Monetary Authority of Singapore

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

Consultation Paper

P016-2023 – October 2023

Consultation Paper on Proposed Shared Responsibility Framework

Contents

1. Preface

1.1. The growth of digital payments and transactions has brought about efficiency and convenience to consumers. At the same time, however, digitally-enabled scams and the corresponding financial losses have risen globally, as scammers employ techniques of increasing sophistication to exploit victims for their own financial gain.

1.2. This consultation sets out a proposed Shared Responsibility Framework (SRF) for sharing responsibility for scam losses amongst financial institutions (FIs), telecommunication operators (Telcos) and consumers, for unauthorised transactions arising from phishing scams. FIs and Telcos will provide payouts to scam victims for a defined set of phishing scams, if specified anti-scam duties are breached. The SRF will provide a more expedient channel for consumer recourse once it is operationalised next year[1].

1.3. The Monetary Authority of Singapore (MAS) and Infocomm Media Development Authority (IMDA) are seeking comments from industry stakeholders and members of the public on the key areas of the framework which will be implemented via a set of Guidelines ("**SRF Guidelines**"), to be jointly issued by MAS and IMDA.

1.4. The SRF builds on MAS' E-Payments User Protection Guidelines (EUPG)[2]. MAS is concurrently seeking comments on proposed revisions to the EUPG, following a review of the EUPG by the Payments Council[3]. These are set out in a separate "Consultation Paper on Proposed Enhancements to the E-Payments User Protection Guidelines", published on 25 October 2023.

1.5. The next sections explain the key proposals for public consultation. The draft version of the SRF Guidelines has been published together with this consultation paper on MAS' and IMDA's website.

1.6. **Please note that all submissions received will be published and attributed to the respective respondents unless they expressly request MAS and IMDA not to do so. As such, if respondents would like –**

[1] Scam cases that occur after the operational launch of the SRF and meet the defined scope will be eligible to be considered for the SRF.

[2] MAS issued the EUPG in 2018 to foster public confidence in using electronic payments (e-payments), by setting out responsibilities and liabilities of consumers and responsible FIs (specifically, banks, non-bank credit card issuers, finance companies, and relevant payment service providers as defined in the EUPG) in relation to unauthorised and erroneous payment transactions.

[3] MAS announced in February 2022 that the Payments Council, chaired by MAS, had been working on a review of the EUPG and the loss sharing approach since July 2021. The industry workstream is co-chaired by Grab and OCBC. Other members of the workstream are from Citibank, DBS, Mastercard, NETS, Paypal, Standard Chartered Bank, UOB, Visa, and Association of Small & Medium Enterprises. The Association of Banks in Singapore and the Singapore Fintech Association are observers of the workstream.

(a) **their whole submission or part of it (but not their identity), or**

(b) **their identity along with their whole submission,**

to be kept confidential, please expressly state so in the submission to MAS and IMDA. MAS and IMDA will only publish non-anonymous submissions. In addition, MAS and IMDA reserve the right not to publish any submission received where MAS and IMDA consider it not in the public interest to do so, such as where the submission appears to be libellous or offensive.

1.7. Please submit written comments through the link below by 20 December 2023:

https://go.gov.sg/srfconsultation2023

2. Introduction

2.1. Scams remain a global challenge as perpetrators continue to exploit vulnerabilities across multiple platforms and sectors. Cases seen in Singapore include the phishing scams impersonating Oversea-Chinese Banking Corporation Limited (OCBC) in late 2021, and the more recent malware scam series[4] that has gained prominence.

2.2. The Government, banks and other ecosystem players have progressively implemented a suite of anti-scam measures to tackle scams in Singapore. Working together with industry stakeholders, the Government takes a multi-layered approach against scams:

(a) Blocking scammers' approach: To protect users from known scam numbers and filter out potential scam Short Message Services (SMS), the Smart Nation and Digital Government Group has developed the ScamShield app. IMDA has implemented the Singapore SMS Sender ID Registry (SSIR) to address the issue of Sender ID spoofing in SMS.

(b) Securing government and banking channels: To secure government and banking channels, all Government agencies have been onboarded onto the SSIR, making Government agencies harder to spoof. MAS also works with the Association of Banks in Singapore (ABS) to implement digital banking safeguard measures.

(c) Strengthening enforcement: The Anti-Scam Command was formed in 2022 to consolidate expertise in combatting scams. The Singapore Police Force (SPF) also works closely with their foreign counterparts to exchange information and conduct joint operations, to address the transnational nature of scams. Legislative levers have also been strengthened, with the passing of the Online Criminal Harms Act, which will allow for anti-scam measures to be prescribed for specified online platforms.

2.3. The Government recognises that responsibility for preventing scams should not lie solely with consumers but also with industry stakeholders such as FIs and Telcos. As part of the overall suite of anti-scam measures, the SRF will be implemented with the following **three key policy objectives**:

(i) To preserve confidence in digital payments and digital banking in Singapore

2.4. Left unaddressed, scam threats and the ensuing losses can undermine public confidence in digital banking and digital payments, particularly where account credentials are divulged through digitally-enabled means of deceit leading to unauthorised transactions being performed digitally without the consumer's knowledge or consent. The SRF will operate alongside other measures in the broader scheme of industry-wide anti-scam efforts to safeguard consumer interests when they

[4] Refer to Section 4 on "Types of Scams" covered under the SRF.

transact via digital banking or digital payments. It sets out clear anti-scam duties for FIs and Telcos to address phishing scams.

(ii) To strengthen relevant entities' direct accountability to consumers on losses incurred from digital scams

2.5. FIs and Telcos involved in the digital banking and digital payments ecosystem are answerable to regulators if they fail to implement the necessary anti-scam measures. However, there is currently no framework for entities to be directly accountable to consumers who have suffered scam losses due to lapses by the said entities. The SRF complements the existing responsibilities that FIs or Telcos owe to regulators, by setting the Government's expectation that the FI or Telco should bear responsibility for scam losses ahead of consumers if the FI or Telco fails to meet a prescribed set of anti-scam duties.

(iii) To emphasise individuals' responsibility to be vigilant against scams

2.6. A discerning and vigilant public remains the first line of defence against scams. Individuals have a responsibility to mitigate the occurrence of scams by practising proper cyber hygiene and not giving away their credentials to a third party under any circumstance. The SRF aims to provide a clear framework for the sharing of responsibility for scam losses among relevant stakeholders for common and known scam typologies where duties of respective stakeholders are more well-defined.

3. Entities Covered under the SRF

3.1. The SRF is expected to apply to all full banks and relevant payment service providers[5] (hereafter, "**responsible FIs**")[6] and Telcos which are mobile network operators (hereafter, "**responsible Telcos**")[7].

3.2. FIs, in particular retail banks and payment service providers providing e-wallet services, are custodians of consumers' money. These entities therefore play a critical role as gatekeepers against outflow of monies arising from scams. Accordingly, they have primary responsibility to implement robust controls to safeguard consumers' accounts and to effectively respond to suspicious transactions.

3.3. Telcos facilitate the sending of SMS, which are often used by businesses, including FIs, as an official communication channel and as a means of sending authorisation access codes such as SMS one-time passwords (OTPs). However, scammers have attempted to impersonate FIs and other businesses via the SMS channel. As an infrastructural player, Telcos therefore play a supporting role in fostering the security of digital banking and digital payments, by implementing scam disruption measures within the SMS communications networks that reduce the risks of scam SMS being delivered to consumers.

3.4. Responsible FIs and Telcos have been working with MAS and IMDA respectively to devise and implement anti-scam measures on an ongoing basis. As such, these entities are well-positioned to work with MAS and IMDA to commence the SRF.

[5] "Relevant payment service provider" refers to major payment institutions providing account issuance services where the payment accounts issued can store e-money.

[6] Major retail banks – DBS, OCBC, UOB, Citibank, and Standard Chartered Bank – and major payment institutions providing e-wallet services (e.g., Grab) have agreed to participate in the SRF.

[7] These responsible Telcos refer to Mobile Network Operators (MNOs) in Singapore. MNOs deploy, own or control wireless network infrastructure and have been given the right to use radio spectrum, to provide telecommunication services to end users. There are currently four MNOs, namely Singtel, StarHub, M1 and SIMBA.

4. Types of Scams Covered

4.1. 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[8], thereby unknowingly revealing these credentials to the scammer. With the stolen credentials, the scammer performs unauthorised transactions from the consumer's account. 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.

