Annex B

Submissions from Respondents to Consultation Paper on Shared Responsibility Framework

Note: The table below only includes submissions for which respondents did not request confidentiality of submissions. Twenty-four respondents have requested confidentiality of identity with their submissions.

S/N	Respondent	Responses from respondent
1	Andrew Chow	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** 4.4. However, the SRF will exclude: (c) Unauthorised transaction scam variants that do not involve phishing (e.g., hacking, identity theft, malware-enabled variants)." It is the author's view that such variants should be included in the SRF if the fraud & scams gateway involve digital processes. Please refer to the attached submissions. While phishing scams remain a common and well-used typology, any new framework should stay flexible and relevant to new typologies which arise. Criminals are highly creative, and tend to remain ahead of law enforcement as their overriding motive is to be as highly profitable as soon as possible. If the SRF is limited to only phishing scams, it may become irrelevant in the future given how quickly new typologies arise. Instead, it is suggested that the SRF could focus on methodology, where the gateway or delivery of the scam is via digital means or platforms. For example, the authorities could introduce the use of "fraudulent digital platform" in conjunction with "fabricated digital platform" in the Draft SRF Guidelines to include e-commerce scams with malicious links and embedded malware. This would establish a limited expansion to the SRF. Android phone takeovers have become extremely prevalent and have resulted in large losses for consumers in Singapore.

S/N	Respondent	Responses from respondent
		"Seemingly authorized transaction" would also require consequential amendments, which could, and should apply to malware phone takeover schemes as the consumer has not authorized the transaction. This enlarged definition will still exclude the "true" consent typologies, such as love or job scams, which may require different solutions. "unauthorised transaction" in relation to any protected account, means any payment transaction initiated by any person without the actual or imputed knowledge and implied or express consent of an account user of the protected account. The SRF should remain consistent with the EUPG. <u>Scope of SRF – Entities</u> It is gratifying to note that the Singapore government takes fraud and scams seriously and have included Telcos in the scope of the SRF, which is novel in nature. However, while the author understands the legal issues relating to the regulation and oversight of social media and e-commerce companies in Singapore, it is suggested that they should be included in the SRF. If the SRF is issued as a guideline downstream of the OCHA, it may be possible to compel such companies to be included in the SRF, or to volunteer to be included, especially given the findings in the TSR, where certain online marketplaces do not implement suggested controls. Please refer to the seminal work undertaken by the UK Home Office in establishing the UK Charter. The signatories include Amazon, eBay, Facebook, TikTok, amongst other tech luminaries, which suggests that such companies are now willing to participate in the fight against fraud and scams."
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** To include social media and e-commence companies.
		Question 6. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility.** To include the typologies referred to by the author in the response to Q1. To exclude Vulnerable Persons in the first instance. In the author's view, it is absolutely essential to protect VPs, given the challenges faced by such persons who have their life savings stolen.

S/N	Respondent	Responses from respondent
		The broad definition of a VP should include a person who is no longer able to generate income to support him or herself in a material way, due to specified issues, such as old age, disability (mental and physical), and/or special needs. The ABS Guidelines already describe processes to identify persons with mental incapacity. If the lost monetary assets are the only source of income for that individual, it is proposed that under the SRF, they should be refunded 100% without the need for a waterfall approach in the first instance, subject to a cap and to certain contractual requirements, such as: • The exclusive use of specified web browsers with built-in anti-fraud filters; • The exclusive use of specified App stores, which vets Apps for malware; • The exclusive use of static IP addresses, with assistance from the internet service provider. If the VP fails to implement such requirements, it is proposed that any subsequent claims (i.e. under new typologies using digital means) under the SRF will be denied, or to fall within the claims outside of the VP category in the waterfall process. This would be a practical means to compel VPs to protect themselves and prevent the spoofing of VPs by fraudsters.
		Question 7. MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper. Agree, subject to the author's responses to Q1., Q2, & Q3. above.
		Question 9. **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.** Agree, subject to the author's responses to Q1., Q2, & Q3. above. Major payment institutions (and other suggested institutions) should be compelled to be part of the processes in the SRF.
2	Ang	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** 4.4(b) should be included in the SRF. If people could be phished into entering account details into websites, what's the difference if it's text or face-to-face? Also,

S/N	Respondent	Responses from respondent
		investigations of phishing scams have shown that it can be multi-stage to induce users to enter their OTP separately into phishing websites after getting their credentials, and not including this in the coverage limits the effectiveness of the framework and users getting 100% of the blame. Also, banks have not implemented features that would make them more phishing resilient, e.g. FIDO2/U2F authentication standards to make them more resilient against reverse proxy phishing, so in this regard, there's still quite a lot to do by the banks to improve the security of authentication before shifting the blame to users. Lastly, it's unclear and unknown if banks implement suspicious login detection to determine if a login is suspicious, and therefore, require additional authentication, sometimes even another authentication method to lock scammers out. This is common in cloud services like Microsoft 365, and is mandated by HKMA by 2024. Investigations into scams show that some scams could have been averted if users are alerted of suspicious logins, but this is currently not in place for various reasons. The compromise of 12 hours or more wait before risky transactions can happen can only mitigate so much, and it's not a very long wait either. This is hardly a deterrence and until banks implement more holistic approaches, protection and detection, banks should take on 100% of the responsibility in SRF whenever phishing occurs. Only when all of those have been implemented, then the SRF could be tweaked to shift the responsibility towards users.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** Based on Annex A, the following case studies are relevant: - Case Study 2 --> Please see Question 4 answers. Banks should be responsible as there is insufficient security by banks. - Case Study 3 --> The case study isn't very realistic as it's lacking certain steps for that to happen. And even if it does happen in real life, it happened because there's insufficient measures. For example, when the scammer

S/N	Respondent	Responses from respondent
		takes over the account to transfer $10,000, there is a possible lag of at least 12 hours based on current regulations. That's hardly a deterrent and so long as I'm patient enough, I would be able to do it. Two, if assuming that's a reverse proxy phishing page (albeit one that's not obvious), me, as an attacker would be able to perform such transactions in real time. Banks do not have sufficient protection against that. Taken altogether, it doesn't seem like banks have implemented the necessary anti-scam measures to absolve themselves of the blame, and therefore, banks should be 100% responsible for the losses instead. It would be more preferable that users take on 10% to 50% of the responsibility for not checking if the prices are reasonable or if the seller is known, but as the framework appears to be rather rigid, it is unfortunate that banks will take on 100% of the responsibility instead. - Case Study 5 --> Banks should alert all outgoing financial transactions, and even if the user did set a threshold before notification, the user should only bear the threshold losses (i.e. $1500 in this case). The rest of the losses should be borne by the banks. Reasoning please see Case Study 2 & 3 as well as Question 4 answer. - Case Study 6 --> Fair enough that the banks will be 100% responsible for the losses as notifications did not come in time and the user isn't able to take further actions to stop those malicious transactions. And it should be noted that again, there are insufficient measures when new digital security token is being activated. 12 hours wait before risky transactions are made is merely a stop gap measure. This could have been avoided if FIDO2 authentication standard is used and the phishing wouldn't even be successful in the first place. - Case Study 7 --> Fair enough, although user should have borne 10% to 50% of the responsibility for not taking actions on the notification. - Case Study 8 --> It's unclear how realistic this could be, mainly because bank accounts are protected by 2FA. Disregarding the possibility of that, it is fair that the banks are responsible for it, although user should have borne 10% to 50% of the responsibility for not checking if the link. - Case Study 9 --> While it's unclear how the user had missed the earlier 9 notifications, but given that the user

S/N	Respondent	Responses from respondent
		checked his monthly statement and alerted the bank, the user had performed his part. In line with Objective (i) of preserving confidence in digital payments and digital banking in Singapore, it is certainly nice that banks take on 100% of the responsibility despite missing to send out the 10th notification. - Case Study 12 --> Based on the reasoning of Case Study 3, banks should have borne 100% of the responsibility. However, it would be more preferable if that is split between the banks, telcos and users as each of them has failed in their own respective area of responsibility. Unsure how the split should be, but I would think banks should take on 80% of that responsibility, 10% by the telcos, and 10% by the users. - Case Study 13 --> See Case Study 12 - Case Study 14 --> See Case Study 12 - Case Study 15 --> See Case Study 3"
		Question 6. IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper. Based on Annex A, the following case studies are relevant: - Case Study 10 --> Disagree with the assessment that the user did not take due care by clicking on the link. In the first place, users rely on various cues (e.g. Likely-SCAM) label to determine if a link should be clicked. Secondly, phishers are known to use shortened URLs to hide the phishing URL, further complicating the matter for users who are deciding if they should click, and if they click to check if the URL is legitimate, they could still make a mistake as phishing websites and domains could be so legitimate looking that they may mistake it for the real website. Also, this is complicated by free SSL certificates, for users who will check the SSL certificates. The onus would be to create a whole-of-Singapore scanning solution, in which all links are scanned, and where possible, warn users that those are not the legitimate banks' websites. Anyway, back to topic. While the telco has failed to connect to an authorized aggregator, the bank has also failed in detecting suspicious transactions, and therefore, the losses should be shared equally between the telco and bank. - Case Study 11 --> See Case Study 10 - Case Study 12 --> Based on the reasoning of Case Study 3, banks should have borne 100% of the responsibility. However, it would be more preferable if that is split between the banks, telcos and users as each of them has

