIs should provide channels for consumers to raise a disputed investigation, promptly assess and investigate the matter within 21 business days, or 45 business days where there are exceptional circumstances, of receipt of the disputed investigation and provide a report of the outcome to the consumer.	
	Charges relating to disputed unauthorised transactions - During the investigation period the FI should withhold/waive any outstanding amount and charges directly relating to the disputed transaction.	

Enhancements to align industry practice across responsible FIs	Further enhancements to the duties of responsible FIs	Enhancements to consumers' duties
	Withholding and/or waiving of outstanding charges and reporting to licensed credit bureaus - If the consumer disagrees with the FI's assessment, the FI should further withhold/waive outstanding charges for 30 calendar days. If the consumer approaches the FIDReC, the FI should withhold/waive outstanding charges until FIDReC completes the adjudication or closes the case. During this period, the FI should ensure that the consumer's credit records with licensed credit bureaus are not adversely affected due to the disputed transaction.	

MAS also proposes to introduce guidelines in the EUPG to cater for the scenario where the unintended recipient of a mistaken transfer of funds is the one who requests for the funds to be returned. These are intended to be consistent, to the extent possible, with the existing timelines in the scenario where the sender requests for the funds to be returned.

Concluding Words

The consultations papers on the proposed SRF and the enhancements to the EUPG signal a clear effort on the part of regulators to protect consumers from phishing scams and to provide greater clarity on the responsibilities of the parties involved.

Industry stakeholders are invited to assess the practicalities and issues that may arise in ensuring compliance with the prescribed responsibilities, as well as the other aspects of the proposed frameworks, such as the waterfall approach to liability and the operational workflow under the SRF. Parties may wish to respond to the consultations so as to ensure that their concerns are taken into account before the finalisation of the framework/enhancements.

Technology, Media & Telecommunications | Financial Institutions

Should you wish to provide your responses or discuss concerns, you may contact our team at Rajah & Tann, who are well placed across the relevant areas of practice to assist in this regard.

Further Information

Please click on the following links for further information on the proposed SRF (available on the MAS website at www.mas.gov.sg):

- Press release titled "MAS and IMDA Consult on Shared Responsibility Framework for Phishing Scams"
- Consultation paper on proposed SRF
- Draft guidelines on proposed SRF

Please click on the following links for further information on the proposed enhancements to the EUPG (available on the MAS website at http://www.mas.gov.sg/):

- Consultation Paper on Proposed Enhancements to the E-Payments User Protection Guidelines
- Annex A Draft Revised E-Payments User Protection Guidelines

Contacts

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.

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.

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

Our Regional Contacts

R&T SOK & HENG | *Cambodia*
R&T 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

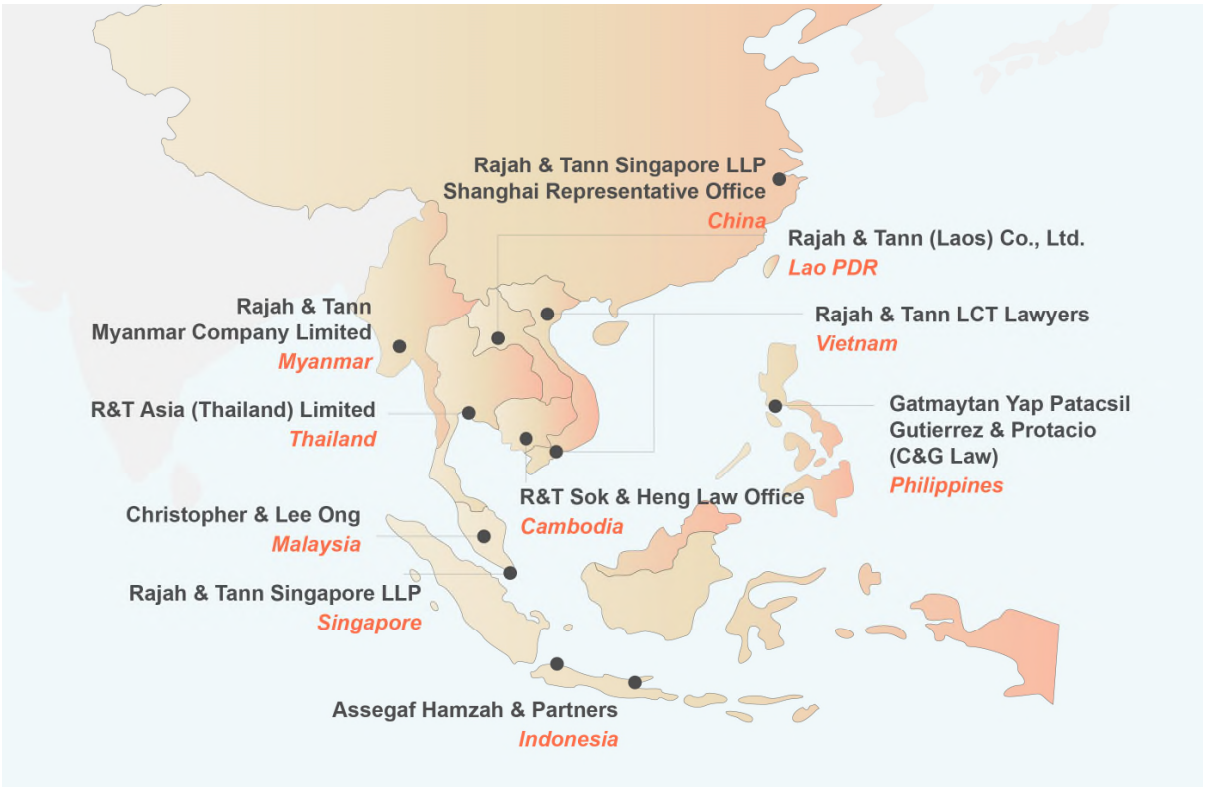
RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

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.