4.2. Such phishing scams should also have a clear Singapore nexus. The impersonated entities should be Singapore based, or based overseas and offer their services to Singapore residents. Consumers should be vigilant and check that the digital platforms they interact with are plausibly legitimate. Confining the SRF's scope to digitally-enabled scams with a clear Singapore nexus is in line with the policy objective of preserving confidence in digital payments and digital banking in Singapore.

4.3. Examples of phishing scams in scope include those where a scammer pretends to be from an entity (e.g., SingPost, DHL) and sends spoofed emails or SMS claiming account-related issues to trick the victim into clicking a uniform resource locator (URL) link to a fake website where he enters his account credentials, or where a scammer pretends to be an FI staff and uses enticements of attractive deals purportedly offered by the FI (e.g., high interest rate fixed deposit, free handphone with deposit) to trick the victim into clicking a URL link to a fake FI website to enter his account credentials.

4.4. However, the SRF will exclude:

(a) Scams where victims authorise payments to the scammer, e.g., payments arising from investment scams or love scams (authorised scams) which victims intended to be performed at the point of the transaction. Such authorised scams will require a different approach, as the victim intended to make the funds transfer but had been deceived as to the underlying premise for the payment. Such authorised scams also do not fundamentally affect confidence in digital payments or digital banking, as they can equally happen in the non-digital world.

(b) Scams where a consumer was deceived into giving away his credentials to the scammer directly via text messages, and non-digital means (i.e., phone calls or face-to-face). This takes into account years of public education to sensitise consumers to the fact that they should never reveal their credentials or OTP directly to anyone under any circumstances.

(c) Unauthorised transaction scam variants that do not involve phishing (e.g., hacking, identity theft, malware-enabled variants).

[8] This refers to a fake digital platform that resembles the legitimate digital platform operated by an FI or other impersonated entity, or any party related to the FI or impersonated entity.

4.5. Malware scams, which are a rising concern, are not covered under the SRF. The SRF is intended to apply to common and known scam typologies for which duties of respective stakeholders are more well-defined. It is premature to set out specific malware scam-related duties for different stakeholders at this stage as these measures are still developing and will evolve significantly given the nature of malware scams. As further elaborated in section 8, Government agencies and banks are nonetheless working closely to tackle malware scams and banks have announced that they will take a more forward-leaning approach towards assessing goodwill payments for customers affected by malware scams.

4.6. For scams that are not in scope, existing avenues of recourse remain open to consumers, including requesting their FIs to assess their case for goodwill payments, or filing a dispute with the Financial Industry Disputes Resolution Centre Ltd (FIDReC).[9]

Question 1. *MAS and IMDA seek comments on the scope of the SRF in sections 3 and 4.*

[9] FIDReC is an independent and impartial institution that resolves consumer financial disputes through mediation and adjudication. Its services are available to consumers who are either individuals or sole proprietors for claims against licensed FIs. It offers an alternative for consumers to have their disputes heard in accessible and affordable manner, instead of going to court.

5. Duties of Responsible FIs and Responsible Telcos

Criteria for SRF Duties

5.1. The SRF will set out specific anti-scam duties for FIs and Telcos. Failure to fulfil any of the relevant duties will render the FI or Telco responsible to make payouts to consumers for their scam losses.

5.2. The anti-scam duties were formulated based on the following principles:

(a) The duty has a role towards disrupting phishing scams defined in Section 4 (hereafter, "**covered phishing scams**").

(b) The duty is discrete (i.e., "yes" or "no"), objective, and verifiable.

(c) The duty aids consumers in reacting promptly to covered phishing scams encountered.

Duties of Responsible FIs

5.3. The duties prescribed for responsible FIs are intended to ensure that crucial communication channels are in place to keep consumers informed when transactions or high-risk activities[10] are performed on their account, as well as safeguards to mitigate consumers' exposure to scam losses when their accounts are compromised.

FI Duty #1: Impose a 12-hour cooling off period upon activation of digital security token during which 'high-risk' activities cannot be performed

5.4. A scammer who successfully phishes the consumer's credentials and activates a digital security token on a separate device, can take over the consumer's account and perform unauthorised transactions. As such, a 12-hour cooling period where no 'high-risk activities' can be performed adds friction and increases the chance consumers can discover unusual activities on their account.

[10] 'High-risk' activities enable a scammer to quickly transfer out large sum of monies to a third party without triggering transaction notification alerts to a consumer. Such activities include (a) addition of new payees to the consumer's account, (b) increasing transaction limits, (c) disabling transaction notification alerts and (d) changes in contact information, specifically mobile number, email address and mailing address. This list represents a baseline set of high-risk activities; responsible FIs may assess and include other activities to be in the 'high-risk' category.

FI Duty #2: Provide notification alert(s) on a real-time basis for the activation of digital security token and conduct of high-risk activities

5.5. Providing such notification alerts on a real-time basis will help alert consumers to high-risk activity that may not have been authorised. Collectively, the 12-hour cooling off period and the notification alerts give consumers some time to react and take preventive action if the activation request was not intended by the consumer.

FI Duty #3: Provide outgoing transaction notification alert(s)[11] on a real-time basis

5.6. Real-time outgoing transaction notifications are essential in prompting consumers to react when there are unauthorised transactions (e.g., immediately reporting to the FI), and enables the responsible FI to take timely remedial action.

FI Duty #4: Provide a (24/7) reporting channel and self-service feature ("kill switch") to report and block unauthorised access to their accounts

5.7. A reporting channel complements FI Duties #1 to #3 above by allowing consumers to reach out to their FI to block a scammer from making unauthorised transactions on their account. FIs should also provide a kill switch that consumers can self-activate to immediately block their account and prevent further unauthorised transactions.

Duties of Responsible Telcos

5.8. Responsible Telcos' duties directly support the responsible FIs' duties by implementing scam disruption measures within the SMS channel to reduce the risks of scam SMS being delivered to consumers. These duties reflect the Telcos' supporting role as infrastructure providers for the SMS mode of communication.

5.9. To safeguard consumers against scam SMS, IMDA has adopted a multi-layered approach to combat scams[12], including with the SMS Sender ID Registry (SSIR) regime and anti-scam filter:

[11] Outgoing transaction notifications must be sent in line with the default industry-baseline notification thresholds or notification threshold selected by the consumer.
[12] See **Annex C** for a detailed list of the anti-scam measures implemented at the telecommunications channels.

(a) Under the SSIR, all organisations that wish to send SMS messages with alphanumeric Sender IDs ("**Sender ID SMS**") to Singapore mobile users must register with the SSIR. Only Sender ID SMS with registered Sender IDs will reach Singapore users with the registered Sender ID. All Sender ID SMS with non-registered Sender IDs will be tagged as "Likely-SCAM". Organisations sending Sender ID SMS must send their SMS through SMS aggregators that are licensed by IMDA and registered with the SSIR to handle these Sender ID SMS to be sent ("**authorised aggregators**").

(b) IMDA has required Telcos to implement anti-scam filters over SMS messages by applying commercial technology solutions. Such technology can filter scam SMS messages using automated machine scanning, based on parameters including (i) SMS messages containing malicious links to phishing websites and (ii) SMS messages containing keywords or phrases indicative of scam SMS message.

5.10. Three duties for Telcos under the SRF are set out below. These duties are a specific subset of IMDA's issued directions to Telcos under section 31 of the Telecommunications Act ("**Directions**") and assessed to be core to Telcos' role in safeguarding their subscribers against phishing scams over the SMS channels. These duties (i) facilitate onward delivery of SMS from verified businesses, and (ii) disrupt the delivery of SMS determined to be a scam.

Telco Duty #1: Connect only to authorised aggregators for delivery of Sender ID SMS to ensure these SMS originate from bona fide senders registered with the SSIR

5.11. This duty requires a responsible Telco to deliver Sender ID SMS to subscribers only if it originates from authorised aggregators[13]. Such SMS would have gone through checks to ensure that they originate from senders registered with the SSIR and who are authorised to use the Sender ID. This reduces the risk of subscribers receiving SMS with a spoofed SMS Sender ID.

Telco Duty #2: Block Sender ID SMS which are not from authorised aggregators to prevent delivery of Sender ID SMS originating from unauthorised SMS networks

5.12. This duty requires a responsible Telco to block Sender ID SMS which are received from sources other than authorised aggregators to prevent consumers from receiving Sender ID SMS from all other channels, including unauthorised or unknown networks connected through overseas network operators. This further closes off any potential risks of Sender ID spoofing.