S/N	Respondent	Responses from respondent
		failed in their own respective area of responsibility. Unsure how the split should be, but I would think banks should take on 80% of that responsibility, 10% by the telcos, and 10% by the users. - Case Study 13 --> See Case Study 10 - Case Study 14 --> See Case Study 10
		Question 7. MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper. The waterfall approach is rigid and doesn't meet the objectives (ii) and (iii), particularly in setting out the responsibilities to be borne by each party. It results in a very lopsided losses bearing outcome when there are clear lapses by each of the party.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** If cybersecurity measures improve to tackle the threats (e.g. a whole-of-Singapore scanning URL solution, implementing more phishing resilient authentication, implementing stronger authentication to avoid the issues of digital token activation, better countermeasures against suspicious outgoing transactions), then it makes sense that the SRF should start shifting some of the responsibilities towards users. However, if it remains as bad as now, banks need to continue to shoulder the losses instead of blaming users for falling for scams. Humans will fall for scams at some point, even for security professionals who may check everything. The framework should ideally drive everyone to be more security conscious and implement better measures and sensible compromise without users having to lose their entire life savings.
3	Beeconomic Singapore Pte. Ltd.	**Question 4. MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** We recommend the “protected account” definition - where references are made for relevant payment service providers - to be amended so that the threshold of the currency equivalent of the e-money within the account is $1,000 instead of $500 so as to align with the “small personal payment account” definition in S24(5) of the Payment Services Act which had already considered what

S/N	Respondent	Responses from respondent
		is the amount regarded as "small" and therefore excluded from specific requirements. Given the cost of compliance (example joining FIDReC and being subject to FIDReC processes) aligning the thresholds will ensure requirements are risk-based – applicable for payment accounts which are larger and more likely to be targeted for phishing. This will also better ensure consistency, and ease of implementation.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** The proposed EUPG and SRFG state that a 24/7 reporting channel should be made available for all consumers to reach out on unauthorised transactions. We will suggest that an industry association led channel be in place to represent MPIs so that escalations outside business hours can accordingly be cascaded to relevant parties given that the number of such transactions for MPIs will likely be significantly lower than that affecting banks, and it will be very operationally costly for each MPI to maintain a reporting channel 24/7.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** The proposed SRFG states that the responsible FI is first in place, as it is the "custodian of the client's money", to assume all liabilities if any of its duties have been breached, and the telecommunication operator ("Telco") is second in place, as it has a secondary supporting role, to assume all liabilities if the FI has fulfilled all its liabilities but the Telco has not. Given that countering phishing scams is a responsibility of all entities – there should not be a distinction between "primary" and "secondary" roles. In the event that the Telco has not discharged its duty, it should be proportionately liable for the losses this lapse caused and it should not be only after the FI was assessed to have discharged all its duties. In other words if both FI and Telco had not discharged their duties they should be proportionally liable. This will encourage all entities including the Telco to play their part as a first priority. The roles of Telco should not be downplayed.
4	Ben Chester Chong	**Question 5.** **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.**

S/N	Respondent	Responses from respondent
		The proposed duties for FIs are commendable, laying a solid foundation for robust security practices. I believe FIs could further enhance their anti-scam efforts by implementing advanced risk-based authentication systems that adapt to individual user behavior and patterns. This would provide a more personalized and dynamic layer of protection compared to a static 12-hour cooling-off period. Additionally, FIs could proactively educate their customers about emerging phishing scams and best practices for safeguarding their financial information. This could include interactive workshops, targeted email campaigns, and readily accessible online resources.
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** The proposed duties for Telcos are crucial for combating SMS-based phishing. To further strengthen their defenses, Telcos could explore implementing AI-powered solutions that analyse SMS content and sender information in real-time to identify and block suspicious messages before they reach users. Additionally, Telcos could partner with FIs and the authorities to establish a secure platform for sharing intelligence on emerging threats and phishing tactics. This collaborative approach would enable comprehensive and proactive defence against evolving scams.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** The waterfall approach provides a clear framework for assigning responsibility and ensuring compensation for victims. To further enhance fairness and transparency, the framework could be expanded to include specific criteria for assessing each party's contribution to the scam, considering factors beyond just negligence. This would provide a more nuanced and equitable approach to compensation. Additionally, the framework could be strengthened by establishing a dedicated ombudsman service to oversee the claims process and mediate disputes between stakeholders. This independent body could ensure impartial and efficient resolution of claims, fostering trust and confidence in the SRF.
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the**

S/N	Respondent	Responses from respondent
		Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper. The outlined operational workflow provides a valuable starting point. However, to improve accessibility and user experience, the claim filing process could be made more user-friendly. This could involve developing a multilingual online platform with interactive guidance and simplified forms. Additionally, providing dedicated customer support for claim inquiries would greatly assist users navigating the process.
		Question 9. **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.** Including major payment institutions in FIDReC is a positive step towards a more comprehensive and inclusive anti-fraud ecosystem. To further enhance its effectiveness, FIDReC could develop standardised best practices and security protocols specifically tailored to the needs of payment institutions. This would provide valuable guidance and ensure consistency across the sector. Additionally, FIDReC could establish a knowledge-sharing platform where member institutions can collaborate, share information on emerging threats, and learn from each other's experiences. This collaborative approach would foster innovation and accelerate the development of effective anti-fraud solutions.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** Regular review and adaptation of the SRF are crucial to maintain its effectiveness in the face of evolving scams. To ensure this process is comprehensive and informed, a dedicated advisory committee could be established. This committee could comprise representatives from FIs, Telcos, consumer groups, and cybersecurity experts, offering valuable insights and expertise to guide the SRF's evolution. Additionally, the SRF could leverage data analytics and machine learning to identify emerging trends and patterns in phishing activity. This proactive approach would enable the framework to anticipate future threats and adapt its defences, accordingly, ensuring its continued effectiveness in protecting consumers.
5	Daniel	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.**

S/N	Respondent	Responses from respondent
		Generally agree with most parts of the scope except for section 4.4(c) and 4.5 whereby scams of unauthorised transactions are left excluded. Victims of such scams typically fall prey not due to faults of their own actions. Hacking, identity theft, malware-enabled variants etc. are sometimes committed by highly sophisticated organisations. An average consumer may not be tech-savvy enough nor have the resources to protect themselves from such scams. Leaving these out of scope could leave the consumers without adequate recourse to recover what are lost due to faults not of their own actions. Perhaps a cap or a limit could be put in place to limit the individuals' losses if the authorities are not ready to tackle such evolving issue.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** Section 5.7 I understand that banks' typically have 24/7 hotline to report stolen cards, fraud transactions etc. However, I am not aware that there is a time limit set by MAS whereby the calls have to be picked up and responded to within a certain time frame. Such limits/SLAs should be put in place and be made aware to the public so that the victims have recourse should the FIs fail to fulfil their obligations.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** The "waterfall" approach is fair in my opinion if the scope of SRF is expanded to cover unauthorised transactions which are of no own fault of the victims. Refer to my comments in 4 above. The consumer is left to bear the brunt of the scam if neither the FI nor the Telco are not found the be at fault based on the proposed "waterfall" approach.
		Question 8. MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper. The details of the investigation, including all relevant reports to the case (including internal reports of the FI/Telco/IMDA/MAS/FIDReC) should be made available to the victim if the FI / Telco chooses not to fully compensate the victim. This is important to facilitate the

S/N	Respondent	Responses from respondent
		victim to seek recourse via the appropriate channel legal or otherwise should he/she choose to do so.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** There seem to be multiple instances whereby consumers are expected to bear the losses based on the proposed SRF. See examples below: Annex A Case Study 2: a) I disagree that it does not have a digital nexus. The 9 unauthorised transaction carried out would likely involve so form of electronic/internet banking. As mentioned in the case, these transactions were carried out during the night which is likely the time when Consumer B is asleep. Even if SMS notifications were sent to Consumer B, he/she may not have the opportunity to react. Even if it is assessed under the SRF, the loss will still likely be borne by the consumer based on the proposed framework. It just goes to show the inadequacies of the SRF in addressing such scams. <u>Annex A Case Study 3:</u> I disagree with the assessment that it does not have a Singapore nexus. Refer to section 4.2. whereby it states that ""The impersonated entities should be Singapore based, or based overseas and offer their services to Singapore residents"". An average consumer cannot be expect to do due-diligence on simple consumer transaction to determine if the impersonated entity is ""legitimate"". Are they expected to do company search with foreign company registrar (ACRA equivalent) prior to transaction? Or are sellers expected to provide their entity establishment documents or certificate of incumbency to consumers? How would an average consumer know if the impersonated entity was known to offer services to Singapore Residents? Is the business expected to have 10,000 Google or Amazon reviews from Singapore Residents? How would new businesses be able to compete if such an interpretation is taken? It is also highly unfair and skewed against the consumers if such an interpretation is taken. <u>Annex A Case Study 4:</u> I have a similar experience to what is mentioned in case study 4. I had purchase a DJI gimbal. In order to use the gimbal, I have to sideload the DJI MIMO app as it is not

S/N	Respondent	Responses from respondent
		made available via official app stores. In this scenario, if malware has somehow entered my device, does that mean that I am not protected and will have to bear 100% of the loss? The proposed SRF is inadequate or minimal at best. Based on my observations, most FIs and Telcos already have put in place the measures mentioned in the consultation paper. Yet the current measures are inadequate to address the current scams landscape. The proposed framework seem to limit the liabilities of and protect the FIs and Telcos much more than it protect the consumers. An apportionment framework should be put in place whereby FIs, Telcos and consumers have all fulfilled their responsibilities. Furthermore, it is my observation that most of these scams are typically conducted through some form of eBanking/internet banking transactions. eBanking/internet was not prevalent till recent times. In the past 10-20 years, the financial industry have been trying hard to push consumers to adopt usage such technologies thereby reducing the need for physical branches and manpower to handle transactions manually. Such cost savings are not passed on to the consumers, yet consumers are expecting to brunt loss of such scams as a result of increase adoption and usage of eBanking/internet banking technologies. How is this fair to the average consumers?
6	Dr Sandra Booysen, Centre for Banking & Finance Law, National University of Singapore	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** Scope of Section 4: Since there are many scams that don't fit the profile of 'phishing' scams, I think that a more holistic approach is needed and that payment service providers should be expected to do more to protect the public from payment fraud generally. Payers must be educated on what they can do to minimise payment fraud but there are limits to what can be expected from the general public. The avenues of recourse identified in para 4.6 offer little comfort to a victim of non-phishing scams. The definition of an 'unauthorised' payment is also problematic, and making the distinction between authorised and unauthorised payments is difficult because of the contract terms used by banks to expand the concept of 'authorised' payments. See eg Major Shipping & Trading Inc v Standard Chartered Bank (Singapore) Ltd [2018] SGHC 4, where an 'Instruction' was

