Monetary Authority of Singapore

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

Response to Feedback Received

P016-2023 – 24 October 2024

Response to Consultation Paper on Proposed Shared Responsibility Framework

Contents

1. Preface

1.1. On 25 October 2023, MAS and IMDA issued a joint consultation paper for a proposed Shared Responsibility Framework (SRF), which assigns financial institutions (FIs) and telecommunication operators (Telcos) relevant duties to mitigate a defined set of phishing scams. The SRF, to be implemented via a set of Guidelines (SRF Guidelines), is aimed at strengthening the direct accountability of FIs and Telcos to consumers for losses incurred from phishing scams. MAS and IMDA expect responsible entities to bear any scam losses arising from failure to fulfill any of the relevant duties, under the "waterfall" approach.

1.2. The SRF will operate as part of the wider efforts by Government and industry to protect consumers against scam losses – this is independent of criminal investigations by the Police. Broadly, these efforts operate on two fronts: first, to hold ecosystem entities accountable for implementing anti-scam measures to protect consumers against scam losses; and second, to provide reasonable avenues of recourse for scam victims.

a) The SRF should be seen in the context of the broader suite of upstream and downstream measures that Government, banks, and other ecosystem players have progressively implemented to tackle scams in Singapore. To hold entities in the scams ecosystem accountable for implementing these anti-scam measures, the Government has set out duties and obligations through a combination of law, regulations, directions, and guidelines.

b) On the recourse front, MAS expects FIs to treat victims of scams fairly. FIs must consider whether they have fulfilled their obligations and whether the victim had acted responsibly. Depending on the facts of each case, FIs may offer payouts to scam victims. If a scam victim is not satisfied with the payout offered, he may decline the offer and instead approach the Financial Industry Disputes Resolution Centre (FIDReC) for mediation or adjudication. Scam victims can also pursue civil claims against the relevant entities through the courts.

1.3. Against this backdrop, the SRF serves to enhance the direct accountability of FIs and Telcos to consumers for implementing anti-scam measures and provides a practical means of how responsibility will be shared for phishing scams. MAS and IMDA expect responsible entities to make direct payouts to consumers for scam losses arising from failure to fulfill any of the relevant duties. In addition, having considered the public feedback received, MAS will introduce an additional duty on fraud surveillance. This additional duty requires FIs to better detect and mitigate cases of consumers' accounts having material sums being rapidly wiped out by unauthorised transactions in a phishing scam.

1.4. For cases which fall outside the scope of the SRF, or where entities have not breached any relevant duties, existing avenues of recourse remain available (as highlighted in para 1.2(b) above). In parallel

to the recourse avenues, the Government will continue to rely on regulations to hold entities in the scams ecosystem, including those outside the SRF, accountable for implementing anti-scam measures.

1.5. The SRF consultation closed on 20 December 2023, and MAS and IMDA would like to thank all respondents for their contributions. The list of respondents is in **Annex A**. MAS and IMDA have carefully considered the feedback received and, where appropriate, incorporated them into the SRF Guidelines. MAS and IMDA will also take into account the valuable insights, in shaping the longer-term policy approach towards enhancing consumer protection for victims of scams arising from unauthorised transactions. Comments that are of wider interest, together with MAS' and IMDA's responses, are set out below.

2. Entities Covered under the SRF

2.1. MAS and IMDA sought comments on the entities to be involved – namely, FIs including all full banks and relevant payment service providers (PSPs), and Telcos which are mobile network operators.

Call for entities in the digital communications layer to be included

2.2. Respondents recognised the crucial role of FIs and Telcos in mitigating phishing risks, as custodians of customers' money, and in facilitating the sending of SMS which is an official communication channel used by FIs, respectively. Many respondents called for more entities in the digital communications layer (including messaging platforms and social media services) to be included in the SRF.[1] Respondents noted that majority of scams were perpetrated by scammers through these channels, particularly digital messaging platforms, social media, and chat-enabled online shopping platforms.

PSPs issuing e-wallets

[1] Some respondents also called for the inclusion of other players such as SMS aggregators, mobile app providers and software companies.

2.3. One respondent sought clarity on the need for PSPs issuing e-wallets to be included in the SRF, given that protective features specific to e-wallets already functioned as natural impediment to the scale of potential scam activities impacting e-wallets.

MAS' & IMDA's Response

2.4. MAS and IMDA note the concerns raised by respondents regarding the role of other entities in the scams ecosystem. Compared to payout frameworks in most other jurisdictions which only cover banks, the SRF already holds a wider scope of entities accountable by covering Telcos.[2] Nonetheless, the Government will continue to study the appropriate measures to hold other industry players in the scams ecosystem more accountable for implementing anti-scam measures, taking into account the practices and ongoing developments in other jurisdictions.

2.5. In relation to the digital communications layer, these online services have increasingly been used by scammers to reach out to victims. The Government is keenly aware of the need to take effective action against scam content online, and hold the online services accountable to better protect consumers. For example:

a) The Online Criminal Harms Act (OCHA), which MHA has progressively operationalised since February 2024, allows the Government to issue Directions to entities or individuals, including internet service providers and messaging app companies, to prevent accounts or content suspected to be involved in scams from interacting with or reaching users in Singapore.

b) In June 2024, the Government issued legally-binding Codes of Practice under the OCHA to require providers of designated online services to put in place systems, processes, and measures to proactively disrupt online scams affecting users in Singapore. Providers that do not comply with the Codes of Practice will be issued a Rectification Notice to rectify the non-compliances.

c) Non-compliance to a direction or Rectification Notice is an offence. An order to restrict access to the service or part of the service, to limit Singapore users' further exposure to the scam, can also be issued as an escalatory enforcement stance, taken only when necessary, if there has been non-compliance.