[13] These are SMS aggregators that are licensed by IMDA and registered under the SMS Sender ID Registry Scheme for Singapore.

Telco Duty #3: Implement an anti-scam filter over all SMS to block SMS with known phishing links

5.13. This duty requires a responsible Telco to implement an anti-scam filter for all SMS that pass through the MNOs' network, where the SMS will be scanned to determine if it contains any URL that matches that of a known malicious URL. The anti-scam filter is required to be implemented for all SMS that originate locally or from overseas. The requirement covers both Sender ID SMS and SMS carrying telephone numbers (e.g., local +65 9 numbers). This duty further mitigates against the risks of scam SMS that may pass through mobile networks in Singapore.

Question 2. *MAS and IMDA invite comments on the duties of responsible FIs and responsible Telcos under the SRF.*

6. Waterfall Approach under the SRF

How responsibility will be shared for phishing scams

6.1. The assessment of how responsibility will be shared for the losses[14] arising from an unauthorised transaction in a covered phishing scam will be based on a "waterfall" approach.

(a) The responsible FI is placed first in line and is expected to bear the full losses if any of its duties have been breached.[15] This recognises the primary accountability that FIs owe to consumers as custodians of their money.

(b) If the FI has fulfilled all its SRF duties 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 Fis) as an infrastructure provider for the SMS mode of communication.

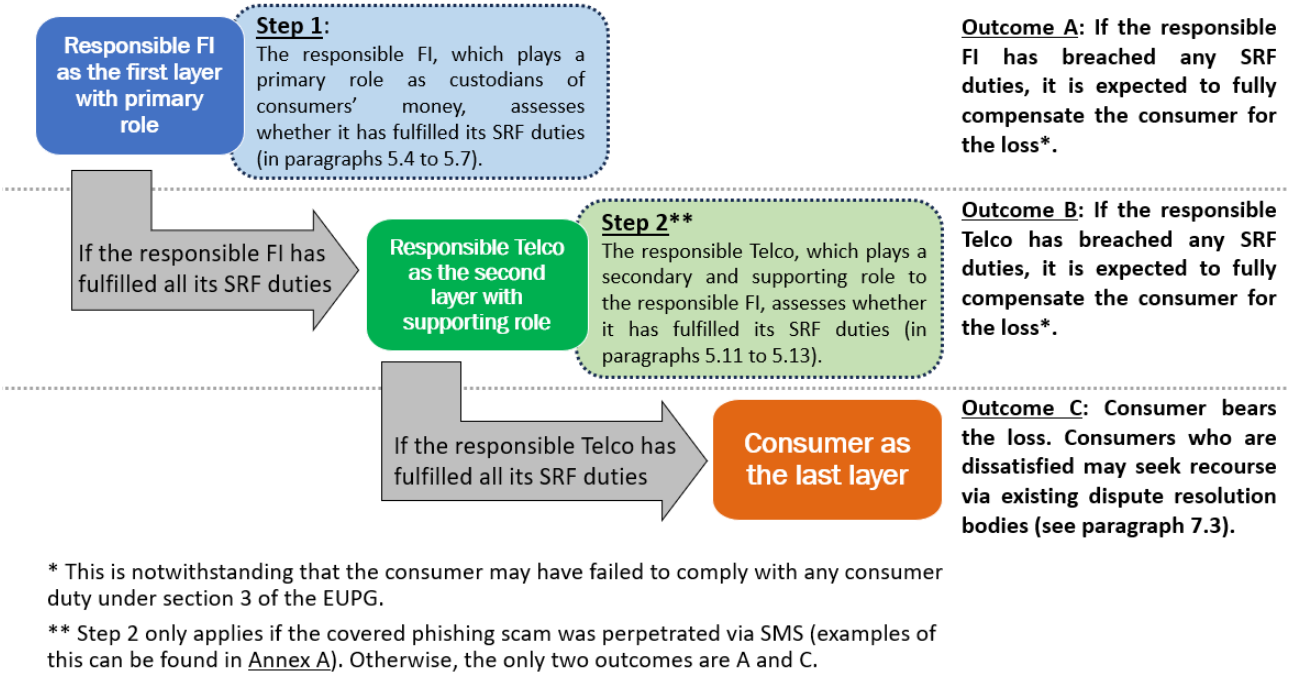
(c) If both the FI and Telco have carried out their SRF duties, the consumer bears the full losses. Nevertheless, consumers may still pursue further action through existing avenues of recourse, such as through FIDReC.

6.2. The "waterfall" approach is intended as a practical means for more straightforward assessment of how responsibility will be shared for covered phishing scams. Importantly, it incentivises all parties to stay vigilant and perform their roles to uphold the safety of e-payments. **Diagram 1** below illustrates the "waterfall" approach.

[14] Holders of credit cards, charge cards and debit cards issued in Singapore currently benefit from liability apportionment in the ABS Code of Practice for Banks – Credit Cards, and existing fraud prevention measures in place. As such, the liability apportionment does not apply to transactions on credit cards, charge cards and debit cards issued in Singapore.

[15] Any contractual agreements between responsible FIs and consumers should not serve to limit consumers' ability to claim payouts from the SRF or seek redress via alternative avenues of dispute resolution.

Diagram 1: The "Waterfall" Approach



* This is notwithstanding that the consumer may have failed to comply with any consumer duty under section 3 of the EUPG.

** Step 2 only applies if the covered phishing scam was perpetrated via SMS (examples of this can be found in Annex A). Otherwise, the only two outcomes are A and C.

6.3. Please refer to **Annex A** for case studies on how SRF duties would be assessed and the corresponding losses to be apportioned.

Question 3. *MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility.*

7. Operational Workflow for Handling Claims

7.1. MAS and IMDA propose the following four-stage workflow for handling consumer claims in respect of losses arising from covered phishing scams. Responsible FIs and Telcos are expected to adhere to this workflow. Consumers who wish to bring a claim under the SRF should provide the necessary information to assist with investigations.

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

(b) **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.[16]

(c) **Outcome Stage** – a responsible FI should inform and explain the investigation outcome to the consumer.

(d) **Recourse Stage** – Where a consumer is dissatisfied with the outcome at the Outcome Stage, he may pursue further action through avenues of recourse such as the FIDReC or IMDA.

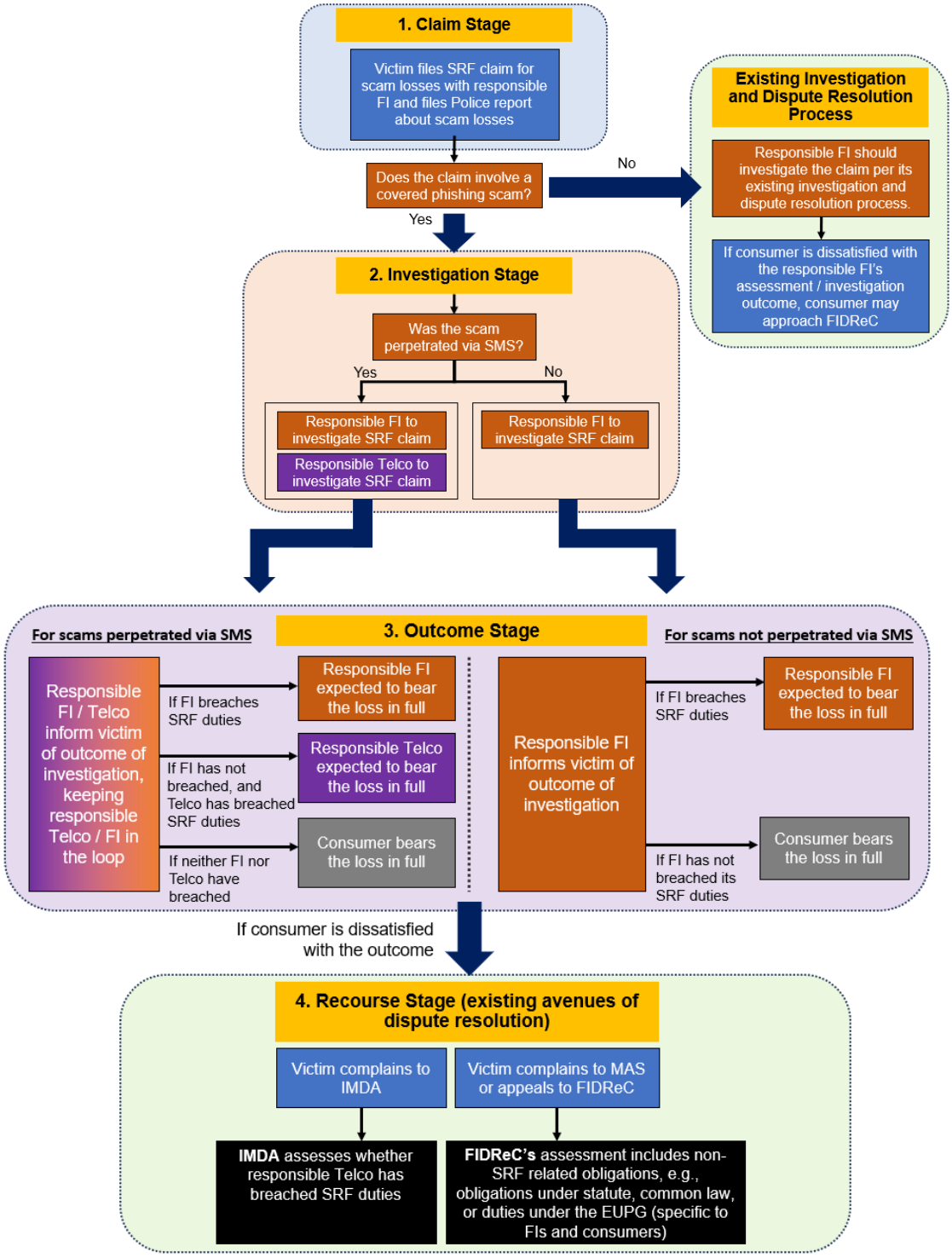
7.2. Throughout the four stages of the SRF claims process, MAS and IMDA propose for responsible FIs to be the primary touchpoint with the consumer. Responsible FIs may loop in responsible Telcos to communicate with the consumer only in specific situations (e.g., to address a Telco-specific query for an SRF claim), but this will be done within a single communication chain. This is to minimise the burden on consumers to liaise separately with the responsible FI and responsible Telco in times of distress.