S/N	Respondent	Responses from respondent
		very widely defined as an instruction that the bank believes in good faith to emanate from the customer. If one looks at the definition of 'unauthorised transaction' in the E-PAYMENTS USER PROTECTION GUIDELINES, it is 'any payment transaction initiated by any person without the actual or imputed knowledge and implied or express consent of an account user of the protected account'. It is unclear when a payer will be 'imputed' with knowledge or be considered to have given 'implied consent' to the payment.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** The 'waterfall' approach is fault-based, with fault being narrowly construed in terms of quite specific duties on FIs and Telcos. These measures will no doubt assist to reduce phishing scams but as noted above, the avenues of recourse referred to in para 6.1(c) offer little comfort to victims. This approach contrasts with the UK approach for APP scams which requires no-fault reimbursement of consumer victims. The UK approach does carry moral hazard but the FCA considers that banks can and should do more to protect consumers through their systems and procedures. A less extreme approach would be for liability to fall on the service providers unless the customer is at fault, with an indication of what will constitute fault for these purposes. It should not penalise customers for falling for plausible scams such as those seen in the OCBC incident.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** The Framework needs to be agile to respond to the evolving landscape, and it should be possible for the duties on FIs and Telcos to be supplemented with relative ease in response to identified loopholes. More detailed data on payment fraud in Singapore should be publicly available to enable those with research interests in the area are able to access the data. More detailed data on the utility of Fidrec as a financial dispute resolution forum should also be publicly available to facilitate research objectives.
7	FlexM Pte. Ltd.	**Question 5.**

S/N	Respondent	Responses from respondent
		MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper. We suggest segregating types of activities that require or do not require cooling off period. As a standard industry practice even genuine customers add beneficiary information at the time of doing the transaction. Cooling off period of 12 hours should be applicable for Changing contact number, Changing Address, Changing Email, Increase transaction limit. However, for other high-risk activities such as adding new beneficiary using MFA or Singpass authentication or shorter cooling off period like 1 hour- instead of 12 hr would be helpful.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** In a scenario where one MPI A provides White labelled eWallet services to another MPI B via APIs, the user journey and the front end (App / Website) is controlled by MPI B. Since MPI A's wallet services is embedded on MPI B's Mobile App / WebApp, MPI A does not have control over notifications and Kill switch being provided by MPI B to the end users. While MPI A may provide guidelines and contractual obligations to MPI B, it is difficult for MPI A to monitor if MPI B follows all the guidelines as defined in EUPG and SRF guidelines. Which of the financial entities (MPI A or MPI B) will be responsible for absorbing the loss, in case of breach in guidelines, in this scenario.
8	Gabriel Cheng	**Question 6.** **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** To allow public to reach out to a single platform to report on scammers. Based on my experience as a IT Security Operation for Resorts World Sentosa, my organisation had 3 Singapore numbers SMS-ing general public impersonating RWS to install dangerous android app. Even after police reports, these 3 numbers still exist today and had taken another identity for scamming. However, as phone number is only a gateway to instant messaging applications, there must also have a channel and playback for telco to these companies to complete a takedown.
9	GSMA	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.**

S/N	Respondent	Responses from respondent
		The GSMA appreciates the opportunity to respond to the joint proposal by the Monetary Authority of Singapore (MAS) and Infocom Media Development Authority (IMDA) on a new Shared Responsibility Framework (SRF). The growth of the digital market in Singapore will continue to flourish with the right regulatory frameworks and mechanisms in place to protect consumers and their privacy, while promoting innovation. For the GSMA and its members, privacy, safety and security are paramount to maintaining consumer trust in mobile services. The mobile industry continues to work tirelessly to educate its customers and looks to government institutions and public authorities to support the adoption of cost-effective security enablers in order to both establish best practice and preserve trust, security and resilience. The GSMA fully supports the intentions and aims of the proposed SRF, but the GSMA would like to express its concern over the intention to hold mobile operators financially liable. First, Phishing in general is widespread and problematic across many different platforms and services, including email, search engines and social media. By limiting the scope of the proposed SRF to SMS Phishing, the mobile operators are being unfairly targeted, and citizens of Singapore will remain unprotected from the wider Phishing scams. Second, mobile operators are infrastructure providers giving access to the communication network through which SMS is transmitted. This is the principle of mere conduit. The operators do not generate or see the content of SMS, nor do they have control over it, and should therefore not be held responsible.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** We request that IMDA carefully considers the negative impact that the proposed framework will have on mobile operators, weigh up benefits of the proposal, and decide if they outweigh the costs of compliance. Implementing the framework in its current state would require a substantial amount of time and resource to implement for a solution that will not fully address the issues and safeguard Singapore's citizens. The GSMA believes that it would be beneficial to allow more time to monitor the effect of the Full SMS Sender ID Registry Regime (SSIR) which came into force on 31 January. There are also a number of global services that

S/N	Respondent	Responses from respondent
		the Singapore operators are able to access, provided by the GSMA to help mitigate fraud and reduce the impact on citizens and customers. This includes the GSMA's Fraud and Security Group (FASG) which drives the industry's management of fraud and security matters related to mobile technology, networks and services. The T-ISAC3 service provides members with a variety of opportunities to engage with industry experts as well as hosting solutions to support secure intelligence sharing. It provides an open and trusted environment within which fraud, security and incident details can be discussed in a timely and responsible way and where members share what they are seeing in real-time to allow for a coordinated and measured response. We urge the IMDA and MAS to take time to consider a fairer, proportionate and more equitable solution that will address the problem of Phishing across all services and platforms, leading to an equitable outcome for all and stronger protection measures for consumers.
10	Hardik Thaker	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** The scope is heavily focussed on SMS based scams and not covering much on email/ WhatsApp. Would like to seek clarity on position regarding RCS chat protocol and iMessages, if they are being covered under the scope or not? Again, if the scope of SRF is going to keep on changing as new Scams methods are identified, the consumer might not be abreast on which available redressal under SRF for the same. With ownership assigned to FI, there would be more disinformation from FI on if the scam falls in SRF or not.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** (a) Section 5.3 (footnote 10). If FI are guided on only these 4 activities as baseline set for high-risk, and the duty is towards it, there is no incentive for FIs to identify more activities as high-risk, and thus shrinking their duty #1 on cooling-off period. (b) Section 5.4: 12 hour is a very arbitrary period for cooling-off, specifically many consumers might not have ability to respond in 12 hours (like overseas, long flights, overnight time period etc). This should be increased to at least 24, ideally 36 hours, specifically as most of these High-Risk activities don't happen that frequently. (c) Include duty/obligation for FI to inform the consumer reaching out to bank for scam

S/N	Respondent	Responses from respondent
		related query to inform consumer that they can file compliant under SRF for further evaluation. Else, FI has no incentive to help consumer to direct to SRF claims.
11	Kelvin Tan	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** I feel that the scope is not wide enough and that the participation of SRF should include the digital banks serving retail customers (Trust, GXS and MariBank), some financial institutions like Singapura Finance and Hong Leong Finance as well as MVNOs targeting consumers. I believe that it should also include Visa, Mastercard, UnionPay, Meta (owner of Facebook, Instagram and WhatsApp), Tencent Holdings (owner of WeChat), LY Corporation (owner of Line), Microsoft, as well as Alphabet (owner of Android and Google), Apple (iOS), Huawei (HarmonyOS) and any mobile phone maker that uses a phone operating system that is not Android or uses a variation of Android, as well as operators of Data Centres, since the security of these DCs could be breached by these scammers and hackers and they have to be responsible to ensure such things don't happen. On the coverage of scams, I think this is not good enough. In recent cases, the scams have evolved, and it is more of malware scams and impersonation scams. I feel that evolving scams should be covered and that FIs should be obligated to settle goodwill payouts to the victims if their cases are genuine and not upon repeated requests/appeals by the victims.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** FI duty #4 should also be used to report BIN attacks on credit cards and debit cards by scammers and fraudsters and they must resolve it within a certain and reasonable timeframe, failing which the FI will have to be penalised.
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** I would like to add another responsibility for the telcos, since I believe IMDA is not in control over this. To prevent malicious actors from trying to scam victims, telcos and the police should ensure that prepaid and postpaid SIM cards can only be sold in limited locations, e.g. CCs, convenience stores, petrol stations and airport, within a certain geographical district. The telcos can also sell their SIM cards directly to consumers online or to validate their identities online. Alternatively, IMDA should allow telcos

S/N	Respondent	Responses from respondent
		to implement eSIMs so that there is no need to even get a SIM card, which the resellers can manipulate by selling to non-existent customers, which was what happened before the culprits were caught. I also believe that telcos, which are also ISPs, should provide a form of anti-virus/anti-scam/anti-phishing software to the consumers for a low fee or for free, so that all customers can have some protection against scams that may not involve SMS.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** This is a chicken and egg issue. Should it be the FI or the telco? I think both should share responsibilities and using a waterfall method might not be applicable depending on the case. E.g. What if the telcos do not provide a form of anti-virus/anti-scam/anti-phishing software or firewall to the consumer? Should they be equally liable? The authorities should also consider other players, e.g. Internet companies like Meta (owner of Instagram, Facebook, and WhatsApp) and Alphabet (which owns Google and Android). I feel that tech companies and Data Centre operators should play a part in dealing with this issue to ensure a more secure environment for everyone as much as possible.
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper.** On 7.1 (b) Investigation Stage, I think it should include the source of the scam to be part of the investigation stage, which can be either Meta or Alphabet, depending on where the consumer first saw the ad or link. I am agreeable with the timeframe provided that enough support is given to the consumer who suffers losses during those 1-2 months where they lost their income and hard-earned money. On 11.5, to remain consistent to the time needed to resolve the issues, MAS should mandate that FIs should take within 21 business days for straightforward cases, or 45 business days for complex cases. This is to ensure that the FIs do not ignore the cases that were put up to them. If the FI concerned does not resolve it by then, the consumer should be allowed to put his/her case up to FIDReC without doubt. On 11.6(b) in Annex B, I feel that the internet company concerned, whether it is Meta (WhatsApp, Facebook, Instagram), or Alphabet Google, Microsoft, Yahoo if it is via Email, should be involved in such investigations.