[2] To avoid doubt, the SRF will currently only apply to Telcos which are Mobile Network Operators (MNOs) (i.e. SingTel Mobile Singapore Pte Ltd, M1 Ltd, StarHub Ltd and SIMBA Telecom Pte Ltd), and not to Telcos which are Mobile Virtual Network Operators (MVNOs).

2.6. In relation to PSPs, MAS notes that larger amounts can be potentially scammed from e-wallets, especially with the raised regulatory "stock" and "flow" caps[3] (e-wallet caps) from 15 December 2023 which allows for larger amounts to be held in and transferred through e-wallets. E-wallet PSPs therefore have the responsibility to implement robust controls to safeguard consumers' accounts and to effectively respond to suspicious transactions. MAS expects e-wallet service providers holding a major payment institution licence to participate in the SRF. For the avoidance of doubt, banks and e-wallet PSPs that do not serve retail customers or do not provide digital services with transaction capability will not be part of the SRF.

3. Types of Scams Covered

3.1. MAS and IMDA sought comments on the proposed scope of phishing scams[4] covered under the SRF. Such phishing scams should also have a clear Singapore nexus in that the impersonated entities should be Singapore based, or based overseas and offer their services to Singapore residents. Excluded scam types are detailed in the consultation paper.

3.2. Several respondents called for the SRF to include more scam variants such as malware-enabled scams (malware scams), or all types of fraudulent payments, as long as they relate to impersonation or compromised credentials. A few respondents suggested expanding the risk vectors covered by the SRF to include phishing scams where credentials were revealed via text messages, and non-digital means (i.e., phone calls or face-to-face), since vulnerable consumers including the elderly may be more susceptible to phishing scams via non-digital means. Other respondents sought clarity on whether the practice of "malvertising" in SMS, which refers to delivering malware through online advertising, would constitute phishing scams with a digital nexus within the SRF's scope. There were no suggestions for the SRF to cover scams involving authorised transactions (e.g., investment scams, love scams).

3.3. A few industry respondents suggested excluding known scam typologies that have already been proactively communicated to customers through official channels, taking into account industry efforts on consumer education.

[3] The e-wallet stock cap (the maximum amount of funds that can be held at any given time in each e-wallet) has been raised from S$5,000 to S$20,000, and the flow cap (the maximum total outflow of funds over a rolling 12-month period from each e-wallet) from S$30,000 to S$100,000.

[4] i.e., phishing scams which are perpetrated through the impersonation of a legitimate business or government entity, where account credentials were revealed on a fake digital platform (e.g., website, application), leading to unauthorised transactions being performed.

MAS' & IMDA's Response

3.4. The SRF focuses on a defined scope of phishing scams where the corresponding duties for FIs and Telcos can be clearly set out. Hence, MAS and IMDA will maintain the consulted policy position as opposed to a broader category of fraudulent payments beyond phishing (some of which may arise from scams involving authorised transactions). The SRF will also not include malware scams and the practice of "malvertising". MAS and relevant government agencies will work with FIs and ecosystem players to put in place measures to mitigate the risk of malware scams, including holding ecosystem players accountable where necessary. While this is being worked out, banks have also taken a more forward-leaning approach towards assessing goodwill payments for customers affected by malware scams[5], given that these are a more sophisticated scam typology which customers may be less well-equipped to protect themselves against. The Government will continue to work closely with the industry to introduce refinements or new measures to keep pace with changes in the threat landscape.

3.5. Regarding the feedback to expand the risk vectors to include phishing scams via non-digital means, MAS and IMDA will maintain the consulted policy position to exclude these types of scams. Phishing via non-digital means form part of the more established phishing scam typologies, where there have been substantial mitigation efforts, including advisories and public education campaigns. These efforts include stepped-up public education to sensitise consumers to the fact that they should never reveal their credentials or one-time password (OTP) directly to anyone under any circumstances. It is important that consumers adopt good baseline hygiene practices to protect themselves against scams and to uphold the principle of consumer responsibility, which is one of the policy objectives of the SRF.

3.6. In relation to the suggestion to exclude known scam typologies that have already been proactively communicated to customers, there will not be a blanket exemption as doing so could disincentivise FIs and Telcos from strictly upholding the desired standards of anti-scam controls at all times.

[5] The Association of Banks in Singapore's media release dated 24 Oct 2023: *abs.org.sg/docs/library/media-release_abs-statement---update-on-scam-stats_goodwill-framework_24-oct-23_final-(v2).pdf.*

4. Duties of Responsible FIs and Responsible Telcos

4.1. MAS and IMDA sought comments on the specific anti-scam duties assigned to FIs and Telcos to mitigate phishing scams. Failure to fulfil any of the specified duties assigned will result in an expectation for the FI or Telco responsible to make full payouts in respect of losses arising from phishing scams.

4.2. A recurring theme among the feedback received was that FIs and Telcos should implement more robust controls, or a wider range of measures to bolster baseline security standards over digital banking and payments, as well as the telecommunications infrastructure. Some respondents commented that an unintended outcome of stipulating explicit duties was that the responsibilities of FIs and Telcos for payouts would be limited.

4.3. With reference to the FI duties under the SRF, several members of the public suggested the inclusion of an additional FI duty on fraud surveillance and detection, as it is reasonable to expect FIs to be able to detect and block potential fraudulent transactions which are unusual or large.

4.4. A key area raised among industry respondents was how the requirements under the SRF applied in the context of PSPs, whose business operations may not directly correlate with some of the FI duties (e.g. provisioning of digital token). A few respondents also indicated the need for a transitional period before the SRF is phased in. Additionally, several respondents sought further clarity on the following:

a) On FI duty #2: Whether MAS would prescribe the mode of notification alerts; and

b) On FI duty #4: MAS' expectations on the types of channels available for customers to perform the kill switch.