7.3. A consumer may approach FIDReC (for further dispute resolution with the responsible FI), write to IMDA (if he or she disagrees with the responsible Telcos' assessment), or file a claim with the courts. While all full banks[17] are members of FIDReC, payment service providers are currently not. MAS' intent is to ensure that consumers of all responsible FIs can approach FIDReC in the event that they have suffered loss from scams (including covered phishing scams) and are dissatisfied with their responsible FI's assessment of responsibility for the scam loss, under the SRF or otherwise. As such, MAS proposes for major payment institutions (MPIs) providing account issuance services for payment accounts that store e-money ("e-wallets")[18], to join FIDReC.[19]

[16] A well-established and accepted practice for FIs' and Telcos' internal handling of claims is for the investigation to be conducted by representatives who are independent from business units.
[17] Full banks are licensed to carry out retail banking business.
[18] Examples include Grab, YouTrip, Revolut, PayPal, Wise, etc.
[19] This will be done via amendments to the Financial Services and Markets (Dispute Resolution Schemes) Regulations 2023.

7.4. Please see a summary of the operational workflow in the following **Diagram 2**. A more detailed explanation on the operational workflow can be found in **Annex B**.

Diagram 2: Operational Workflow for claims brought under the SRF



Question 4.	*MAS and IMDA seek comments on the proposed operational workflow (in paragraphs 7.1 to 7.4, Diagram 2, as well as in Annex B) for investigating claims under the SRF, including the information to be provided by parties involved, the timeline for completing investigations, and having the responsible FI as the primary touchpoint.*
Question 5.	*MAS seeks comments on the proposal for major payment institutions providing account issuance services, where the issued payment accounts can store e-money, to be members of FIDReC.*

8. An Evolving Approach to Combat Scams and Support Victims of Scams in Singapore

8.1. The SRF should be viewed in totality with other measures in the broader scheme of anti-scam efforts across the government and industry to preserve public confidence in digital banking and digital payments. As newer scam typologies surface in the digital payments system (e.g., the rise in malware-enabled scams[20] since start of 2023), the Government's overall framework for combatting scams will similarly need to evolve.

8.2. Alongside the SRF, the Government has worked extensively with relevant industry players on anti-scam efforts, including (i) the recent implementation of enhanced safeguards by banks to address malware scams[21], and (ii) banks' respective goodwill payouts to support victims of malware scams and other emerging scam types. These measures have mitigated the threat of malware scams.[22] The Government will continue to review and augment its anti-scam efforts to ensure that these measures remain relevant.

8.3. In designing the SRF, MAS and IMDA have studied the reimbursement frameworks for scam losses in other jurisdictions. Scam landscapes differ across jurisdictions, and would necessitate different approaches. The three areas of comparison are as follows.

(a) **Scam typologies**: The SRF's coverage of phishing scams is narrower than certain other jurisdictions that cover unauthorised transactions arising from all types of scams, such as in the United Kingdom (UK) and European Union (EU) member states. That said, phishing scams are a key category of unauthorised transactions in Singapore, and account for a sizeable proportion of unauthorised transactions. On the whole, Singapore's approach is still broadly consistent with most other jurisdictions where authorised transactions are not covered under the reimbursement model.

(b) **Coverage of entities:** The inclusion of Telcos will be a unique aspect of Singapore's SRF. Currently, no known jurisdictions have included telecommunication operators or other infrastructure service providers in their scam reimbursement frameworks. In placing duties on responsible

[20] Malware scams typically occur when a scammer deploys a sophisticated scheme to deceive consumers into installing malicious apps on their devices. These malicious apps subsequently allow scammers to remotely access the victim's device and steal sensitive information (including banking credentials and authentication codes) to perform unauthorised transactions on the victim's account.

[21] Refer to Channel News Asia, "DBS, UOB become latest banks to restrict access if unverified apps are found on customers' phones", 26 September 2023; and The Straits Times, "At least $2m in savings prevented from being stolen in malware attacks after OCBC app security update", 8 September 2023.

[22] Refer to ABS' media release "Banks in Singapore will do their part to protect customers against scams", 24 October 2023.

Telcos, the Singapore Government seeks to disrupt scammers' abuse of the SMS channel to send scam SMS, with the intent of reducing the risks of scam SMS being delivered to consumers.

(c) **Payout conditions**: The SRF is aimed at strengthening the direct accountability of responsible FIs and Telcos to consumers for losses incurred from digital scams. Accordingly, payouts for scam losses are premised on whether FIs and Telcos, rather than consumers, had fulfilled their duties.[23] Under the SRF, duties are well-defined and payout conditions are designed to ensure a straightforward process for allocating losses based on the "waterfall" approach. It therefore incentivises responsible FIs and Telcos to strictly uphold the desired standards of anti-scam controls.

8.4. The current development of the SRF around the more established phishing scam typology, as well as the "waterfall" approach to assessing payouts for scam losses, represents a starting point for the framework where two groups of key ecosystem players – FIs and Telcos – are held accountable. The Government intends to review and update this framework (e.g., coverage of scam types, participating players, duties of stakeholders, payout conditions), taking into account the practices and ongoing developments in other jurisdictions.

Question 6. *The Government welcomes comments on how the SRF should evolve taking into account the changing scams landscape.*

[23] Under the UK and EU models, consumers will be reimbursed unless the FI can prove that the consumer was grossly negligent or fraudulent.

9. List of Questions

10. Annex A – Application of SRF to Case Studies

	Details	Assessed under the SRF? (Yes/No)	Responsible FI breached SRF duties? (Yes/No)	Responsible Telco breached SRF duties? (Yes/No)	Outcome
Case Study 1 – Investment Scam	Consumer A decided to participate in an investment program offering lucrative returns via a Facebook advertisement. However, the 'investment program' was in fact being operated by a scammer. Consumer A clicked on the link in the Facebook advertisement and was given instructions to make fund transfers to the 'investment company' for 'investment'. Over a course of 5 days, Consumer A logged into his banking app and made 10 bank account transfers totaling $50,000 to the 'investment company' (i.e., the scammer). Real-time SMS transaction notifications were sent by the responsible FI for all the transactions, and there were no other lapses observed of the responsible FI. Months later, Consumer A realises that this was a scam after he was unable to contact the 'investment company' or withdraw the 'profits'.	No. These transactions made to the scammer were authorised by the consumer and therefore will not be assessed under the SRF.	N.A.	N.A.	**100% of the loss will be borne by the consumer.** The consumer may approach existing avenues of dispute resolution if he wishes to seek further recourse. However, losses are likely to still fall on the consumer as these are transactions which the consumer had knowledge of and/or intended to execute.