S/N	Respondent	Responses from respondent
		Question 9. **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.** I support the move for major payment institutions providing account insurance services to be members of FIDReC. This will help manage cases where the fault might be with major payment institutions but FIs which are members of FIDReC were unable to continue investigations due to lack of jurisdiction over these major payment institutions.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** FIs and Telcos should be graded by their responsiveness to scams, credit card/debit card fraud and phishing, e.g. red, yellow and green or A, B, C, D. If they are not able to perform well, customers will decide if they want to put their monies into the FI or to sign up as a mobile subscriber/broadband user with that telco/MVNO. I would like to add that data security companies like McAfee, Bitdefender, Norton, and many others should be allowed to share the latest findings to the FIs and Telco/MVNO/ISPs on scams to make it robust. Ultimately the goal is to have a more collaborative system among all relevant stakeholders which will make it more sustainable in the long run.
12	Law Reform Committee, Singapore Academy of Law	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** We note that the SRF is only designed to cover phishing scams but excludes other types of unauthorised transaction scam variations that do not involve phishing, such as hacking, identity theft and malware-enabled variants. The SRF uses a very narrow definition of phishing – that the consumer must, inter alia, be deceived into entering her credentials into a fabricated digital platform. The purported rationale behind the limited scope is because of challenges in specifying what measures ought to be taken by different stakeholders for all types of scams. However, we suggest that the better approach is for the SRF to cover all unauthorised transactions, regardless of the underlying scam type. There are significant overlaps between the scam typologies identified in the Consultation. In the computer science field, phishing is broadly defined as "the act of

S/N	Respondent	Responses from respondent
		impersonating a legitimate entity… in order to obtain information such as passwords, credit card numbers, and other private information without authorisation." Its essence is the use of social engineering to allow an initial compromise to a consumer's IT system. No distinction is normally drawn as to how the information (typically credentials) is subsequently obtained by the bad actor. While a typical attack involves the use of a fabricated digital platform to collect a consumer's credentials, other attacks include causing malware to be downloaded (such as a keylogger) to obtain the consumer's credentials. Given the overlaps between the scam variants, as well as the proposed duties under the SRF being broadly applicable to a wide spectrum of scams, we are of the view that drawing a distinction between phishing scams involving only fabricated digital platforms and all other scams would be unduly restrictive and difficult to defend in principle. We further note that even without limiting the scope of the SRF, to the extent that the specified duties are ineffective in preventing, or mitigating the losses from unauthorised transactions, the breach of such duties would not allow a claimant to succeed under the SRF. This is because for a claim to succeed, it must be established that "the loss arises from any non-compliance". We understand this to refer to the traditional 'but for' test of causation which is applicable to contract and tort cases. Concerns about over-compensation are unlikely to arise as such. This would also be the case, even if the duties are expanded.
13	Lawrence Tang	**Question 6.** **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** Telcos is the gateway and more features and functions to be able to block calls, not just SMS, is a way to prevent incoming messages that is the "start" of misleading the recipients. The so called "Multi-layered approach to address scam calls and scam SMS" has been good but not effective enough. Overseas Telcos allow individual to block "country codes" but not in Singapore. Most scammers are now dialling in from Msia, Indonesia, India, etc. While such features may cause some issues for older folks, the general populations are tech savvy enough to make decisions. I would like MAS and IMDA to get our telcos to be cleverer and more active in providing "more control

S/N	Respondent	Responses from respondent
		features" to end-users where we can set those "blockage" via our mobile phone easily. Also, each call received, we should have a function where we can send a "note" back to the telcos that this number that just called in was a scam. If a certain no. of complaints has been received, telco should either investigate or temporarily block the number for XX days or weeks. Question 7.
		MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper. Gatekeeping by TELCOs is the first line of defence together with the call recipients. They are not separated. They are "SAME" category.
14	LSL Boey	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** The Financial Institution has a duty to protect joint account holders as well. Upon suspicious or large transactions from a joint account, such as change in daily limit or withdrawal of more than 50% of the balance, the bank should notify the other joint account holder and implement a 'cooling off' period to allow the joint account holder to liaise with the initiator of the transaction.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** The Financial Institution has a duty to protect joint account holders as well. Upon suspicious or large transactions from a joint account, such as change in daily limit or withdrawal of more than 50% of the balance, the bank should notify the other joint account holder and implement a 'cooling off' period to allow the joint account holder to liase with the initiator of the transaction.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** As long as the Financial Institution or telco has breached clearly defined duties of care, they should be responsible for the loss suffered. Some blame-sharing may be considered if the customer has ignored notifications.
		Question 8. MAS and IMDA seek comments on the proposed operational workflow for claims brought under the

S/N	Respondent	Responses from respondent
		Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper. Banks are very good at stonewalling and protecting themselves from customers' queries. This has happened to me as the bank refused to address my complaint as a joint account holder who has suffered loss because the other joint account holder was scammed. There should be an independent Ombudsman channel for complaints about Financial Institutions failure to respond.
15	M1 Limited	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** M1 wishes to emphasize that any intended duties imposed on the relevant entities to combat scams must be appropriate and proportionate. Financial institutions ("FIs"), as custodians of consumers' money, are rightly held to a higher bar and are expected to commit to more stringent and robust controls to safeguard their clients' funds. MNOs, in relation to SMS delivery, merely provide a conduit service, which support the FIs as well as many other businesses in their communications with consumers. The business models of the FIs and MNOs are different, and hence, the respective culpability and ability to absorb customer losses are also vastly different. Our overall aim is to ensure that there will be a proportionate regulatory approach and practical implementation of the SRF. If the intent of the SRF is to preserve confidence in digital payments and take a whole-of-ecosystem approach, then it should also be recognised that MNOs are not the only players when it comes to the transmission of information to account holders. Within the SMS ecosystem, Participating Aggregators ("PAs") are also key players who play a significant role in the routing of SMSes to MNOs. As part of the responsibilities imposed on PAs today, who are similarly licensed by IMDA, they are required to ensure that only SMSes sent from organisations who have registered with the Singapore SMS Registry are passed onwards to MNOs. However, the SRF places no responsibility on the PAs if they breach IMDA's regulations, nor are they covered under the SRF. Beyond the SMS ecosystem, we note from SPF's press release dated 13 September 2023 that messaging platforms (excluding SMSes) and social media form the top two means by which scammers contacted the victims. The SRF does not cover these channels, nor are there as

S/N	Respondent	Responses from respondent
		extensive anti-scam regulatory requirements imposed on these platforms as those currently imposed on MNOs. The SRF in its current form may result in regulatory arbitrage where scammers continue to utilise these platforms to reach out to potential victims. In this regard, we note that Australia's co-regulatory code developed by the Australian Competition and Consumer Commission will involve "big social media platforms" as well.
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** On the specific duties for the MNOs in the SRF, we wish to emphasize that it is neither practical nor realistic to ensure a 100% system uptime and service availability, even with resiliency measures in place. As such, there should be reasonable provisions to cater for MNO operations.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** The SRF proposes an all or nothing approach when it comes to coverage of losses. Under the proposed waterfall approach, it is stated that the party(ies) in breach (be it the FI or the MNO or both) are expected to compensate the consumer in full, regardless of the culpability of the consumer. Such an approach may encourage syndicates to target Singapore, with the knowledge that there would be an entity being the backstop for scam losses. For consumers, the SRF may also create a moral hazard in that it inadvertently encourages consumers to be less careful under the misguided impression that they would be compensated by the FIs and/or the MNOs in the event of falling prey to scams. Scammers will always find ways to get around – if not by SMS, then by some other communication means. The SRF will not resolve the issue in the long term. Consumer education, awareness and vigilance remain the better means.
16	Mr Tim Goodchild	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** The importance of fighting against the scourge of financial scams is beyond question. However, the proposed Shared Responsibility Framework ("SRF") set out in Section 3 is likely to be restrictive, inefficient, and discriminatory in its scope.

S/N	Respondent	Responses from respondent
		According to SPF's "Mid-Year Scams and Cybercrimes Statistics 2023", for Jan-Jun 2023, the primary means used by scammers to contact victims were: • Messaging platforms (31% of cases); • Social media (25% of cases); • Phone calls, (18% of cases); • Online shopping platforms (11% of cases); • SMS (4% of cases); and • Others, such as emails, (11 of cases%). The proposed SRF only covers scams where the primary means used by scammers to contact victims was via SMS. As such, the proposed SRF addresses only 4% of scam cases. As for the remaining 96% of scam cases (using social media such as "Instagram", Online Shopping Platforms such as "Facebook Marketplace", etc), these are outside of the SRF's scope, and the owners of those platforms have no responsibility whatsoever under the SRF to help combat scams. In considering the focus of the SRF on SMS-based scams, it should be noted that (according to SPF's 2022-23 figures), SMS has declined as a means used by scammers to contact victims. By comparison, over the same period, the use of Messaging Platforms by scammers to contact victims more than doubled. It is unclearly why the proposed SRF is focused on SMS traffic, rather than more prevalent (and important) avenues of scam traffic. In addition, Section 3 of the SRF specifies that the "responsible Telcos" (i.e. the 4 mobile operators), who handle the "last-mile" delivery of SMS traffic effectively have uncapped financial liabilities under the SRF. However, the "authorised aggregators", responsible for carrying the SMS traffic up to the mobile operators, and for ensuring that the traffic is filtered for scam messages, are apparently exempted from the SRF. Given the role played by the aggregators, and the fact that aggregators are IMDA Licensees (a fact noted in the consultation paper), the logical for exempting aggregators from the SRF is unclear. The consultation paper is silent on what happens if an "authorized aggregator" fails in its responsibilities and allows scam SMS traffic to be forwarded to customers who then suffer losses. In such circumstances, will the "authorized aggregator" be responsible for compensating customers, or will customers be expected to cover the cost of the aggregator's error?