4.5. In relation to Telcos' duties under the SRF, there were suggestions to implement additional security measures, including the use of AI to pre-emptively detect and block malicious SMS. Additionally, a respondent sought clarity on whether there should be an equivalent SRF duty for Telcos to ensure SMS delivery, given the existing SRF duty for FIs to provide notification alerts on a real-time basis for activation of digital security token, high-risk activities, and outgoing transactions.

MAS' and IMDA's Response

4.6. The duties for FIs and Telcos under the SRF are fundamental duties identified to be directly relevant to combatting phishing scams. These duties were formulated based on the principles that they are discrete, objective, and verifiable. Under the SRF, FIs and Telcos are expected to pay full scam losses to consumers if they breach any of the relevant duties, based on a "waterfall" approach. Rather than limiting the responsibilities of FIs and Telcos for payouts, the SRF serves to achieve the policy objective of direct industry accountability to consumers, which had not hitherto been provided for in any other frameworks. MAS and IMDA will retain the proposed duties as consulted, and will add a new FI duty for fraud surveillance, in response to feedback received. MAS and IMDA will continue to review the duties under the SRF as necessary.

4.7. MAS agrees with the feedback to include an additional FI duty in the area of fraud surveillance. A key objective here is to strengthen FIs' fraud surveillance controls to substantially reduce cases of customers having material sums being rapidly wiped out from their accounts without their knowledge – such cases are of greatest concern to MAS. In turn, customers must expect some added friction in their payment transactions, as banks progressively step-up anti-scam safeguards and fraud surveillance monitoring to achieve better security:

SRF Duty on Fraud Surveillance
• FIs must have in place real-time fraud surveillance directed at detecting unauthorised transactions in a phishing scam to a scammer(s). • If a customer's account is being rapidly drained of a material sum to a scammer(s), FIs must either block the transaction until it is able to reach the customer for positive confirmation, or send a notification to the customer and block or hold the transaction for 24 hours.

MAS will allow a 6-month transition period (from the date of the SRF's commencement) for FIs to be held to the fraud surveillance duty, as this duty was not part of the four FI duties originally consulted on. Once this transition period is over, FIs would be expected to provide payouts to consumers if they breach the fraud surveillance duty.

4.8. For PSPs, specific to the imposition of a 12-hour cooling off period (FI Duty #1), this would apply to logins to an e-wallet on a new device.[6] As to the provision of notification alert(s) on a real-time basis (FI Duty #2), these apply when there is a login to an e-wallet on a new device, or during the conduct of high-risk activities (i.e. change of account contact details, increase in transaction limits, disabling

[6] MAS has informed all relevant PSPs the expectations of them to implement anti-scam duties prior to effecting the higher e-wallet cap. MAS wishes to highlight that a subset of these measures are applicable to the SRF, and MAS has amended the SRF Guidelines to reflect this, where relevant.

transaction notifications, and adding new payee). The provision of outgoing transaction notification alerts (FI Duty #3) and reporting channel including a self-service feature (FI Duty #4) are relevant to PSPs the same way that these duties apply to banks. On the basis that these are fundamental anti-scam duties that were raised as part of the consultation process. MAS will not be granting a transition period for implementation of these four duties. Instead, PSPs are expected to implement these duties, prior to the commencement of the SRF.

4.9. On the following feedback:

a) Mode of notification alerts (whether via SMS, in-app, email or otherwise)

MAS will not prescribe the mode of notification alerts. This considers feedback received from FIs, that not all consumers had registered valid phone number(s) or email address(es) upon account opening, in addition to the fact that not all consumers are digital mobile application users. It would therefore be more practical to require FIs to send the notification alerts through the mode that is already familiar to their existing customer, or one that the consumer had explicitly opted for.

b) Types of channels available for customers to perform the kill switch

The purpose of a kill switch is to allow consumers an avenue through which they can quickly block their account and prevent further unauthorised transactions. Accordingly, such a channel must be readily accessible and user friendly (i.e., customers must be able to easily find the kill-switch and knows how to use it intuitively), and typically availed over the phone or via the FI's mobile application.

4.10. On the feedback for Telcos to use AI to pre-emptively detect and block malicious SMS, Telcos have already implemented an analytics-based module with machine learning to filter scam SMS. However, with machine learning, continuous training is needed to improve the model to detect scam SMS accurately. For the purposes of the SRF, Telcos' compliance with the obligation to implement an anti-scam filter will be assessed based on whether its filter successfully blocked SMS with known malicious URLs that Telcos received from the Police on an ongoing basis. **Annex C** sets out an overview of the measures for Telcos suggested by the public, and the suggested measures that Telcos have already implemented.

4.11. Moreover, IMDA notes that SMS is only one of the many modes of notification (e.g. in-app notifications, emails) used for online banking transactions. As supporting infrastructural providers for the SMS mode of communication, Telcos serve as a conduit in managing the storage of SMS sent by FIs, before they are forwarded to the recipient. However, the successful delivery of an SMS depends on multiple factors, not all of which are within the Telcos' control. For example, SMS delivery cannot be guaranteed in scenarios where the recipient's phone is inactive or experiencing technical difficulties. There may also be cases where an SMS aggregator fails to send an SMS to a Telco, in which case the Telco cannot

deliver the SMS to the recipient. Additionally, factors such as poor reception or the network that the recipient is connected to (i.e. local or overseas) can also affect the timely receipt of SMS. Acknowledging these inherent limitations of the SMS mode of communication underscores the need for multi-channeled notification to enhance online banking security.[7]

4.12. For completeness, the duties of FIs and Telcos under the SRF are set out in **Annex D** below.

5. Waterfall Approach under the SRF

5.1. MAS and IMDA sought comments on the "waterfall" approach for sharing of responsibility for scam losses arising from the covered phishing scams.

