LEGAL ALERT

26 June 2024

How Are Digital Scams Being Addressed?

Earlier this year, it was reported that victims of online scams have collectively lost up to a total of RM3.2 billion between 2020 and 2023 in Malaysia[1]. Common types of digital scams currently include phishing, formjacking, identity theft, fake anti-virus software and malware. In an effort to curb such scams, our former finance minister had this month[2] called for a law holding financial institutions and telecommunication companies (telcos) partially liable for financial losses resulting from digital scams to be introduced in Malaysia.

As at today, victims of scams in Malaysia may seek existing avenues of recourse by commencing a civil action or reporting the matter to the relevant authorities, depending on the nature of scam. For instance:-

- victims of cyber scams can resort to the Malaysian Communications and Multimedia Commission (MCMC);
- victims of consumer-related scams may report to the Ministry of Domestic Trade and Consumer Affairs; and
- victims of financial scams can turn to Bank Negara Malaysia.

In this regard, Singapore may be a step ahead of the curve in Asia. The Monetary Authority of Singapore (MAS) and Infocomm Media Development Authority had late last year published a joint consultation paper proposing a SRF for phishing scams. The SRF focuses on phishing scams as they are a common and known scam type that result in unauthorised transactions in Singapore, and clear duties can be set for ecosystem players to safeguard against phishing risk[3]. Under

Contact Information:

Datin Jeyanthini Kannaperan
Consultant
jeyanthini@rajasekaran.co

Annabel Kok Keng Yen
Partner
+6012 905 1082
annabel@rajasekaran.co

[1] *https://www.thestar.com.my/news/nation/2024/03/04/rm23bil-lost-to-online-scams-from-2020-to-2023-says-kulasegaran#:~:text=KUALA%20LUMPUR%3A%20A%20total%20of,Kulasegaran.*

[2] *https://www.freemalaysiatoday.com/category/nation/2024/06/04/make-banks-telcos-share-responsibility-for-scam-losses-says-guan-eng/, https://www.msn.com/en-my/news/national/make-banks-telcos-share-responsibility-for-scam-losses-says-guan-eng/ar-BB1nBvqe*

[3] *The SRF is designed to cover phishing scams with a digital nexus, where a consumer is deceived into clicking on a phishing link and entering his credentials on a fake digital platform thereby unknowingly revealing these credentials to the scammer. With the*

Rajasekaran
Unit 27-13A, Menara Q Sentral,
No 2A, Jalan Stesen Sentral 2,
Kuala Lumpur Sentral,
50470 Kuala Lumpur.

T +603-2707 5757 (General)
+603-2707 5758 (Direct)
E info@rajasekaran.co
W www.rajasekaran.co

Singapore's proposed "shared responsibility framework" (SRF), financial institutions and telcos are to provide payouts to scam victims for a defined set of scams in cases where specific anti-scam duties are breached. Such framework is aimed at strengthening the overall resilience of Singapore's digital landscape against the threats posed by cybercriminals.

The following scams are excluded from the proposed SRF:-

- Scams where victims authorize payments to the scammer, e.g. payments arising from investment or love scams;
- Scams where a consumer was deceived into giving away his credentials to the scammer directly via text messages, and non-digital means;
- Unauthorised transaction scam variants that do not involve phishing, e.g. hacking, identity theft, and malware-enabled variants; and
- Malware scams.

The proposed SRF was intended to be implemented via a set of guidelines which will assign financial institutions and telcos relevant duties to mitigate phishing scams, and requires payouts to affected scam victims where duties are breached. Measures under the proposed SRF in Singapore include banks sending outgoing transaction alerts to customers, telcos implementing scam filters for SMS and strictly maintaining standards of anti-scam controls.

Under Singapore's proposed SRF, a "waterfall" approach[4] was to be adopted for sharing of responsibility, in that:-

- The responsible financial institution is placed first in line and is expected to bear the full losses if any of its duties have been

stolen credentials, the scammer performs unauthorised transactions from the consumer's account. (https://www.mas.gov.sg/publications/consultations/2023/consultation-paper-on-proposed-shared-responsibility-framework).

[4] https://www.mas.gov.sg/-/media/mas-media-library/publications/consultations/pd/2023/srf/consultation-paper-on-proposed-shared-responsibility-framework.pdf

Rajasekaran

breached. This recognizes the primary accountability that financial institutions owe to consumers as custodians of their money.

- If the financial institution has fulfilled all of its duties under the SRF, and the telco is assessed to have breached its SRF duties, the telco is expected to bear the full losses. Telcos' placement in the "waterfall" approach is commensurate with their secondary and supporting role (relative to financial institutions) as an infrastructure provider for the SMS mode of communication.
- If both the financial institution and telco have carried out their SRF duties, the consumer bears the full scam losses. However, the consumer may still pursue further remedies through existing avenues of recourse, such as through the Financial Industry Disputes Resolution Center (FIDReC).

Aside from the SRF guidelines, MAS had proposed enhancements to its E-Payments User Protection Guidelines (EUPG). The EUPG deals with unauthorized and erroneous transations (and not just phishing scams), setting out the responsibilities of financial institutions and consumers, and their liability for losses. The proposed enhancements to the EUPG would cover added responsibilities of (i) financial institutions with regard to anti-scam measures in relation to phishing and malware-enabled scams; and (ii) consumers to take necessary precautions. As at the date of this alert, it is expected that the SRF will be rolled out in Singapore sometime in 2024 although there has been no further media reports on progress.