S/N	Respondent	Responses from respondent
		It is understood that, at some point, the recently passed Online Criminal Harms Act may be used in some form to combat scams using the channels outlined above. However, it is unclear how the "operationalization" of the Online Criminal Harms Act will be aligned with the proposed SRF. There is no inherently logical reason why (say) an operator of an online marketplace that contains scam advertisements should be treated any differently than a mobile operator delivering SMS that contain scams. If separate tools are used to regulate different parties involved in combatting the same scams, the results are likely to be patchwork, piecemeal, and ineffective. Rather than implementing a SRF that excluding 94% of scam traffic, it would be more effective to take a holistic approach to scams. This would necessitate involving all the stakeholders (including messaging platforms, social media entities, and online shopping platforms), and detailing their: (i) regulatory responsibilities for combatting scams; and (ii) individual obligations to scam victims if they fail to meet those responsibilities. These responsibilities and obligations could be specified in the SRF in a comprehensive and transparent manner.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** It is beyond question that the primary responsibility for addressing anti-scam measures must remain with the Financial Institutions ("FIs"). After all: (a) the FI Institution has the contractual relationship with the customer for the holding and disbursement of their customer's funds; (b) it is entirely at the discretion of the FI (not the "responsible Telco") as to how the FI engages with their customers (e.g. via the FI's App, via SMS transactions, via face-to-face transaction, etc); and (c) Only the FI can determine the validity of transactions carried out by their customers (e.g. via One-Time-Passwords, or multiple notification messages). In all circumstances, as the custodian of the customer's funds, the FI must act as the point-of-contact with the customer for scam cases. It is important to ensure that customers who have been potentially scammed are not pushed between various parties involved in a transaction.
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** The proposed SRF effectively imposes unlimited penalties on "responsible Telcos"" (but not on aggregators,

S/N	Respondent	Responses from respondent
		messaging platforms, social media entities, and online shopping platforms) for the carriage of a SMS message. This is discriminatory and unreasonable. Unlike the FIs, the ""responsible Telcos"" have no control over the means used by the FIs to communicate with the customer, and they have no ability to verify the bona-fides of the communication with the customer. To give an analogy, if FIs unilaterally decided to send out customer ATM PIN details via postcards (delivered via SingPost), it would be entirely unreasonable to expect SingPost to accept unlimited liability should criminals gain access to those PINs. Similarly, the mobile operators, as the last-mile delivery mechanism, should not be required to accept unlimited liability for the FI's decision to use SMS delivery (particularly as the "responsible Telcos" might only be receiving a few dollars per month in revenues from that mobile customer). Pending the creation of a holistic SRF framework applying to all parties involved in transactions, the liability on mobile operators should be capped at a set amount, such as the monthly charge to the customer for mobile service provided. It is also necessary for IMDA to specify several undefined elements of the proposed SRF. For example: i. If an “authorized aggregator”, as an IMDA licensee, fails to distinguish between scam and non-scam SMS traffic, what penalties will IMDA levy on that aggregator? ii. What notification period will IMDA give to the ""responsible Telcos"" should IMDA remove the “authorized” status of an aggregator? iii. If a scam message does not pass through the SMSC of a ""responsible Telcos""(for example, in a roaming scenario, or if RCS is used), presumably the ""responsible Telcos"" if not responsible for any losses incurred by a customer? iv. The consultation paper makes explicit reference to a ""responsible Telcos"" anti-scam filter … ""not [being] operational for 48 hours”. Given that anti-scam filters, like any other IT systems, will need downtime for essential maintenance, upgrades, etc, what essential downtimes will be considered acceptable by IMDA?"
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.**

S/N	Respondent	Responses from respondent
		Given that the FI has the direct contractual relationship with the customer, it is entirely responsible for the FI to be at the "head" of the waterfall, and for the FI to act as the point-of-contact with the customer in all cases. It is important to remember that, in the case of Mobile Virtual Network Operators, the mobile operator may have no contractual relationship whatsoever with the customer. To avoid confusing the customer, it is appropriate for the FI to act as the point-of-contact with the customer throughout the complaint process. However, as noted above, given the number of parties involved in this environment (including online marketplaces, social media companies, etc), the "waterfall" must include more than just the FIs and the "responsible Telcos".
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper.** The proposed operational workflow has several ambiguities, which need to be addressed in the finalized SRF. These ambiguities include: • Stage 1 of the proposed SRF appears to require the customer to file a report with the SPF. What happens if this is not done? Does the complaint cease? Upon receiving the customer complaint, what actions will the SPF undertake? For example, will the SPF seek information on the case from the FIs and the mobile operators (thereby unnecessarily increasing the workload on the FIs and the ""responsible Telcos""). What happens if the SPF determine that local agents or money mules are involved in the scam? How will this impact the processing of the case? If SPF or the FIs can recover some of the scammed funds, how will the recovered funds be factored into the SRF processes? • In Stage 4 of the proposed SRF, the SRF appears to assume that customers who are unhappy with the outcome of an investigation can appeal its findings to IMDA. However, the proposed SRF is silent on the process to be followed by IMDA "to assess whether responsible Telco has breached SRF duties". Presumably, IMDA will adopt an objective measure, but many requestions outstanding. For example: • In this investigation will IMDA play the role of an adjudicator or an investigator?

S/N	Respondent	Responses from respondent
		• Will the "Responsible telco" be allowed to respond in full to allegations made by the customer? Will this be a single round or multiple-round process? • How will IMDA assess "whether the responsible Telco has breached SRF duties"? What criteria will be followed? • If a party (the customer or the "responsible Telco") is unhappy with the results of IMDA's investigation, can that party seek an appeal or reconsideration pursuant to its rights the Telecommunications Act? If parties are not able to draw on their existing rights under the Telecommunications Act, will the Act be amended to reflect this? These matters, in addition to the other ambiguities set out above, need to be clarified before the SRF is implemented.
		Question 9. **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.** If it is intended that consumers can pursue further action through such avenues as the FIDReC, and if membership of the FIDReC does not include major payment institutions providing account issuance services (which are potentially subject to scams), it is logical that those major payment institutions should be members of the FIDReC. If they are not, this will lead to customer confusion and dissatisfaction.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** The proposed SRF appears to focus only on SMS-based scams, which account for approximately 4% scammer contacts (with that percentage declining over time). The proposed SRF explicitly excludes the growing new areas of scams, such as: • Malware embedded in QR codes and advertisements; • Messaging platform containing job scams and phishing scams; • social media (particularly "WhatsApp" and "Instagram"); and • Online shopping platforms, including cases with non-existent goods or fraudulent transactions. If it is intended to seriously combat the growing threat of scams, it will be necessary to take a holistic approach, and to address all the growing trends in scams (as outlined

S/N	Respondent	Responses from respondent
		above). This will require IMDA and MAS to regulate a considerably large group (including parties incorporated and operating outside of Singapore). It will be necessary for these parties to be subject to the same regulatory obligations and penalties, to prevent discriminations and distortions from occurring. Simply focusing on locally based entities, and on only 4% of scam traffic, is unlikely to be successful. It must be assumed that scammers will change their business models over time, and that they will seek to take advantage of any perceived weaknesses, gaps, or ambiguities in the existing regulatory regime. For this reason alone, it is necessary for the scope of the proposed SRF to extend beyond FIs and "responsible Telcos".
17	MyRepublic Group Limited	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** Section 3 - Entities covered under the SRF from telecommunications perspective should remain as MNOs as the measures applied to protect Singaporeans are applied at the MNO layer. We agree that MVNO customers should not be excluded and therefore the underlying MNO should be accountable per the SRF to the MVNO end user. MVNOs are happy to facilitate any compensation, but this must be funded by the MNO, where the MNO has failed to meet its obligations as a responsible Telco. Section 4 - Types of scams covered under the proposed SRF are appropriate. Phishing links can be blocked if sent from known and notified scam sources. We agree malware scams are much more difficult to prevent. The telecommunications provider cannot monitor what is downloaded by an end user onto their phone and therefore we do not support the SRF, in its current guise, where responsible Telcos have a duty to end users and ultimately responsible for end user compensation, ever being applied to such malware scams."
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** We believe the three duties are appropriate measures to limit the success of the in-scope SMS phishing scams. None of these technical measures can be administered or managed by MVNOs. The responsible Telco in all cases therefore is the MNO. MVNOs will need to ensure the delivery of these three duties is an obligation and

S/N	Respondent	Responses from respondent
		included within the scope of services provided by MNOs to their MVNO partners. Additionally, should the MNO be found to have not fulfilled its obligations, the MNO must compensate affected MVNO end users, in exactly the same manner that the MNO must do so for their own end user customers.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** Section 6 - The "waterfall" approach assumes the respective responsible FI and Telco duties are sufficient, if in place, to protect consumers from the in-scope SMS phishing scams. As long as this assumption holds and is true, then a layered "waterfall" approach for responsibility and ultimately accountability to the end user for any loss incurred is appropriate and the FI should be the predominant service provider and first layer in the "waterfall" as the FI administers the account the threat actor(s) is wishing to access via such scams. The inclusion of responsible Telcos as the secondary layer in the "waterfall" approach to accountability makes sense to ensure the service provider responsible for the SMS services potentially being exploited by the scammers has applied the required SMS protections as set out in the duties of the responsible Telco. As explained previously, an MVNO has no ability to apply the mandated protection measures set out in the duties of the responsible Telco, and therefore the MVNO is entirely reliant on the MNO, as responsible Telco, to apply the required protection measures for SMS phishing scams. Therefore, it must be the sole responsibility of the MNO to compensate all end users, both direct MNO and MVNO end users, where the MNO has failed to meet its obligation as a responsible Telco.
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper.** Section 7 - The proposed operational workflow appears appropriate for the in-scope phishing scams. It makes sense for the responsible FI to field complaints or enquiries from end users and conduct the initial investigation. If MVNO customers are to benefit from the SRF, which is our preference, then the responsible FI in each investigation should engage directly with the MNO,