5.2. Responses were mixed. Some respondents supported the principles-based nature of the SRF in placing the FI as the predominant service provider and the first-in-line expected to provide payouts when SRF duties are breached. Telcos are included as the secondary and supporting layer in the "waterfall" in recognition of their responsibility in protecting consumers from the in-scope SMS phishing scams. These respondents noted that the "waterfall" approach was a fair and clear framework to assign responsibility and payouts. Other respondents commented that the "waterfall" approach would result in disproportionate loss-bearing outcomes when there is a clear breach of SRF duties by either the FI or Telco.

5.3. There were multiple suggestions on alternatives for assigning responsibility for losses. A few respondents suggested equally assigning the responsibility for losses between FIs and Telcos in situations where both had breached their respective duties under the SRF. Others suggested that the FIs and Telcos should assume liability as a default unless the customer was deemed to be at fault. Some respondents suggested factoring in the consumer's contributory role in determining the payout amount, to encourage consumer responsibility and reduce moral hazard. A few Telco industry respondents also suggested a liability cap for losses.

MAS' and IMDA's Response

5.4. MAS and IMDA had, in consultation with industry players, considered alternative approaches for allocating responsibility for scam losses. The "waterfall" approach was ultimately chosen as it provides

[7] To reduce phishing risk, major retail banks in Singapore have been reducing their reliance on SMS One-Time Passwords (OTPs) for authentication. For instance, since July 2024, the banks have progressively phased out the use of SMS OTPs for bank account login by customers who are digital token users.

a straightforward assessment of how responsibility will be shared. This is a practical and simple approach for consumer recourse. By assigning the order in which entities in the SRF are assessed for breaches of SRF duties to determine who will bear the scam losses, the "waterfall" approach incentivises all parties to stay vigilant and perform their roles to uphold the safety of the digital banking and payments ecosystem.

5.5. For the avoidance of doubt, the FI will be expected to bear the scam losses in situations where both the FI and Telco have not met their specified duties. This is in accordance with the "waterfall" approach.

5.6. On the issue of moral hazard, the SRF seeks to instill the principle of shared responsibility and clearly defines conditions under which the consumers' scam losses are made good. FIs or Telcos are expected to provide payouts under the SRF only if there is failure to discharge their specified duties. This preserves the incentive for all parties to exercise vigilance. Nonetheless, scam victims who do not receive payouts under the SRF can still seek recourse via other existing channels mentioned earlier in this paper.

5.7. On the issue of a liability cap for losses, MAS and IMDA recognise that unlike FIs, which are the custodians of consumers' monies, Telcos are communications providers that play a secondary and supporting role to the FIs in the SRF. This distinction has been duly reflected in the waterfall approach, which places the FIs first in line to bear consumers' full losses if any of the FIs' SRF duties have been breached. At the same time, MAS and IMDA consider FIs' and Telcos' SRF duties to be fundamental anti-scam duties. This is reflected through the expectation of full payouts in the event of breach.[8]

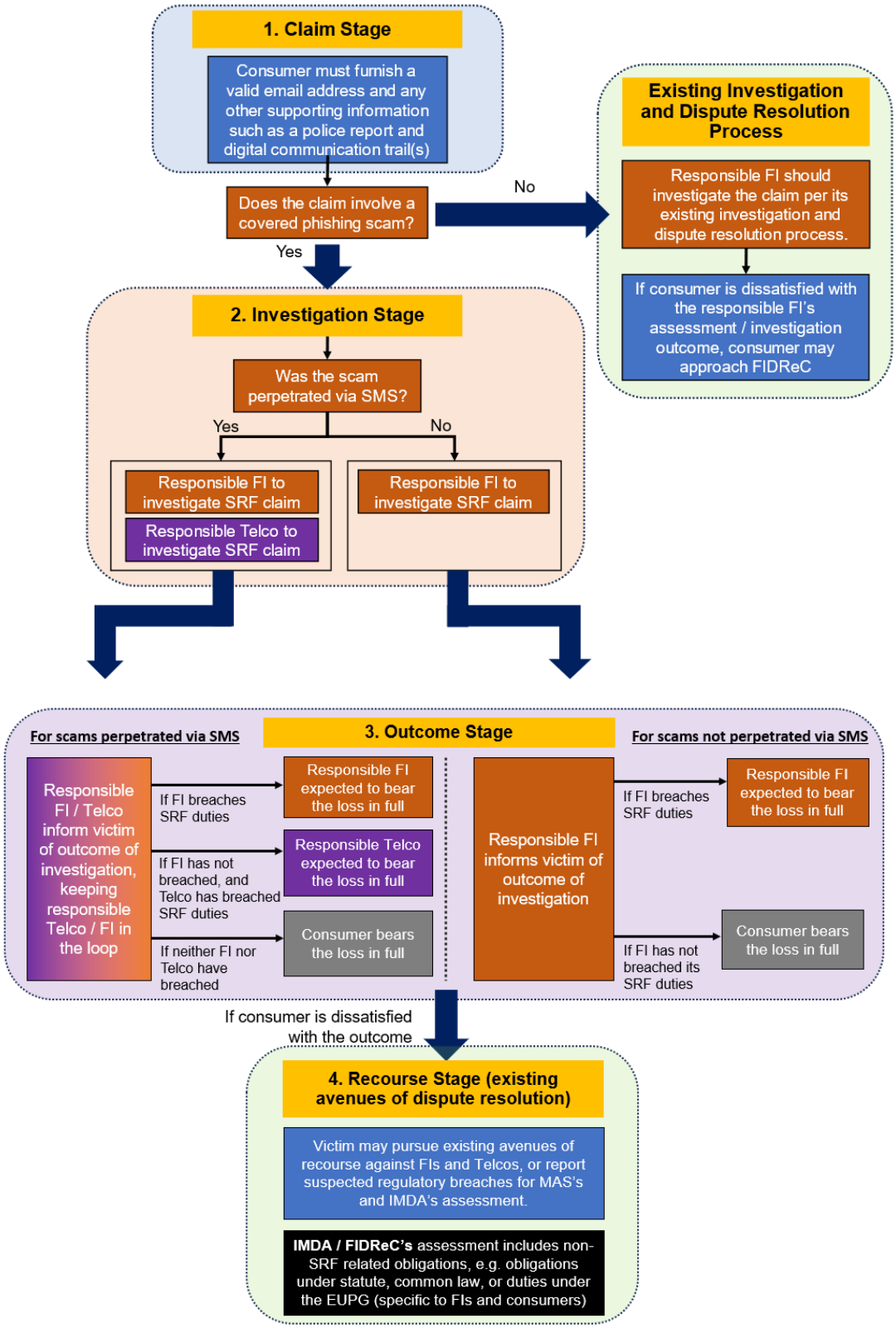
[8] Barring extraordinary events or circumstances beyond a Telco's control, which would have to be assessed on a case-by-case basis.