In Australia, its government had introduced the Scam-Safe Accord[5], a concerted initiative led by the Australian Banking Association (ABA) and the Customer Owned Banking Association (COBA). The Accord includes six priority initiatives in a bid to make banking safer for Australian consumers which include: advanced name-checking technology, biometric checks, and intelligent threat-sharing mechanisms. These countermeasures aim to detect suspicious activities more effectively, disrupt scam operations and block the flow of funds into high-risk

[5] *https://ministers.treasury.gov.au/ministers/stephen-jones-2022/media-releases/government-welcomes-scam-safe-accord*

Rajasekaran

channels[6]. This Accord demonstrates commitment from Australia's financial institutions, including community-owned banks, building societies, credit unions, and commercial banks, to elevate the standard of customer protection and effectively counter scams. At the same time, the Australian government is working on tough new industry codes for banks, telcos and digital platforms, which will set clear, robust obligations to protect Australians from scams which is targeted to sit alongside the work on cybersecurity and information privacy. However, it is pertinent to note that as at the date of this alert, the current codes applicable in Australia do not cover a liability shift from consumers to financial institutions and telcos, as in the case of the SRF in Singapore, despite recent calls by consumer groups and community legal centres to do so[7].

Over in the United Kingdom, a mandatory reimbursement requirement for authorized push payment (APP)[8] fraud has been introduced, with such rules requiring UK payment service providers to reimburse all in-scope customers who fall victim to APP fraud, save for limited exceptions[9]. In this respect, all UK Payment Service Providers will be required to reimburse[10] their customers for APP fraud losses, but there will be a 'standard of consumer caution' applied which could see reimbursement claims denied. Under this standard, customers might not be reimbursed if the financial provider can demonstrate the customer hasn't been careful or cooperative enough. Hence, customers would need to pay attention to warnings about suspected APP fraud attempts

---

[6] https://securitybrief.com.au/story/australia-introduces-scam-safe-accord-to-combat-aud-3-1bn-scam-crisis
[7] https://www.bankingday.com/call-for-australian-scam-reimbursement-plan
[8]Authorised Push Payment (APP) fraud was discussed in detail in the recent United Kingdom (UK) Supreme Court decision in Philipp v Barclays Bank [2023]. APP fraud involves a fraudster posing as a customer's bank or third party to convince the customer to transfer monies to an account controlled by the fraudster. Provided the customer's account is in credit, the UK Supreme Court's view is that the ordinary duty of the bank when instructed by its customer to make a payment from the account is to carry out the instruction and make the payment. In making the payment, the bank must execute the transaction and do so promptly. The Court noted: "It is not for the bank to concern itself with the wisdom or risks of its customer's payment decisions" However, the Court has left open the prospect that the bank might still be liable for not acting promptly to recall the payments after being notified of the fraud (https://www.actons.co.uk/latest/2023/07/supreme-court-rules-in-favour-of-barclays-in-app-fraud-case/), (https://www.herbertsmithfreehills.com/insights/2023-07/payment-scams-implications-for-australian-banks-of-uk-supreme-court-judgment-on)
[9] https://www.lendingstandardsboard.org.uk/the-new-rules-for-authorised-push-payment-fraud-reimbursement-and-what-they-mean-for-scam-prevention/
[10] Ibid.

Rajasekaran

from their bank, notify their bank about the fraud in good time, share information about the fraud with their bank, and consent to fraud details being reported to the police. With regards to liability of financial institutions, the responsibility for reimbursement is shared between the originating bank and receiving bank in relation to the APP fraud. This is in contrast with the "waterfall approach" adopted by the SRF to be introduced in Singapore.

Similar regulatory developments in relation to addressing scams are being developed across various jurisdictions, and countries across Asia are likely to observe and learn from these solutions tailored to each unique financial ecosystems and consumer base.

Should a similar "shared responsibility framework" be adopted in Malaysia in relation to the accountability of financial institutions and telcos to consumers, it is pertinent for such framework to set out clearly the definition and scope of scams to be covered under such framework and the enforceability of such framework within the existing Malaysian legislative structure. Potential legal issues such as data protection issues and clear stages in the handling of claims process and dispute resolution process should also be considered. Further, the implementation of a "shared responsibility framework" in Malaysia may pose a set of challenges that span technological, operational, and regulatory domains. In this regard, financial institutions and telcos may face the need to overhaul existing technological systems to meet requirements imposed under such a framework.

Alert by Annabel Kok (Corporate Partner) of Messrs Rajasekaran.

The contents of this alert do not constitute legal advice nor an expression of legal opinion and should not be relied upon as such. If you require any further information, kindly contact annabel@rajasekaran.co.

Rajasekaran
Unit 27-13A, Menara Q Sentral,
No 2A, Jalan Stesen Sentral 2,
Kuala Lumpur Sentral,
50470 Kuala Lumpur.

T +603-2707 5757 (General)
+603-2707 5758 (Direct)
E info@rajasekaran.co
W www.rajasekaran.co