S/N	Respondent	Responses from respondent
		rather than the MVNO, as it is the MNO that is responsible for providing the required protection measures and they are best placed to conduct the telco portion of the investigation.
18	Network for Electronic Transfers (Singapore) Pte Ltd	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** Definition of Protected Account As set out in the E-Payments User Protection Guidelines a "protected account" means any payment account that— (a) is held in the name of one or more persons, all of whom are either individuals or sole proprietors; (b) is capable of having a balance of more than S$500 (or equivalent amount expressed in any other currency) at any one time, or is a credit facility; (c) is capable of being used for electronic payment transactions; and (d) where issued by a relevant payment service provider is a payment account that stores specified e-money. We would like to seek the MAS' clarification whether card-present transactions are within the scope of a protected account. Generally, card-present transactions are considered less risky as the merchants can physically inspect the card and, in some cases, verify the cardholders' identity. For example, our NETS Prepaid Card is a stored value card that allows the cardholder to pay for goods and services at merchants in Singapore and public transport such as buses and MRT. The maximum amount that can be loaded onto one single NETS Prepaid Card is S$1,000. The NETS Prepaid cardholder can choose to pair and register their NETS Prepaid cards with the NETS App to • access past transactions; • top-up the card value; • set daily transaction limits; • lock/unlock the card; • add/edit name to a card; and • terminate and refund. Transitional Period We would like to propose a transition period of 12 months after publication of the revised E-Payments User Protection Guidelines.
		Question 9. **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.** We are supportive of the MAS' proposal for major payment institutions providing account issuance services to be members of FIDReC. We would like to seek the MAS' clarification on the implementation timeline i.e.

S/N	Respondent	Responses from respondent
		upon the issuance of Shared Responsibility Framework or after the Financial Services and Markets (Dispute Resolution Schemes) Regulations 2023 has been amended to include major payment institutions as members of FIDReC.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** The SRF should evolve to be more end-user centric. While Financial Institutions and Telcos can implement measures to mitigate the risks relating to scams, consumers need to be educated and prudent. Transitional Period We would like to propose a transition period of 12 months after publication of the Shared Responsibility Framework.
19	PwC	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** The scope covers full banks and major payment institutions (MPI is a type of license) providing account issuance service (wallet that can store e-money) only. MPI covers majority of payment institutions, including ez-link, YouTrip etc. The FI duties are good practices for other FIs and MPIs that process domestic and cross border money transfers via e-wallets. While not mandatory, such FIs should consider incorporating these FI duties. If protecting consumers is the intent, would it be clearer to define the Banks/FI and Telcos obligation to their respective Singapore Customers regardless of source of fictitious entity origination (which could be person or company) or website domain hosting, etc. In reference Case Study 3 (p.23), it concludes that SRF not applicable because the entity does not have a Singapore nexus. How would the authority determine what is a Singapore nexus or a legitimate business that offer services to Singapore residents? Given that the consumer has access to the internet, consumers can access any online presence regardless of location. How would a Bank/FI and/or Telco be able to identify what is "known to offer services to Singapore residents"?
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.**

S/N	Respondent	Responses from respondent
		On FI Duty #1, not all major payment institutions (MPIs) require activation of digital security token i.e. GrabPay, etc. In such cases, does it mean that FI Duty #1 is not applicable where an FI does not have a digital security token? MAS and IMDA may want to consider alternate controls for FIs who do not use digital security tokens for e.g. monitoring on the login from a new device. On FI Duty #2, not all MPIs require a digital security token i.e. GrabPay, etc. In such cases, does it mean that FI Duty #2 is not applicable where an FI does not have a digital security token? MAS and IMDA may want to consider alternate controls for FIs who do not use digital security tokens for e.g. real-time alerts on changes to accounts and high risk activities. 2. Considerations needs to be put in place to ensure that the real-time notifications are sent to contact points that have not been compromised. For e.g. changes to contact points may be considered a high risk activity, or real-time notification need to be sent to the old and new email address / phone number. As real-time alerts are sent to a registered mobile phone number and email address, consumers may not be aware of the real-time alerts if contact points have been modified by scammers. High risk activities, including changes to contact points, can only take effect after the 12 hours cooling period to allow consumers to monitor the real-time alerts. 3. From a customer-experience angle, a 12-hour cooling period may be too long for customer's convenience. A customer would not be able to make large transactions or transactions that are not common based on transaction history (deemed as high-risk transactions) using the bank account/e-wallet for 12 hours. Will MAS and IMDA consider a shorter cooling period for customer convenience, through additional identification and validation of the customer identity? On FI Duty #3, does "outgoing transaction" refer to outflow of funds? On FI Duty #4, over and above FI Duty #4, as additional considerations, FIs could consider allowing blocking at

S/N	Respondent	Responses from respondent
		different levels, e.g. blocking at the account level, logged in devices, or last transaction. 2. In the event that the kill switch is initiated through the reporting channel or self-service, FIs may need to consider additional validation that the kill-switch request is genuine.
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** On Telco Duty #2, in carrying out this duty, Telcos may need to consider how to address potential consumers concern on privacy.
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper.** The information may not be readily available. Whilst the FI require certain information to investigate the claim, it is not common to take screenshots of communication and transaction during the course of normal transactions where the consumer is unaware of the scam. Do consumers have other avenues of recourse if they are unable to provide the requested information for the claim? In the event that the FI and Telco not come to an agreement on the responsible party to continue the investigation, or outcome of the investigation to determine breach of duties, is there a clear pathway for the FI and Telco for mediation?
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** What is the expectation on FIs and Telcos to meet the requirements in the framework and the timeframe? In view of newer types of scams and evolving requirements of the SRF, additional considerations may be needed for FIs and Telcos to uplift the processes and systems to support the requirements.
20	Securities Association of Singapore	**Respondent has requested for submissions to be kept confidential.**
21	Shannon Lim	**Question 10.**

S/N	Respondent	Responses from respondent
		The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape. Platforms like Facebook, which host the scam ads, should be part of the shared responsibility framework as well. They should be responsible for thoroughly vetting the ads that they allow on their platforms, instead of only focusing on maximising profits from advertising revenue.
22	Shean Yeo	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** 1. Limited enforcement mechanisms: The SRF should outline clear enforcement mechanisms and consequences for non-compliance. Financial institutions and technology service providers may have different levels of risk management capabilities and resources. The SRF should provide guidance on how to address these variations to ensure a consistent and effective approach across the industry. 2. Inadequate oversight of subcontractors: The SRF focuses on the relationship between financial institutions and technology service providers but may not adequately address the risks associated with subcontractors or sub-service providers. The SRF should consider extending its guidance to cover the entire supply chain to mitigate potential vulnerabilities. 3. Evolving technology landscape: The rapid pace of technological advancements may render certain aspects of the SRF outdated or insufficient over time. The framework should be periodically reviewed and updated to keep pace with emerging risks and evolving technologies. Addressing these potential loopholes will be crucial to ensure the effectiveness and resilience of the SRF and its ability to mitigate technology risks in the fintech and telco sectors.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** 1. Fragmented oversight and enforcement: Dividing responsibility among multiple parties may result in fragmented oversight and enforcement, leading to gaps in accountability and potential regulatory breaches. 2. Complexity and inefficiency: The shared responsibility approach can introduce complexity and inefficiency in

S/N	Respondent	Responses from respondent
		the decision-making process, as different parties may have varying views and interests. This could lead to delays and suboptimal outcomes. 3. Disputes and finger-pointing: With multiple parties involved, there is a risk of disputes arising regarding specific responsibilities, potentially leading to a blame game scenario where each party tries to shift responsibility onto others rather than taking immediate action to resolve the issue. 4. Inadequate risk assessment and management: Different parties may have different risk appetites and levels of understanding, resulting in inconsistencies in risk assessment and management. 5. Lack of transparency and trust: If responsibilities and accountability are not clearly defined and communicated, it may erode trust among stakeholders, including customers who rely on fintech and telco services. 6. Regulatory gaps and overlaps: The shared responsibility framework can create challenges in regulatory coordination and enforcement, resulting in gaps or overlaps in regulations. 7. Unclear liability and recourse: In the event of an issue or breach, it might be challenging to determine the responsible party and establish liability. This could create difficulties in compensating affected parties or resolving disputes, potentially resulting in legal complexities and reputational damage. 8. Inconsistent standards and practices: With multiple parties involved, there is a risk of inconsistent application of standards and practices, especially if there is a lack of harmonization or coordination among different stakeholders. This may result in varying levels of security or service quality, affecting customer experience and overall trust in the sector. 9. Limited adaptability and innovation: The shared responsibility framework might limit the ability of fintech and telco companies to innovate and adapt quickly to changing circumstances or emerging risks. The need to involve multiple parties in decision-making and coordination might slow down the implementation of new technologies or services.