6. Operational Workflow for Handling Claims

Design of workflow for investigating claims

6.1. MAS and IMDA sought feedback on a four-stage operational workflow for handling claims – namely, the 'Claim Stage', 'Investigation Stage', 'Outcome Stage' and 'Recourse Stage'. Under the proposed workflow, the FI will be the primary touchpoint with the consumer, and communications will be done within a single communication chain to include the Telco where relevant. The workflow is intended to streamline the process and to avoid the need for consumers to liaise separately with the FI and Telco especially during such times of distress. Please see a summary of the operational workflow in the following **Diagram 1**.

Diagram 1: Operational Workflow for claims brought under the SRF



6.2. Respondents did not specifically comment on the various stages of the operational workflow, but generally opined that the communications between FIs and Telcos on workflow coordination should be made seamless to reduce consumer burden in times of distress. An area of focus from the public feedback received was on the importance of effective oversight by regulators, which was seen as critical to facilitate a more transparent and collaborative process in establishing workflow protocols. Some queried the criteria that MAS and IMDA will follow in determining a breach of SRF duties. One respondent suggested making internal reports by FIs and/or Telcos accessible to scam victims, regardless of whether a duty was breached, to aid victims in seeking alternative recourse channels.

6.3. Many industry respondents raised clarifications pertaining to workflow coordination matters, in particular investigation timelines and mode of communication channel. Feedback from the industry respondents is summarised below:

a) On the claims stage, industry respondents sought clarity on the specific information to be furnished by consumers in making claims under the SRF, while also highlighting the challenge in determining the accuracy of such evidence. One respondent highlighted that scam victims could be limited by their ability to provide evidence for how their information had been compromised. Relatedly, respondents emphasised the need for timely reporting of covered phishing scams to facilitate investigations under the SRF, as system logs showing the sender of the SMS are only retained for a limited period of time after the SMS is sent. There was also a suggestion for MAS to align the timeline for customers to report unauthorised transactions under the SRF with that of the E-payments User Protection Guidelines (EUPG), for consistency.

b) Respondents also sought clarity on the investigation timeframe for SRF cases, as well as the dispute resolution process should the FI and Telco be misaligned regarding the SRF case or the investigation outcome (e.g., whether the transaction falls within the scope of a covered phishing scam under the SRF).

c) Specific to the recourse stage, respondents commented on the possible inconsistent application of SRF claim processing protocols, especially if there is a lack of coordination among different stakeholders.

d) Industry respondents also weighed in on suggestions to improve the operational workflow, including setting out factors for dispute resolution bodies (e.g., FIDReC) to consider so that consumers can assess the viability of a claim before initiating the claim, as well as establishing an Ombudsman to oversee the SRF claims process and to mediate disputes between stakeholders.

Proposal for e-wallet providers to join FIDReC

6.4. Specific to the recourse stage, MAS sought feedback on the proposal for major payment institutions providing account issuance services for payment accounts that store e-money (e-wallet providers), to join FIDReC. As these institutions are currently not members of FIDReC, the intent is to similarly avail the avenue for recourse to customers of e-wallet providers, in the event of disputes.

6.5. All respondents were supportive of the proposal, except one who suggested that the existing 'Small Claims Tribunal' process could be better placed to handle disputes for phishing scams.

MAS' and IMDA's Response

6.6. MAS and IMDA take a serious view of ensuring accountability and collaboration throughout the four stages of the SRF claims process. FIs and Telcos have the primary responsibility to handle disputes and complaints, as they are consumer-facing. This entity-consumer relationship extends to all cases, beyond SRF phishing scams, and it is imperative that this responsibility is also preserved in the SRF. FIs and Telcos are ultimately answerable to MAS and IMDA, as their respective regulators.

6.7. In terms of monitoring FIs' compliance with the SRF, MAS' supervisory oversight includes the monitoring of FIs' resolution with consumers in relation to cases lodged with the FI concerning scam losses, amongst others. The purpose of this is to ensure compliance with regulations and guidelines applicable, and that consumers are treated fairly. MAS will take into account the FIs' demonstrated compliance with the prescribed duties under the SRF, as part of ongoing supervision. MAS has also set out expectations (within the Fair Dealing Guidelines) that FIs must treat customers fairly and investigate all cases of customer disputes independently. Similarly, IMDA will monitor Telcos' responses to consumers in escalated scam cases that involve breaches of Telcos' SRF duties, to have oversight of how Telcos account to these consumers. IMDA will also put in place ex-ante measures at a systemic level to monitor Telcos' compliance with their regulatory duties, which can be objectively verified.

6.8. The anti-scam duties were formulated based on the principles that they are discrete, objective, and verifiable. This underscores the clear and measurable nature of these duties, which reinforces the expectation for impartial and demonstrated actions from FIs and Telcos in fulfilling their anti-scam responsibilities within SRF.