	Details	Assessed under the SRF? (Yes/No)	Responsible FI breached SRF duties? (Yes/No)	Responsible Telco breached SRF duties? (Yes/No)	Outcome
Case Study 2 – Phishing Scam where consumer gave away credentials *verbally* to scammer	Consumer B received a call from a scammer impersonating the local Police, claiming that the 'Police' needed to access his account to secure funds due to money laundering allegations. Consumer B revealed his account credentials and OTP directly to the 'Police' (i.e., scammer) over the phone. During the night, 9 unauthorised transactions were made from consumer's account, totaling $8,000.	No. Although this case involves a phishing scam, it does not fall within the scope of the SRF because it does not have a digital nexus. Consumer B had divulged his account credentials over the phone, rather than on a fake digital platform.	N.A.	N.A.	**100% of the loss will be borne by the consumer.** The consumer may approach existing avenues of dispute resolution if he wishes to seek further recourse.
Case Study 3 – Phishing Scam involving the impersonation of an unknown foreign entity	Consumer C received a WhatsApp message containing a clickable link from a scammer purporting to be a foreign seller of furniture. While the foreign 'furniture seller' was an unknown one and its brand was not recognisable, Consumer C felt that the prices offered were very attractive and decided to make a purchase. Clicking on the link in the WhatsApp message, Consumer C was re-directed to a fake digital platform where she keyed in her account credentials and OTPs to make the 'purchase'. This allowed the scammer	No. Although this case involves a phishing scam, it does not fall within the scope of the SRF because it does not have a Singapore nexus. The foreign furniture seller that had been impersonated was neither a legitimate Singapore-based entity nor a legitimate overseas-based entity	N.A.	N.A.	**100% of the loss will be borne by the consumer.** The consumer may approach existing avenues of dispute resolution if he wishes to seek further recourse.

	Details	Assessed under the SRF? (Yes/No)	Responsible FI breached SRF duties? (Yes/No)	Responsible Telco breached SRF duties? (Yes/No)	Outcome
	to obtain her credentials and OTPs. The scammer then proceeded to enter Consumer C's bank account and make unauthorised transfers amounting to $10,000.	that is known to offer services to Singapore residents.			
Case Study 4 – Malware-enabled Scam	Consumer D accessed an online advertisement from a 'seller' of goods/services and was contacted by the scammer (posing as the 'seller') via a digital messaging platform. Consumer D was instructed by the 'seller' to sideload an app as part of the purchase process, and to enable accessibility permissions. Sometime later in the day, Consumer D logged into the mobile banking app on his phone to make other banking transactions. Scammer was then able to remotely view Consumer D's login credentials by using the malware. During the night, while Consumer D was unaware, the scammer remotely controlled his phone using the malware and entered the consumer's banking app to make outgoing transactions, authenticating it using the digital token on the same phone.	No. This case will not be assessed under the SRF, as the consumer's credentials were not entered into a fake digital platform, and the 'seller' who had reached out to him was not impersonating a legitimate business entity.	N.A.	N.A.	**100% of the loss will be borne by the consumer.** The consumer may approach existing avenues of dispute resolution if he wishes to seek further recourse.

	Details	Assessed under the SRF? (Yes/No)	Responsible FI breached SRF duties? (Yes/No)	Responsible Telco breached SRF duties? (Yes/No)	Outcome
Case Study 5 – Responsible FI fulfilled all SRF duties; Telco not involved	Scammer impersonating an FI sent a phishing email to Consumer E informing him of an attractive product. Consumer E clicked on the link within the phishing email, which led him to a spoofed 'FI' website. Consumer E entered his account credentials and OTPs on the fake website to purchase the product. The account credentials, including OTPs, were later used by the scammer to initiate 3 FAST transactions of $1,000, $2,000 and $3,000 respectively, to another local account. As Consumer E had previously adjusted his transaction notification threshold to $1,500, transaction notifications were only sent by the responsible FI for the FAST transactions of $2,000 and $3,000.	Yes. This case is assessed under the SRF, as all elements of an SRF-covered phishing scam have been met.	No. While the responsible FI did not send out notification alerts for the $1,000 transaction, this does not constitute a breach of duty, as Consumer E had opted to raise his transaction notification threshold to $1,500.	N.A. Given that the link leading to the spoofed 'FI' website was sent to the consumer via email and not SMS, Telcos will not be involved in this assessment.	**100% of the loss will be borne by the consumer.** The consumer may approach existing avenues of dispute resolution if he wishes to seek further recourse.
Case Study 6 – Responsible FI did not send notification alerts for outgoing transactions and activation of new digital security	A scammer impersonated the local Police and contacted Consumer F via WhatsApp message. Consumer F was directed by a link in the scammer's WhatsApp message to a fake ICA website to pay for "outstanding fines". Consumer F then entered his banking credentials and OTPs	Yes. This case is assessed under the SRF, as all elements of an SRF-covered phishing scam have been met.	Yes. Responsible FI had failed in its duty to send real-time notification alerts for the activation of a new digital token and	N.A. Telcos will not be involved in this assessment, as the link leading to the fake ICA website	**The responsible FI is expected to bear 100% of losses ($500 x 10 + $4,000)**.

	Details	Assessed under the SRF? (Yes/No)	Responsible FI breached SRF duties? (Yes/No)	Responsible Telco breached SRF duties? (Yes/No)	Outcome
token, and did not provide a kill switch; Telco not involved	into the fake banking website directed from the fake ICA website. Scammer used Consumer F's banking credentials and OTPs to activate a new digital security token on the scammer's phone. The scammer then made 10 FAST transactions of $500 each to another local account. As the bank's system was down, notification alerts for the 10 outgoing transactions and activation of a new digital security token were sent to Consumer F only after 2 days. When Consumer F received the notification alerts, he immediately tried to report to the responsible FI but to no avail due to high call volume. He then tried to activate the kill switch but was unable to do so due to a system issue. 20 minutes later, the scammer made further unauthorised transaction amounting to $4,000 on Consumer F's account, as Consumer F did not manage to have his account blocked. A notification alert was sent for this further $4,000 transaction.		for the first 10 unauthorised transactions. Responsible FI also failed in its duty to make a kill switch available for the consumer at all times.	was sent through WhatsApp, not SMS.	

	Details	Assessed under the SRF? (Yes/No)	Responsible FI breached SRF duties? (Yes/No)	Responsible Telco breached SRF duties? (Yes/No)	Outcome
Case Study 7 – Responsible FI failed to provide a 12-hour cooling off period	A scammer impersonated an FI and contacted Consumer G via a phishing email. The email informed Consumer G that his account was about to be suspended. Consumer G clicked on the website link in the email which brought him to a spoofed 'FI' website where he entered in his account credentials, believing that by doing so, it would prevent his account from being suspended. Scammer subsequently used the account credentials and OTPs provided to take over Consumer G's account without his knowledge and set up a digital token on the scammer's own device. Due to a system error, the responsible FI did not impose a 12-hour cooling off period during which high-risk activities could not be performed. As a result, the scammer was able to increase Consumer G's online transaction limit from $5,000 to $10,000 (which is a high-risk activity) within the 12 hours following the new digital token's activation. Although Consumer G saw the notification alerts informing him of the activation of a new	Yes. This case is assessed under the SRF, as all elements of an SRF-covered phishing scam have been met.	Yes. The responsible FI had failed in its duty to impose a minimum 12-hour cooling off period, which enabled the scammer to increase Consumer G's transaction limit within what should have been the 12-hour cooling off period.	N.A.	**The responsible FI is expected to bear 100% of losses**, even though Consumer G had failed to take due care by clicking on the link in the phishing email and choosing to ignore the notification alerts that were sent to him.