S/N	Respondent	Responses from respondent
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** Same as above.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** Same as above.
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper.** There are certain risks and concerns associated with this proposed workflow. 1. Complexity and Clarity: One concern is the potential complexity and lack of clarity in the operational workflow. The proposed workflow involves multiple stages, including the identification of responsible parties, the submission of claims, and the assessment and resolution of claims. Ensuring that the process is simple, transparent, and easily understood by all parties involved is crucial to avoid confusion and potential disputes. 2. Timeliness and Efficiency: The proposed workflow may raise concerns regarding the timeliness and efficiency of claim processing. It is important to establish clear timelines and service level agreements to ensure that claims are processed in a timely manner. Delays in claim resolution could lead to financial losses for affected parties and undermine trust in the Shared Responsibility Framework. 3. Dispute Resolution Mechanism: The proposed workflow involves the use of dispute resolution mechanisms, such as mediation or arbitration, to resolve claims. It is important to ensure that these mechanisms are fair, impartial, and accessible to all parties. Additionally, the availability of qualified mediators or arbitrators with relevant expertise in fintech and telco matters needs to be considered. 4. Data Protection and Privacy: The operational workflow involves the collection and sharing of personal and sensitive data. Ensuring compliance with data protection

S/N	Respondent	Responses from respondent
		and privacy regulations is crucial to safeguard individuals' rights and prevent misuse of personal information. 5. Jurisdictional Challenges: The proposed workflow may face jurisdictional challenges, particularly in cases involving cross-border transactions or parties. It is important to establish mechanisms for cooperation and coordination between relevant authorities in different jurisdictions to ensure effective resolution of claims. 6. Cost Implications: The proposed workflow may have cost implications for all parties involved in the claims process. It is important to consider the potential financial burden on both claimants and responsible parties and ensure that the cost of claim resolution is reasonable and proportionate. Overall, the proposed operational workflow for claims brought under the Shared Responsibility Framework raises risks and concerns related to complexity and clarity, timeliness and efficiency, dispute resolution mechanisms, data protection and privacy, jurisdictional challenges, and cost implications. These concerns need to be carefully addressed to ensure a fair, efficient, and effective claims process under the Shared Responsibility Framework.
		Question 9. **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.** There are certain risks and concerns associated with this proposal. 1. Consumer Protection: One concern is the adequacy of consumer protection measures. The proposal may require a careful evaluation of whether FIDReC's existing dispute resolution framework is suitable for handling e-money related disputes. Additionally, ensuring that consumers' funds stored in these payment accounts are adequately protected against fraud or unauthorized access is crucial. 2. Operational Risks: Allowing major payment institutions to provide account issuance services could result in an increased number of participants in the e-money ecosystem. This may lead to operational risks such as

S/N	Respondent	Responses from respondent
		system failures, cybersecurity threats, or potential money laundering activities. Robust risk management measures and regulatory oversight would be necessary to mitigate these risks. 3. Regulatory Compliance: The proposal would require major payment institutions to comply with regulatory requirements, including anti-money laundering (AML) and counter-terrorism financing (CTF) regulations. Ensuring that these institutions have robust AML and CTF controls in place is essential to prevent the misuse of e-money and maintain the integrity of the financial system. 4. Systemic Risks: The participation of major payment institutions in providing account issuance services may introduce systemic risks to the financial system. It is important to assess the potential impact on financial stability and consider appropriate safeguards to prevent any adverse consequences. 5. Governance and Accountability: The proposal raises questions about the governance and accountability of major payment institutions as members of FIDReC. It would be necessary to ensure that these institutions have appropriate governance structures and are held accountable for their actions in providing account issuance services. Overall, the proposal to allow major payment institutions to provide account issuance services and be members of FIDReC presents several risks and concerns related to consumer protection, operational risks, regulatory compliance, systemic risks, and governance. These concerns need to be carefully addressed through robust regulatory frameworks and oversight to ensure the safe and secure provision of e-money services.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** Looking at silo-operations perspective in regulatory compliance and technological risk will not be sufficient, the SRF will need to aim for a governance framework that seeks out in striking a balance between FIs' (including payment service providers) possible operational capabilities as each FI will have their own operational risk difference and appetite, although a mainframe in MAS' TRM and ORM is proposed as a guideline. Each moving day into current and future cybersecurity risk concerns, the threat landscape has been evolving way too fast for

S/N	Respondent	Responses from respondent
		any framework to be easily adopted and adapted by any FIs or Telcos firms in timeframe that needs to be realistically pushed. I would propose for maturity level ascendence when the exploits over different technological capabilities are way too much and too fast for instant operational changes adaptation, then the logical operational framework by each FI in terms of process will need to be in place akin to a resiliency plan such as BCP component as a relevant substitute workaround which needs to be accounted for (in terms of evidence trailing not compromising on either Integrity, Non-Repudiation, and Confidentiality).
23	SIMBA Telecom Pte. Ltd.	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** 20 years, is the duration a subscriber would need to stay subscribed to SIMBA's $10 mobile plan for us to recover the compensation in revenue should SIMBA be required to compensate the $2,400.00 average loss suffered by phishing scam victims in the first half of 2023. SIMBA's primary view regarding the SRF is simply that the Telcos should not be held responsible for losses arising from any scams whatsoever, and the responsibility to safeguard consumer deposits should fall squarely on the parties who have direct interaction with the deposits (i.e. the consumer, and their FI). To clarify, SIMBA accepts that there is a rising trend of scams in Singapore, and there is a pressing need for the Government to enact measures in order to combat it. On that front, the MNOs have collaborated with the IMDA to introduce a plethora of measures that is aimed to reduce the risk of consumers being exposed to known scams. Some of these measures are listed in the SRF as the duties of the responsible Telcos. The SRF has characterized the Telcos as infrastructural player(s) that play a supporting role in fostering the security of digital banking and digital payments, but this is an oversimplification of the relationship the Telcos have with the banking industry. This will be explained in detail below. Telcos enter into a contract with Participating Aggregators ("PA") for the latter to send SMS Sender ID ("SSID") SMS messages on behalf of their clients. FIs enter into a contract with PA to send SSID SMS messages, where there are assumably commercial and technical policies governing the relationship between the FI and the PA. As the Telcos do not have a direct contractual

S/N	Respondent	Responses from respondent
		relationship with the FIs, the Telcos are not the FIs' service provider and do not owe any specific duties or obligations to the FIs. Stemming from this, the Telcos also do not owe any specific duties or obligations to the FIs' customers. FIs have traditionally rejected the notion of contracting directly with the Telcos, resulting in the Telcos having no input on the content of SMS that the FIs can send. In its current state, the FIs have taken to sending risk-heavy SMS messages to facilitate the digital banking and digital payments ecosystem for the benefit of themselves and their customers. If the SRF is introduced, the FIs will essentially be passing on the risk associated with this practice to the Telcos, but without sharing either the benefit or the risk controls. Furthermore, the Telco's customer and the FIs' customer may be the same person under the SRF, but should be viewed as different entities. The reason for this is simple: the Telco's customer contracts with the Telco to be provided telecommunications services by the Telco, and the FIs' customer contracts with the FI to be provided banking services by the FI. The Telco's customer will not reasonably expect the Telco to protect the money held by the FI for the FI's customer – such an expectation is reasonably and naturally placed on the FI. It is not conceivable that "protecting a customer from scams" is a telecommunications service that the Telcos are meant to provide. As such, the failure to protect a customer from scams should not result in the Telco being responsible to the FIs' customer. One of the biggest challenges that we feel that the SRF needs to overcome is the interaction between SSID SMS messages and Rich Communication Services ("RCS") Messages. Telcos do not have the means and are not expected by the IMDA to monitor RCS messages. These non-SMS messages are not filtered by the Telcos but are presented in not dissimilar manner to the consumer as SMS messages. Whilst the SRF is clear that Telcos do not bear any liability for scams arising from non-SMS messages, it is not likely that the average consumer will appreciate the difference. The Government should therefore increase awareness and public understanding between SMS and non-SMS messages which can both be displayed as SSID messages.
		Question 6.

S/N	Respondent	Responses from respondent
		IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper. If the SRF is enacted, it should clearly outline, beyond a shadow of a doubt, that Telcos do not owe a duty to our customers to safeguard their deposited funds with their FIs in the event of a scam, or prevent them from being scammed. This is not a service provided by Telcos, and it is not a duty owed to either our customers or the customers of the FIs. With particular regard to the Telco Duty #3, the SRF must be limited to malicious URLs that have been made known to the Telcos by the Government through its updating of a centralized list of malicious URLs, and account for the lag-time between the updating of the centralized list and the updating of the Telco's filter. The Telco's inability to update its filter immediately after being informed of the malicious URL should not be a breach of this duty to the IMDA. Additionally, if the consumer clicks on a malicious URL that was flagged to be malicious, but the SMS message that the consumer clicked the malicious URL on was received before the URL was flagged, the Telco must be found to not have breached this duty under the SRF regardless of whether the SMS message containing the malicious URL was eventually blocked at the time the customer clicked on the malicious URL. Lastly, under this duty, the SRF must be clear that only known malicious URLs are blocked. Consumers should not be given the impression that they will not receive SMS messages with malicious URLs at all because filtering is conducted on a best-efforts basis by the Telcos. Consumers should still be vigilant, be accountable for their own actions, and understand that if they click on a link and got scammed, it does not mean that that link was already flagged to the Telco to be blocked.
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper.** The operational process of the SRF is presently unclear. SIMBA would propose that if the SRF is enacted in its current form, the 30 days period should be strictly conformed to, and not be wavered under any circumstance. This means that a consumer filing their claim from the 31st day after the scam should have the

S/N	Respondent	Responses from respondent
		claim discontinued for lack of jurisdiction for the FIs/Telcos to consider the claim; and there should be no abridgement of timelines or goodwill exception to jurisdictional discontinuances. If the SRF is enacted, Telcos must be allowed to limit our liability by way of contract. If the Government does not allow this, it is expected that the price of consumer mobile services will increase to account for the potential liability the telcos are being forced to bear. If a claim is accepted by the FI to be within the scope of the SRF, but it is later assessed by the responsible FI and/or Telco that their duties were complied with, it is imperative that the principles of issue estoppel must be applied. The consumer should not be allowed to re-file their claim with the FIs. If the consumer is dissatisfied by the findings of the responsible FI and/or Telco, the SRF envisions a "Recourse Stage" where the consumer makes a further complaint to IMDA, MAS, or FIDREC via an appeal. SIMBA cautions here that the Recourse Stage for the Telcos must be a *de facto* appeals process that is reasonable, decided by an objective arbiter, and should not involve a mediation stage. It is preferable that the Recourse Stage is conducted by the judicial branch of government as opposed to the executive branch of government. A central avenue for recourse will safeguard against "forum shopping" and prevents concurrent or consecutive appeals to the respective recourse avenues of the FIs and Telcos. Another aspect that the SRF should clarify is the Telcos' role in recovery of the monies lost to the scam, and the Telcos' entitlement to any monies that is recovered if they had borne the losses of the consumer. It is reasonably understood that under the SRF, monies lost by the consumer will usually be by way of inter-bank transfer. If any part of the monies is recovered, as stated above, the Telcos have no contractual nexus with it, and does not have, in our view, the requisite *locus standi* to make a claim for monies recovered due to the SRF being a guideline that imposes expectations, rather than directions. The SRF must provide that any amount recovered will be used to make whole the entity that had borne the loss of