6.9. MAS and IMDA agree with the feedback on ensuring consistent standards for determining responsibility and liability, and consumer recourse pathways. MAS agrees with the feedback to align the timeline for customers to report unauthorised transactions under the SRF (i.e. no later than 30 calendar days after

becoming aware of the seemingly authorised transaction) with that of the EUPG (i.e. 30 calendar days from when the responsible FI sends the notification alerts). This is in recognition that under the original wording, it would be operationally difficult to prove when a customer was "made aware" of the transaction. In other words, there would have been potentially no limit nor basis for audit trail on the time period for which a victim can report the case to the FI for claim assessment.

6.10. Given the cross-industry nature of handling SRF claims, coordination between FIs and Telcos requires careful consideration of operational structures and workflows. Other factors, such as consumer response time, extent of consumer evidence or records and the operational requirements for investigating potential breaches in SRF duty, may also influence this process. Additionally, FIs and Telcos will need time to investigate and assess a consumer claim under the SRF. MAS and IMDA have been in discussions with FIs and Telcos to establish appropriate timeframes for cross-industry coordination, aimed at ensuring that the processes do not impede their ability to respond to consumers and, where applicable, process payouts in a timely manner.

6.11. Arising from the public responses, MAS and IMDA have been studying refinements to the workflow in the areas below and will finalise them before commencement of the SRF:

a) **Claim Stage**

To initiate the SRF claims process, consumers are required to provide details of the phishing scam to their FI, including a valid email address and any other supporting information such as a police report and digital communication trail(s), within 3 calendar days from the date of notification to the FI. Where practicable and available, the consumer should furnish the records including the date, time, and sender of the communication with the scammer on the digital messaging platforms such as SMS, emails, and WhatsApp. This information is essential for FIs to facilitate the claims investigation process effectively.

FIs and Telcos will seek to be accommodative on the extent of communication records that are required to make an SRF claim, taking into consideration the challenges highlighted in determining the accuracy of information, and the limitations faced by scam victims in providing such information.

b) **Investigations Stage**

MAS and IMDA recognise the potential for disagreements among FIs, Telcos, and consumers during the investigations stage, such as assessments of whether a case qualifies as an in-scope phishing scam. Moreover, the assessment of an SRF case at the Telco layer will only be applicable if the

covered phishing scam was perpetrated via the SMS channel. Both regulators are in discussion with FIs and Telcos to establish internal processes for resolving such issues.

MAS and IMDA are also in discussion with FIs and Telcos on finalising the investigations protocols, whilst FIs and Telcos each conduct their investigations concurrently and independent of each other. As a general guide, FIs, and Telcos where applicable, should complete an investigation of any relevant claim within 21 business days for straightforward cases or 45 business days for complex cases. As the first and overall point of contact with the consumer, FIs may only loop Telcos into the communication chain with the consumer in specific situations, for example, to address a Telco-specific query for an SRF claim. MAS and IMDA encourage a collaborative approach between the FIs and Telcos to work within the expected timeline to respond to the consumer.

c) **Outcome Stage**

MAS and IMDA note the public feedback that the communication process should be seamless for consumers. It is our intent for all communications in relation to an SRF claim to be done within a single communication chain.

d) **Recourse Stage**

For cases which fall outside the scope of the SRF, or where entities have not breached any relevant duties, existing avenues of recourse remain available, including mediation and adjudication with FIDReC. Scam victims can also pursue civil claims against the relevant entities through the courts. Specific to the proposal for e-wallet providers to join FIDReC, MAS will proceed as consulted given that there is general consensus. This would mean that when a consumer is dissatisfied with the outcome of a e-wallet provider's assessment of his claim under the SRF, he may pursue an additional avenue of recourse through FIDReC[9].

[9] FIDReC's mediation and adjudication services, in relation to e-wallet providers that join FIDReC, will be limited to disputes involving SRF claims and other claims pertaining to the e-wallet provider's e-wallet related payment services only.

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

7.1. MAS and IMDA sought feedback on how the SRF should evolve, taking into account the changing scams landscape. Respondents generally supported maintaining a principles-based approach in the SRF to promote flexibility in addressing new scam typologies.

7.2. A common theme among all respondents was to bring more stakeholders (e.g., app developers and app stores, social media platforms) into payout frameworks like the SRF in the longer term.

7.3. A few respondents suggested for more collaboration and information sharing amongst industry players, including regular platforms for sharing intelligence and updates to scam typologies for enhanced defence.

7.4. Another key area of feedback was to enhance consumer protection efforts for vulnerable consumer segments, for example, through special accounts with higher levels of security to offer more protection for such consumers. FI industry respondents also suggested additional efforts for vulnerable consumers who, due to their personal circumstances, are especially susceptible to harm. Some respondents suggested enhancing awareness of scams among vulnerable consumers by conducting upstream digital financial literacy or cyber hygiene programs in schools, and educational programs for the elderly.

MAS and IMDA's Response

7.5. MAS and IMDA thank respondents for contributing views on how the SRF could evolve. The Government will take these views into account as it studies and considers how to enhance consumer protection for scam losses. The SRF should be seen within the context of the Government's overall approach towards consumer protection and combatting scams, which entails holding entities accountable for implementing anti-scam measures, as well as ensuring there are reasonable routes of recourse for scam victims. Combatting scams is a top priority at the Whole-of-Government level, and there is close coordination between Government agencies on anti-scam initiatives, of which the SRF is one initiative.

7.6. As presently designed, the proposed SRF imposes calibrated duties on FIs and Telcos according to their respective roles in fighting scams, while incentivising consumers to remain vigilant and not let their guard down. The broader work to address vulnerabilities beyond phishing scams continues, so that confidence in digital banking and payments in Singapore can be preserved. For cases which fall outside

the scope of the SRF, other measures will be used to hold entities accountable and to provide avenues of recourse for scam victims (as elaborated in para 1.2).