	Details	Assessed under the SRF? (Yes/No)	Responsible FI breached SRF duties? (Yes/No)	Responsible Telco breached SRF duties? (Yes/No)	Outcome
	digital token and the increase of his transaction limit, he did not act on it. The scammer then proceeded to make multiple transactions of $10,000 each, out of Consumer G's account.				
Case Study 8 – Responsible FI did not send notification on change in contact details due to fault of FI's outsourced service provider	Consumer H responded to a phishing SMS which contained a clickable link to a spoofed 'FI' website and provided his account credentials to "pre-order new Singapore commemorative notes". The scammers used Consumer H's account credentials to change his contact details to that of the scammer's. Due to system issue by the responsible FI's vendor, the responsible FI did not send a notification alert to Consumer H's original contact to inform him of the change in contact details. Subsequently, the scammer made multiple overseas transfers from Consumer H's account amounting to $100,000, and SMS transaction notification alerts were instead sent to the scammers' contact. Throughout this incident, the responsible Telco had met its prescribed SRF duties.	Yes. This case is assessed under the SRF, as all elements of an SRF-covered phishing scam have been met.	Yes. The responsible FI had failed to provide the notification of the change in contact details to the consumer, leading to the delayed discovery of all the subsequent fraudulent transactions. The responsible FI is responsible for failure of duties by its vendor.	No.	**The responsible FI is expected to bear 100% of losses**, even though Consumer H had initially failed to take due care by clicking on the link in the phishing SMS.

	Details	Assessed under the SRF? (Yes/No)	Responsible FI breached SRF duties? (Yes/No)	Responsible Telco breached SRF duties? (Yes/No)	Outcome
	Consumer H informed the responsible FI about the fraudulent transactions immediately after receiving the monthly statement. He was fully cooperative during this period.				
Case Study 9 – Responsible FI did not send notifications for *some* transactions	Consumer I responded to a phishing email and provided his account credentials on a spoofed 'FI' website, to sign up for a "fixed deposit at promotional rates". The account details, including OTPs, were used to initiate 10 FAST transactions amounting to $10,000 to another local account. SMS transaction notifications were sent to Consumer I for the first 9 FAST transactions. Due to a system issue encountered by the responsible FI, the 10th SMS transaction notification was not sent. Throughout this incident, the responsible Telco had met its prescribed SRF duties.	Yes. This case is assessed under the SRF, as all elements of an SRF-covered phishing scam have been met.	Yes, but only with respect to the 10th transaction. First 9 transactions: The responsible FI had fulfilled its duties in relation to the first 9 unauthorised transactions. 10th transaction: The responsible FI had failed in its duty to send a transaction notification alert for the 10th transaction.	N.A. Given that the link leading to the spoofed 'FI' website was sent to the consumer via email and not SMS, Telcos will not be involved in this assessment.	**The responsible FI is expected to bear 100% of losses for the 10th transaction.** **Consumer I will bear the losses for first 9 transactions.**

	Details	Assessed under the SRF? (Yes/No)	Responsible FI breached SRF duties? (Yes/No)	Responsible Telco breached SRF duties? (Yes/No)	Outcome
	Consumer I informed the responsible FI about the unauthorised transactions immediately after receiving the monthly statement, within 30 days of the last unauthorised transaction. He did not notice the transaction notification alerts sent on the first 9 transactions earlier.				
Case Study 10 – Responsible Telco connected to non-authorised aggregator	Consumer J received an SMS with the Sender ID "DBS Bank". The SMS was in fact sent by a scammer impersonating DBS. A responsible Telco connected to a non-authorised aggregator to deliver the SMS with the Sender ID "DBS Bank" to Consumer J. The SMS informed Consumer J to reset his digibank password by clicking on a link. Consumer J did so accordingly and keyed in his account details. Consumer J's account credentials, including OTPs, were used by the scammer to initiate 5 FAST transactions amounting to $10,000 to another local account. SMS transaction notifications were sent by the responsible FI for all the transactions,	Yes. This case is assessed under the SRF, as all elements of an SRF-covered phishing scam have been met.	No.	Yes. The responsible Telco had failed in its duty to connect only to authorised aggregators.	**The responsible Telco is expected to bear 100% of losses**, even though Consumer J had failed to take due care by clicking on the link in the phishing SMS.

	Details	Assessed under the SRF? (Yes/No)	Responsible FI breached SRF duties? (Yes/No)	Responsible Telco breached SRF duties? (Yes/No)	Outcome
	and no lapses by the responsible FI were observed.				
Case Study 11 – Responsible Telco did not block unverified SMS not from authorised aggregator	An overseas entity sent an SMS with the Sender ID "DBS Bank" to Consumer K through an overseas network operator directly connected to a responsible Telco. The responsible Telco did not block this SMS. The SMS was in fact sent by an entity impersonating DBS. The SMS informed Consumer K to reset his digibank password by clicking on a link. Consumer K did so accordingly and keyed in his account details. Consumer K's account credentials, including OTPs, were used to initiate 5 FAST transactions amounting to $10,000 to another local account. SMS transaction notifications were sent by the FI for all the transactions, and no lapses by the responsible FI were observed.	Yes. This case is assessed under the SRF, as all elements of an SRF-covered phishing scam have been met.	No.	Yes. The responsible Telco had failed in its duty to block unverified SMS that are not from authorised aggregators.	**The responsible Telco is expected to bear 100% of losses**, even though Consumer K had failed to take due care by clicking on the link in the phishing SMS.
Case Study 12 – Responsible Telco did not	Consumer L receives a scam SMS from a scammer pretending to be a well-known company selling durians. The responsible	Yes.	No.	Yes.	**The responsible Telco is expected to bear 100% of losses**, even

	Details	Assessed under the SRF? (Yes/No)	Responsible FI breached SRF duties? (Yes/No)	Responsible Telco breached SRF duties? (Yes/No)	Outcome
implement anti-scam filter	Telco's anti-scam filter was not operational for 48 hours. The SMS was labelled as "Likely-SCAM" as the entity was not registered with the SSIR. The SMS informed Consumer L to click on a link to purchase cheap durians by keying in his banking account credentials. Consumer L did so accordingly. The link was a malicious link known to the Telco. Consumer L's account credentials, including OTPs, were used to initiate 5 FAST transactions amounting to $10,000 to another local account. SMS transaction notifications were sent by the responsible FI for all the transactions, and no lapses by the responsible FI were observed.	This case is assessed under the SRF, as all elements of an SRF-covered phishing scam have been met.		The responsible Telco had failed in its duty to implement an anti-scam filter.	though Consumer L had failed to take due care by clicking on a link in an SMS labelled as "Likely-SCAM".
Case Study 13 – Responsible FI did not send transaction notification and Responsible Telco connected to	Consumer M received an SMS with the Sender ID "UOB Bank" to Consumer M. The SMS was in fact sent by a scammer impersonating UOB. A responsible Telco connected to a non-authorised aggregator to deliver the SMS with the Sender ID "UOB Bank" to Consumer M.	Yes. This case is assessed under the SRF, as all elements of an SRF-covered phishing scam have been met.	Yes. The responsible FI had failed in its duty to provide transaction notifications.	Yes. The responsible Telco had failed in its duty to only connect to authorised aggregators.	**The responsible FI is expected to bear 100% of losses**, despite the responsible Telco also failing in its duty to only connect to authorised aggregators and Consumer M

	Details	Assessed under the SRF? (Yes/No)	Responsible FI breached SRF duties? (Yes/No)	Responsible Telco breached SRF duties? (Yes/No)	Outcome
non-authorised aggregator	The SMS informed Consumer M to reset his digibank password by clicking on a link. Consumer M did so accordingly and keyed in his account details. Consumer M's account credentials, including OTPs, were used to initiate 5 FAST transactions amounting to $10,000 to another local account. The responsible FI failed to send SMS transaction notifications for all the transactions.				failing to take due care by clicking the phishing link.
Case Study 14 – Responsible FI did not send transaction notification for some transactions and Responsible Telco connected to non-authorised aggregator	Consumer N receives a scam SMS with the spoofed Sender ID "OCBC Bank". The SMS was in fact sent by a scammer impersonating OCBC. The responsible Telco connected to a non-authorised aggregator to deliver the SMS. The SMS informed Consumer N to reset his digibank password by clicking on a link. Consumer N did so accordingly and keyed in his account details. Consumer N's account credentials, including OTPs, were used to initiate 5	Yes. This case is assessed under the SRF, as all elements of an SRF-covered phishing scam have been met.	Yes, but only in respect of the 4th and 5th unauthorised transactions.	Yes. The responsible Telco had failed in its duty to only connect to authorised aggregators.	<u>First 3 transactions</u>: As the responsible FI had met its duties in respect of the first 3 transactions, the responsible FI is not expected to bear these losses. **The responsible Telco is therefore expected to bear 100% of the losses for the first 3 transactions,** even though Consumer N had failed to take

	Details	Assessed under the SRF? (Yes/No)	Responsible FI breached SRF duties? (Yes/No)	Responsible Telco breached SRF duties? (Yes/No)	Outcome
	FAST transactions amounting to $10,000 to another local account. The responsible FI sent SMS transaction notifications only for the first 3 FAST transactions. The system of the responsible FI went down before the 4th and 5th transaction notifications were sent.				due care by clicking on the link in the phishing SMS. <u>4th and 5th transactions</u>: The responsible FI had failed in its duty to provide transaction notifications for the 4th and 5th transactions. **The responsible FI is therefore expected to bear 100% of losses for the 4th and 5th transactions**, despite the responsible Telco also failing in its duty to only connect to authorised aggregators and Consumer N failing to take due care by clicking on the link in the phishing SMS.