7.7. The Government has partnered with industry to put in place robust upstream and downstream anti-scam measures, and will continue to work on strengthening these measures. Ultimately, the best defence against scams is a vigilant and discerning public – this is why public education remains a critical part of our anti-scams strategy. For example, in schools, students are taught to guard against scams through various subjects and resources, including Character and Citizenship Education classes which teach them to evaluate and verify the credibility of online information sources, and to recognise and report different types of online scams. To better support vulnerable groups such as the elderly, the Government works with partners to roll out targeted programmes – for example, the Police works with Silver Generation Ambassadors to educate the elderly on scams. The Government has also recently consolidated anti-scam resources into a one-stop portal, the ScamShield Suite, which aims to enable members of the public to better protect themselves against scams by equipping them with anti-scam resources. This was launched on 27 September 2024, comprising four anti-scam resources - the ScamShield helpline, ScamShield app, ScamShield website and ScamShield Alert social channels.

7.8. The Government is resolute in its commitment to fighting scams and works closely with the public and industry to promote resilience and vigilance in protecting against scams. Given the fast-evolving scams landscape, the Government will continue to study and work towards enhancing the overall suite of consumer protection measures, both in terms of accountability and recourse.

8. Others

Eligible Claims

8.1. With reference to the defined scope of phishing scams, several FI industry respondents sought clarity on the following:

a) Whether instances of phishing scams enabled by Rich Communication Services ("RCS")[10], which is a communication protocol that offers enhanced messaging features beyond traditional SMS, would fall in scope of the SRF;

b) If the SRF applies to corporate customers of FIs;

c) Whether customers of responsible FIs who are foreign residents and receiving the services overseas would be within the scope of the SRF; and

d) Whether scam losses that arise from pre-paid/debit cards issued by PSPs would fall into the scope of the SRF.

"Protected account" definition

8.2. One respondent suggested for the definition of "protected account" to be amended to any payment account that is capable of having a balance of more than $1,000 (from current $500), to align with the threshold of "small personal payment account" in the Payment Services Act.

MAS' and IMDA's Response

8.3. MAS and IMDA would like to clarify the following regarding eligible claims under the SRF:

a) The SRF duties apply in relation to phishing scams enabled by digital messaging platforms, specifically where the scammer impersonates a legitimate entity and makes use of such a platform to correspond with the account user. Digital messaging platforms include, but are not limited to, RCS messages, email, and WhatsApp. MAS notes that some FIs do utilise RCS to communicate with

[10] RCS is available via Google SMS App, which comes preloaded on most Android phones. Apple introduced support for RCS on iPhones in September 2024.

their customers and would like to clarify that RCS is in-scope of the SRF for FIs. However, Telcos' SRF duties do not apply to messages delivered by RCS because RCS is a service provided by Google over the internet and not via the Telcos' SMS channels.

b) The SRF does not apply to corporate customers.

c) The SRF will apply to all customers of FIs in Singapore. Customers of FIs who are foreign residents, and who receive the FIs' services overseas, would fall within the scope of the SRF.

In relation to the Telco layer, the SRF does not apply to subscribers who use mobile services provided by non-local Telcos, e.g., Telcos' subscribers travelling overseas and who use SIM cards or eSIM from overseas telco operators.

d) 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. As such, the liability apportionment under the SRF does not apply to transactions on credit cards, charge cards, and debit cards issued in Singapore.

8.4. In relation to the definition of a "protected account", MAS will align with the threshold of "small personal payment account" in the Payment Services Act such that PSPs providing e-wallets that do not have the capability of having an e-money balance of more than $1,000 will not be scoped into the SRF. From an anti-scams perspective, efforts would be better focused on accounts that are capable of holding balances more than $1,000. Likewise, accounts that are not capable of holding balances more than $1,000 are excluded from specific requirements under the Payment Services Act.

Annex A

List of respondents to the consultation paper on Shared Responsibility Framework

*Note: Respondents who requested confidentiality of submission are marked with a **

1. Andrew Chow, personal capacity
2. Ang
3. Beeconomic Singapore Pte. Ltd.
4. Ben Chester Cheong
5. Daniel
6. Dr Sandra Booysen, Centre for Banking & Finance Law, National University of Singapore
7. FlexM Pte. Ltd.
8. Gabriel Cheng
9. GSMA
10. Hardik Thaker
11. Kelvin Tan
12. Law reform committee, Singapore Academy of Law
13. Lawrence Tang
14. LSL Boey
15. M1 Limited

16. Mr Tim Goodchild
17. MyRepublic Group Limited
18. Network for Electronic Transfers (Singapore) Pte Ltd
19. PwC
20. Securities Association of Singapore*
21. Shannon Lim
22. Shean Yeo
23. SIMBA Telecom Pte. Ltd.
24. SingCash Pte Ltd
25. Singtel Mobile Singapore Pte Ltd
26. StarHub Ltd ("StarHub"), on behalf of the StarHub Group.
27. Sylvia Lim (Personal Capacity)
28. Tan Eng Teck
29. Tan Geok Lan
30. Tanla Platforms Limited
31. Trust Bank Singapore Limited*
32. You Technologies Group (Singapore) Pte Ltd

Twenty-four respondents have requested confidentiality of identity.

Sixteen respondents have requested both confidentiality of identity and submission.

Please refer to Annex B for the submissions, which are published separately.