	Details	Assessed under the SRF? (Yes/No)	Responsible FI breached SRF duties? (Yes/No)	Responsible Telco breached SRF duties? (Yes/No)	Outcome
Case Study 15 – Responsible FI and Telco fulfilled all SRF duties	A scammer impersonating DHL attempted to send a spoofing SMS containing a clickable link to Consumer O, requesting for the consumer to pay for a "customs fee". The responsible Telco involved in the delivery of the SMS had connected only to authorised aggregators to the deliver the SMS, and had also implemented an anti-scam filter. The Sender ID of the SMS was reflected as "Likely-SCAM" when it reached Consumer O. Consumer O proceeded to click on the link within the phishing SMS that led to a fake OCBC website. Believing it to be OCBC's real website (he was a customer of OCBC), he entered his account credentials and OTPs to pay the "customs fee" on the fake website, allowing the scammer to obtain his credentials and OTPs. The scammer then used the above information to login to Consumer O's account and perform outgoing transactions amounting to $5,000. No high-risk activities were performed by the scammer. The responsible FI (OCBC) provided transaction notifications on a real-time basis. As Consumer O was away from his	Yes. This case is assessed under the SRF, as all elements of an SRF-covered phishing scam have been met.	No.	No.	**100% of the loss will be borne by the consumer.** The consumer may approach existing avenues of dispute resolution if he wishes to seek further recourse.

	Details	Assessed under the SRF? (Yes/No)	Responsible FI breached SRF duties? (Yes/No)	Responsible Telco breached SRF duties? (Yes/No)	Outcome
	device for a short while, he only noticed the unauthorised transactions about 30 minutes later. He immediately activated the kill switch and reported the transactions to the responsible FI via the 24/7 reporting channel. No further unauthorised transactions took place. The responsible FI was unable to recover the $5,000 lost, as within the 30 minutes before Consumer O reported the unauthorised transactions, the funds had been transferred overseas.				

11. Annex B – SRF Operational Workflow

Claim Stage

11.1. The responsible FI will be the first and overall point of contact with the consumer. At the time the consumer files a claim, the responsible FI should explain the scope of covered phishing scams and assess if the claim falls within that scope. It should also explain the operational workflow to the consumer at the time he or she files a claim, and inform the consumer of the projected investigation timeline as set out in paragraph 11.7.

11.2. The consumer must furnish a valid email address and a police report within 3 calendar days from the date of notification of the phishing scam to the FI, in order to facilitate the claims investigation process. Where requested, the responsible FI should also guide the consumer on the procedure to file a police report.

Information gathering

11.3. The responsible FI may request for the consumer to provide information set out in paragraph 3.18 of the EUPG. If requested by the responsible FI, it is the consumer's responsibility to provide records of communication with the scammer on digital messaging platforms and, where relevant, the name of the responsible Telco whose services the consumer had subscribed to and associated mobile phone number. Such communication records may take the form of screenshots capturing the communications sent by the scammer to the consumer. Where the scam was perpetrated via the SMS channel, the consumer should also provide details of the purported SMS message which was used to scam the consumer including the date, time and sender of the SMS. The communication records should also sufficiently demonstrate that the scammer:

(a) had posed as an impersonated entity;

(b) intended to obtain account credentials under false pretences; and

(c) had directed the consumer to a digital platform of the impersonated entity to enter his or her account credentials.

11.4. Upon enquiry by the consumer, the responsible FI will be expected to provide the consumer with relevant information that the responsible FI has of all transactions arising from the covered phishing scam which were initiated or executed from the consumer's account, including transaction dates, transaction timestamps and parties to the transaction.

Investigation Stage

Where consumer's claim is not eligible for assessment under the SRF

11.5. If the consumer's claim is assessed to fall outside the scope of the SRF (i.e., the loss did not arise from a covered phishing scam), it will not follow the "waterfall" approach (in section 6). The responsible FI should investigate the claim per its existing investigation and dispute resolution process in a fair, reasonable and timely manner. In line with the current process for all scam cases reported to FIs, if the consumer is dissatisfied with the outcome of the responsible FI's assessment or investigation, he or she may approach FIDReC.

Where consumer's claim is eligible for assessment under the SRF

11.6. On the other hand, if the consumer's claim *does* involve a covered phishing scam, the responsible FI will next assess whether the scam was perpetrated through SMS, and inform the responsible Telco where applicable. A responsible FI, and responsible Telco where applicable, should conduct the investigation in a fair, reasonable and timely manner.

(a) **If the scam was perpetrated through SMS**, the responsible FI and Telco should both commence their investigation of the consumer's claim, and whether each of them had fulfilled their respective duties under section 5. On completion of the investigation, the responsible FI should notify the consumer accordingly.

(b) **If the scam was not perpetrated through SMS** (e.g., the scam was perpetrated via WhatsApp or email), only the responsible FI will need to commence its investigation of whether any duties have been breached, and notify the consumer on completion.

Timelines to complete investigation(s)

11.7. The responsible FI, and responsible Telco where applicable, shall endeavour to complete an investigation of any relevant claim within 21 business days for straightforward cases, or 45 business days for complex cases. Complex cases may include cases where the consumer or any other party involved in the claim is overseas and uncontactable during the investigation period.

Outcome Stage

11.8. The responsible FI should within the stipulated periods in paragraph 11.7 provide the consumer with a written reply of the investigation outcome and the assessment of the consumer's responsibility for the losses. This will include the quantum of payout to the consumer, if any. The responsible FI should seek the said consumer's acknowledgement (which need not be an agreement) of the written reply of the investigation outcome.

Recourse Stage

11.9. If the consumer does not agree with the investigation outcome (i.e., where the responsible FI has assessed that the claim falls out of the SRF's scope, or where the claim was eligible for assessment under the SRF but no breach of duties was found and the loss falls on the consumer), the consumer may pursue other avenues for redress. The consumer may approach FIDReC for dispute resolution with the responsible FI, write to IMDA if he or she disagrees with the responsible Telco's assessment on the breach of its duties, or file a claim with the Courts.

11.10. The assessments made by existing dispute resolution bodies may consider factors beyond the duties under Section 5 of this paper, based on the facts and circumstances of each case. These may include whether statutory duties, duties under common law, or duties under the EUPG (in the case of responsible FIs and consumers), have been fulfilled.

12. Annex C – Multi-Layered Approach to Combat Scam SMS and Scam Calls

12.1. IMDA's anti-scam strategy has been developed with the intention to disrupt scam operations across various communications channels via a multi-layered approach. IMDA has partnered with Telcos to implement anti-scam measures that strengthen safeguards for SMS and calls to Singapore users:

Safeguards Implemented for SMS Channel

(a) **Reactive blocking of SMS**: Since 2019, reactive blocking of SMS with malicious links in SMS upon notification by the police has been in place.

(b) **Pre-emptive Blocking Measures:**

(i) **Anti-scam filters:** Since October 2022, IMDA has required Telcos to implement anti-scam filtering solutions at the network level. The anti-scam filtering solutions filter scam SMS messages through the detection of known malicious URLs, and suspicious patterns (e.g., keywords, phrases and message formats that are typically used in scam SMS).

(ii) **SMS Sender ID Registry Regime (SSIR):** Since 31 January 2023, all organisations that send Sender ID SMS must register with the SSIR. All Sender ID SMS with non-registered Sender IDs will be tagged as "Likely-SCAM". There has been strong support for the SSIR, with more than 3,600 merchants onboard the SSIR as of June 2023. These 3,600 merchants – which includes financial institutions, e-commerce operators, logistics providers – account for over 96% of Sender ID SMS.

Safeguards Implemented for Calls Channel

(c) **Verification of Domestic Callers**: Since 2017, Telcos have been conducting verification before setting up local calls, as a means of preventing domestically originating calls from being spoofed.

(d) **Reactive Blocking of Specific Spoofed Numbers**: Since 2019, Telcos have been blocking commonly spoofed local trusted numbers such as emergency hotlines and Government agencies.

(e) **Pre-Emptive & Wholesale Blocking of International Spoofed Calls**: Since July 2022, Telcos have been blocking spoofed fixed line and mobile numbers i.e., international calls bearing the "+65 6", "+65 9", "+65 8" prefix.

Next Bound Anti-Scam Efforts

(f) **Blocking Residual Overseas Risk:** To address residual risks in the calls and SMS channels arising from international numbers, IMDA is working with the Telcos to give consumers the option not to receive international calls and SMS. These service options will made available progressively as early as end-2023.

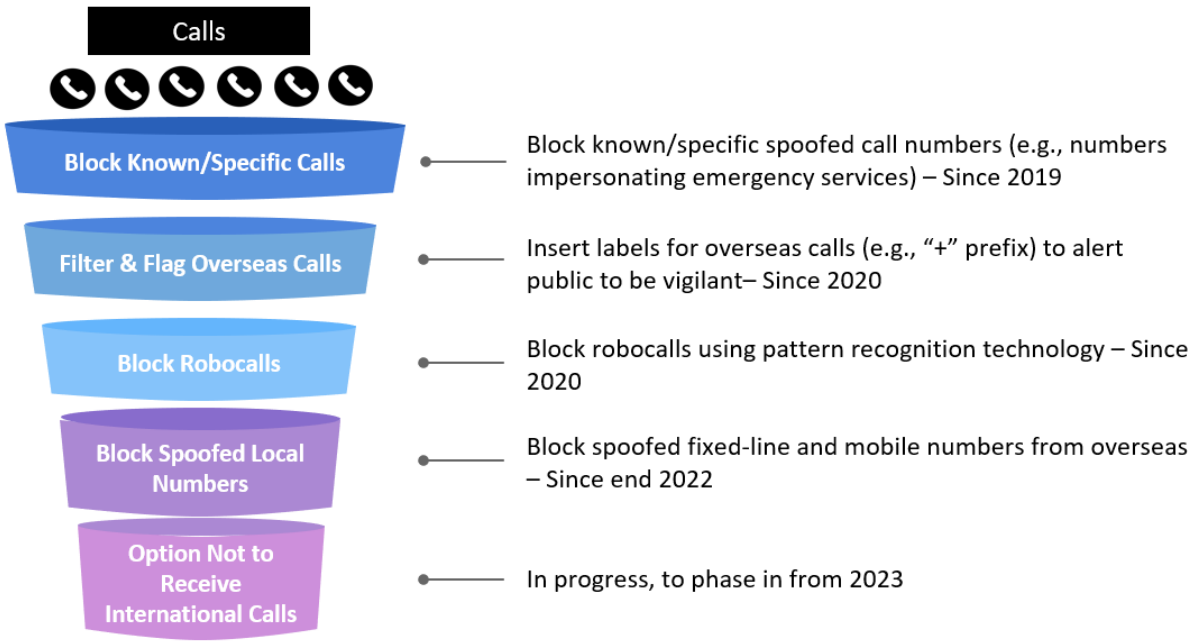
12.2. IMDA's multi-layered approach has been effective in the fight against scams:

(a) Scam cases perpetrated via SMS have declined significantly. In the 3 months following the launch of the mandatory SSIR regime in January 2023, scam SMS cases fell by 70% compared to the three months before.

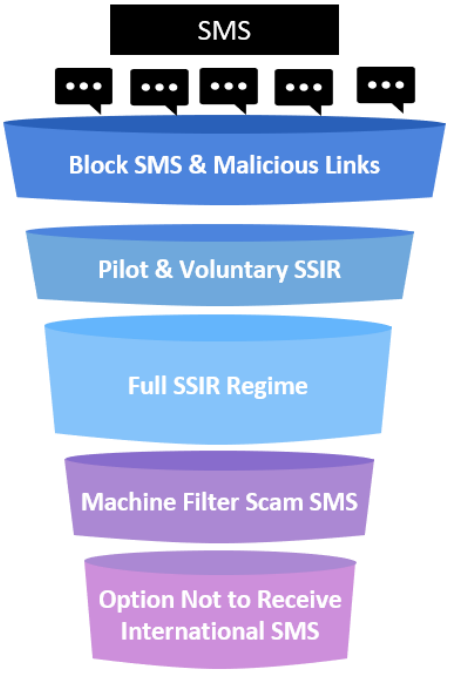
(b) The public has also responded positively to the SSIR. In a survey conducted, 4 in 5 agreed that the "Likely-SCAM" label made them more cautious about whether the SMS is real or fake, and 92% would choose to ignore or delete the SMS that are labelled "Likely-SCAM".[24]

(c) Significant volume of scam calls has been blocked upstream. In Q1 2023, around 22 million international calls were blocked per month (or 720,000 per day). This translates to one call blocked for every four international incoming calls made to Singapore.

Summary of multi-layered approach to address scam calls and scam SMS



[24] SSIR Likely-SCAM Online Study conducted by MCI in June 2023 with more than 1,000 Singapore residents aged 15 and above to understand public responses to the "Likely-SCAM" label.



- Block SMS and malicious links within SMS once notified – Since 2019
- Pilot SMS Sender ID Registry in Aug 2021; Voluntary Singapore SMS Sender ID Registry "SSIR" – block upfront scam SMS using spoofed Sender IDs – Mar 2022
- Make Sender ID registration a requirement for organisations that use Sender IDs – 31 Jan 2023
- Implement solution to identfy & filter scam SMS – Since Oct 2022
- In progress, to start in mid-2024

13. Annex D – Jurisdiction Comparison

13.1. Scams are a growing problem worldwide. Around US$55.3 billion was lost to scams worldwide in 2021, up by 15.7% from 2020.[25] From a broad survey of other jurisdictions, namely the UK, the EU (with Germany and France as case studies) and Australia, we understand that these jurisdictions have existing regulations and/or guidelines which converge on providing reimbursement mostly for unauthorised payments. Recently in June 2023, the UK Payment Systems Regulator (PSR) has also confirmed its reimbursement framework for authorised push payment (APP) fraud (i.e., authorised transactions made through the UK's Faster Payments system arising from fraud, such as love, job, or impersonation scams). Some details on the approaches in the UK, EU and Australia are set out in the following table.

	UK	EU	Australia
Entities covered, with relevant instrument(s) (e.g., rules, guidelines)	Entities covered: Payment service providers (e.g., banks, building societies, payment firms). Relevant instruments: Payment Services Regulations 2017; and Contingent Reimbursement Model (CRM) Code[26].	Entities covered: Payment service providers (e.g., banks, other FIs). Relevant instrument: Payment Services Directive 2.	Entities covered: Banks, credit unions, building societies and other providers of e-payment facilities. Relevant instrument: ePayments Code.
Coverage of unauthorised transactions	Generally, consumers are reimbursed for losses arising from unauthorised transactions, as long as the consumer was neither fraudulent nor grossly negligent.	Generally, consumers are reimbursed for losses arising from unauthorised transactions, as long as the consumer was neither fraudulent nor grossly negligent.	The ePayments Code sets out conditions under which consumers will not be liable for losses arising from unauthorised transactions. Conditions include where: i) the loss arose from the fraud or negligence of the FI's employee or agent;

[25] Source: Global Anti-Scam Alliance, The Global State of Scams Report – 2022.

[26] Under the voluntary CRM Code, UK Finance reports that reimbursement for victims whose institution participates in the CRM was about 48% of losses in 2021 and 60% for the first half of 2022. Victims of institutions not participating in the program received 27% reimbursement overall in 2021 and 44% in the first half of 2022.

			ii) the unauthorised transaction could be made using an identifier without a passcode or device; or iii) it is clear that the consumer did not contribute to the loss.
Coverage of authorised transactions	Upcoming rules in the UK would assess APP fraud (e.g., scams such as love / job scams that result in authorised transactions via the UK Faster Payments system), requiring payment firms to reimburse all in-scope customers who fall victim to APP fraud, unless the consumer had been fraudulent or grossly negligent. The UK PSR is consulting on the parameters of the reimbursement model (e.g., maximum level of reimbursement, claim excess, additional guidance on the customer standard of caution) and targets for implementation in 2024.	Nil.	Nil. Australia announced in May 2023 that there will be a mandatory co-regulatory code developed by the Australian Competition and Consumer Commission that involve banks, telcos, and big social media platforms to mitigate scams.