Annex B – refer to separate attachment

Submissions from Respondents to Consultation Paper on Shared Responsibility Framework

Annex C

IMDA's Response to Suggested Measures for Telcos

1. The list below provides an overview of the measures which were suggested by the public in relation to the SMS channel which is under the scope of the SRF:

    a) **Deploy AI to detect malicious SMS and URLs:** This suggestion was made by some public respondents. Telcos have already implemented systems that analyse and filter out scam SMS based on patterns and rules. These systems use machine learning to learn and improve the analytic capability in identifying scam SMS. Telcos use such systems to supplement filters that identify scam SMS based on known malicious URLs.

    b) **Remove URLs from SMS messages by default:** This suggestion was made by one public respondent. The concern that URLs in SMS increases the risk of phishing is acknowledged. Banks in Singapore are phasing out clickable links in SMS to enhance digital banking security. If Government agencies send clickable links in SMS, they will ensure that the URLs end with ".gov.sg". The Government will study the use of URLs in other sectors and work with sector partners to make adjustments if necessary.

    c) **Provide single platform for reporting scam SMS and calls to Telcos:** Some respondents opined that a central repository should be made accessible for public to report scams. Consumers who encounter a suspected scam incident or would like to share scam-related information should file a police report or call the Anti-Scam Hotline.

2. IMDA acknowledges other suggested measures such as whitelisting all government entities' phone numbers and making caller ID a free service. However, these measures relate to other call-related risk

surfaces and fall outside of the scope of SRF. Many of these suggested measures have also been implemented. For completeness, IMDA sets out these suggestions and our responses below.

a) **Limit the sale of prepaid and postpaid SIM cards:** One public respondent suggested that the sale of SIM cards should be limited to specific "geographical district".

IMDA's Response: Mobile service providers have the commercial and operational flexibility to determine the location of their retail shops to better serve their customers. However, to prevent fraudulent registration of mobile services, IMDA requires all mobile service providers to comply with stringent SIM card registration requirements. These requirements include limits on the number of SIM cards that any individual can register. Since 2014, each individual is only allowed to register a maximum of 3 prepaid SIM cards. From 15 April 2024, a limit of 10 postpaid SIM cards per individual was imposed. IMDA will continue to work with mobile service providers to tighten the SIM card registration process and prevent fraudulent registration of SIM cards.

b) **Block robocalls and international calls:** One public respondent suggested that Telcos should provide "more features and functions to be able to block calls".

IMDA's Response: IMDA has been working with the Telcos to systemically reduce scam calls coming through the telecommunications networks. Since 2020, Telcos have taken measures at the network level to identify and block robocalls using pattern recognition technology. Since 2022, Telcos have rolled out wholesale blocking of all overseas calls that bear any Singapore fixed line or mobile line numbers, while catering for legitimate use such as inbound and outbound roamers. In January 2024, Telcos have also offered the feature for mobile subscribers to block calls from international numbers.

c) **Provide anti-virus/anti-scam/anti-phishing software as baseline service:** One public respondent suggested that Telcos, which are also Internet Service Providers, should provide such a form of software to protect consumers against scams that may not involve SMS.

IMDA's Response: Telcos in Singapore offer mobile security software as a service to safeguard consumers against increasingly sophisticated cyber threats. Some of the Telcos also bundle antivirus software with mobile phone plans by default. Consumers may wish to check in with the respective Telcos for details.

Monetary Authority of Singapore

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

Annex D

[SRF Duties of Responsible FIs and Responsible Telcos]

FI Duty #1: Impose a 12-hour cooling off period upon activation of digital security token during which 'high-risk'[11] activities cannot be performed

This duty requires the FI to put in place a 12-hour cooling period upon activation of digital security token, during which no 'high-risk activities' can be performed. The equivalent duty applies in the context of accounts issued by relevant payment service providers when there is login on a new device. This additional friction to the process increases the chance that consumers can discover unusual activities on their account.

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

This duty requires the FI to provide notification alerts on a real-time basis, which will help alert consumers to high-risk activity that may not have been authorised by the consumer. The equivalent duty applies in the context of accounts issued by relevant payment service providers when there is a login on a new device, or during the conduct of high-risk activities. 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) on a real-time basis

This duty requires the FI to provide real-time outgoing transaction notifications, which are essential in prompting consumers to react when there are unauthorised transactions (e.g., immediately reporting to the FI), and enables the 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

This duty requires the FI to provide a reporting channel. It 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.

[11] 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.

[New] FI Duty #5: Put in place real-time fraud surveillance directed at detecting unauthorised transactions in a phishing scam that results in an account being rapidly drained of a material sum to a scammer

This duty requires the FI to detect if a customer's account is being rapidly drained of a material sum to a scammer(s) for an unauthorised transaction in a phishing scam. In such scenarios, FIs must either block the transaction until it is able to reach the customer for positive confirmation, or send a notification to the customer and block or hold the transaction for 24 hours.

Telco Duty #1: Connect only to authorised aggregators for delivery of Sender ID SMS

This duty requires a responsible Telco to only deliver, to subscribers, Sender ID SMS which is received from authorised aggregators. Authorised aggregators are aggregators which are licensed by IMDA to send SMS that bears a Sender ID with an alphanumeric sender ID registered with the Singapore SMS Sender ID Registry (SSIR). The purpose of this duty is to ensure that subscribers only receive SMS which originate from bona fide senders registered with the SSIR. 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

This duty requires a responsible Telco to block Sender ID SMS which it receives from sources other than authorised aggregators. This prevents subscribers from receiving Sender ID SMS from all other channels, including unauthorised or unknown networks connected through overseas network operators. The purpose of this duty is to prevent delivery of Sender ID SMS originating from unauthorised SMS networks, thereby further reducing the risks of Sender ID spoofing.

Telco Duty #3: Implement an anti-scam filter over SMS to block SMS containing malicious URL in designated database

This duty requires a responsible Telco to implement an anti-scam filter for all SMS that pass through its network, where the SMS will be scanned to determine if it contains any URL that matches that of a known malicious URL in a designated database. The anti-scam filter is required to be implemented for all SMS, regardless of whether the SMS originates locally or from overseas. This duty covers both Sender ID SMS and SMS carrying either local or overseas telephone numbers. The purpose of this duty is to further mitigate against the risks of scam SMS that may pass through mobile networks in Singapore.