S/N	Respondent	Responses from respondent
		the consumer, regardless if this was done strictly in accordance with the SRF's or by virtue of goodwill. Conversely, if the Government does not intend for monies recovered to go towards making whole the entity that had borne the loss of the consumer, the SRF must state how the Government intends to deal with it. It is not conceivable that the lost monies is returned to the consumer if they have been made whole, and we posit that confiscation of the sum, or holding the sum in perpetuity, is inequitable to the participating entities in the SRF. Lastly, the SRF must provide for how it intends to address inverse scams and the exploitation of the guidelines.
24	SingCash Pte Ltd	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** SingCash's Dash is an all-in-one mobile wallet. Dash is a mobile payments application that allows users to commute, shop in-store and at online retailers worldwide with their Visa Virtual Account and send money locally and overseas. In relation to the entities covered under the SRF, SingCash notes that the SRF is expected to apply to all full banks and relevant payment service providers, where "relevant payment service providers" includes licensed major payment institutions providing account issuance services such as payment accounts that can store e-money. We are of the view that it should not be necessary for e-wallets to also be additionally covered under the SRF by the same duties applicable to full banks, because e-wallets have a fundamentally different risk profile compared to bank accounts. For example, unlike bank accounts, e-wallets or payment accounts already have specific protective features arising from requirements imposed by the MAS, such as: (a) wallet caps; and (b) annual flow caps. Under the Payment Services Act 2019 (read with the Payment Services Regulations 2019), payment institutions who offer account services that issue e-money (i.e. e-wallets) may only issue e-wallets containing e-money of up to S$5,000, and the total value of e-money transactions per annum for that e-wallet cannot exceed S$30,000.

S/N	Respondent	Responses from respondent
		These protective features specific to e-wallets already function as natural impediments to the scale of potential scam activities impacting e-wallets, relative to bank accounts. As such, we believe that it is not necessary for payment service providers issuing e-wallets to be included in the SRF. Our response to Question 2 will further explain this comment.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** FI Duty #1: Impose a 12-hour cooling off period upon activation of digital security token during which 'high-risk' activities cannot be performed. We submit that there is no need to impose on e-wallet providers the proposed 12-hour cooling off period upon activation of the digital security token. Consistent with the fundamentally different risk profile of e-wallets compared to bank accounts as discussed above, industry practice for the provision of e-wallets does not typically necessitate digital security tokens. Instead, e-wallets typically feature two-factor authentication (2FA) solutions, e.g. via email or SMS, having regard also to the nature of e-wallets being limited to low-risk and routine transactions with market expectations for quick processing time. Further, as earlier discussed, e-wallets transactions are typically subject to limits on the amount that can be remitted in each instance (as a practical consequence of the threshold caps already required under the Payment Services Act 2019). Accordingly, the 12-hour cooling off period under the SRF need not apply to e-wallets. FI Duty #2: Provide notification(s) alerts on a real-time basis for the activation of digital security token and conduct of high-risk activities. We refer to our comments above. The concept of "high-risk transactions" under the SRF appears to be more tailored to the risk profile of bank accounts, which does not align with the operational nature of typical e-wallets. We note that the SRF currently describes high-risk transactions as including, for example, increasing the transaction limits for outgoing payment transactions from the payment account. However, generally, e-wallets do not provide granular layers of flexibility for users in terms of the transactional limits, and users are not able

S/N	Respondent	Responses from respondent
		to increase or reduce those limits as they wish, unlike bank accounts. This is often a practical consequence of the threshold caps already required for e-wallet transactions under the Payment Services Act 2019 as earlier discussed. We also wish to highlight that the requirement for the FI to provide the notification on a "real-time" basis can only be viable if such notifications may be sent out via the payment provider's own platform, e.g. in the case of an e-wallet, via the app. In the case of an e-wallet, if such notifications has to be sent out via SMS or a third-party platform, there will inevitably be the technical possibility of a time-lag. In this regard, we consider timely the MAS's proposal to amend the E-Payments User Protection Guidelines ((EUPG)1 to allow payment institutions the flexibility to deliver real time notifications via the app. FI Duty #3: Provide outgoing transaction notification alert(s) on a real-time basis. We note that under the relevant payment notices, a payment institution is already required to provide notifications and receipts to its users of every transaction (i.e. activities) regardless of the value. Again, we reiterate that payment institutions should be allowed to use in-app notifications in order to comply with this requirement; for this, we appreciate that the MAS has taken this into consideration in its ongoing consultations to the amendments to the EUPG. FI Duty #4: Provide a (24/7) reporting channel and self-service feature ("kill switch") to report and block unauthorised access to their accounts. Generally, in the case of e-wallets, the customers are able to log out of the e-wallets given the existence of the 2FA authentications. As such, kill-switches are not be necessary.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** Limit for losses Under paragraph 5.1 the EUPG, "[t]he account holder of a protected account is liable for actual loss arising from an unauthorised transaction where any account user's recklessness was the primary cause of the loss", so the account user held responsible as the first line of defence under the EUPG.

S/N	Respondent	Responses from respondent
		In contrast, under the "waterfall approach" of the Draft Guidelines on the SRF, the position appears to be reversed: the FI is "expected to bear any loss arising from a seemingly authorised transaction" [emphasis added] so long as the loss arises from any non-compliance by the FI with the applicable duties, even if the account user has failed in its account user duties under the EUPG. Whilst the duties of account users under the EUPG are reiterated under paragraph 3.1 of the Draft Guidelines, such duties of account users are described as mere "best practices"; and under Case Studies 7 & 8 of Annex A of the Consultation Paper, it was confirmed that the FI "is expected to bear 100% of losses, even though Consumer [G/H] had … failed to take due care by clicking on the link in the phishing SMS and Consumer G in the case of Case Study 7 choosing to ignore the notification alerts that were sent to him" [emphasis added]. This is of significant concern as the users could potentially claim up to millions of dollars in losses in the aggregate, resulting in disproportionate financial burden. Typically, claims of these values will require a fair period of dispute resolution, including detailed documentation and perhaps court adjudication. The proposal under the Draft Guidelines places an undue onerous burden on FIs and will encourage account users (as defined in the EUPG) to not also take responsibility for their online activities as the first line of defence – which remains a very critical component of being able to achieve a robust cyber defence against scams. The FIs may not be in any better position to address risk for example on account of a zero-day exploit affecting third party systems (which may include the user's device operating system) facilitating seemingly authorised transactions, or where the user has failed to mitigate the risk of such exploits by promptly applying updates, and for the FI to be fully at risk of loss is unreasonable and inequitable. Given that the Government has also affirmed in the Consultation Paper that "[a] discerning and vigilant public remains the first line of defence against scams" (paragraph 2.6), we submit that – consistent with the spirit of a "shared" responsibility framework – account user duties should be a real, enforceable and substantive aspect of the equitable risk sharing. Otherwise, the risk burden on FIs may also in turn be a deterrent to FIs

S/N	Respondent	Responses from respondent
		offering new and innovative payment services, which can ultimately be detrimental to Singapore's leadership in developing new payments solutions, or at very high cost to consumers given the risk undertaken by the FI. Regarding the nature of losses claimable, whilst footnote 8 of the Draft Guidelines states that "For the avoidance of doubt, losses arising from unauthorised transactions exclude any loss of business or profit, special, punitive, indirect or consequential loss and any other losses", it might be clearer for the Draft Guidelines to state positively that claimable losses will be limited to only the transaction amount of the "seemingly authorised transaction".
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** We would emphasise the importance of consumer participation in scam prevention and mitigation as part of an equitable approach to risk sharing. In this regard, we propose for a more targeted application of the SRF to specifically vulnerable consumer segments, such as the elderly who may be more susceptible to scams. Indeed, there are already extensive public awareness programs and initiatives by the Government, media, and industry (both in the financial and telecommunications sectors) that should have sufficiently equipped a significant portion of the population with awareness and appropriate tools, supporting a more focused application of the SRF. We also welcome further refinements to establish a more nuanced and equitable approach to liability sharing under the SRF, for example excluding the FI's liability in cases where the scam's success was predominantly due to the actions/failures of external service providers and outside of the reasonable control of the FI.
25	Singtel Mobile Singapore Pte Ltd	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** In relation to the entities covered under the SRF, Singtel Mobile submits that the SRF should provide for other key players to be accountable. In particular: (a) Participating Aggregators (PAs) under the SSIR are key players that play an integral role in the transmission of SMS and should be covered under the SRF. Telcos are required by the IMDA to connect to PAs under the SSIR for the sending

S/N	Respondent	Responses from respondent
		of SMS, and two of the three duties applicable to Telcos under the SRF relate to PAs, i.e. to connect only to authorised aggregators for delivery of Sender ID SMS to ensure these SMS originate from bona fide senders registered with the SSIR (paragraph 5.2.1), and to block sender ID SMS which are not from authorised aggregators to prevent delivery of Sender ID SMS originating from unauthorised SMS networks (paragraph 5.2.2). Given the Telco's dependency on PAs, the PAs should be accountable for non-performance. Excluding PAs from the SRF is likely to create an imbalance of responsibilities and inequitable allocation. (b) E-commerce platforms and social media service providers are also key players that should be covered under the SRF. E-commerce platforms and social media services appear to be the most common channels by which an account user engages with scammers in connection with seemingly authorised transactions, as well as the usual channels through which scams are often initiated/executed. For example, referring to The Straits Times articles on 13 September 2023, statistics released by the Singapore Police Force show that SMS-related scams accounted for only approximately 4.3% of scam cases received in the first half of 2023;1 by compassion, in the preceding 6 months, social media and online shopping platforms, etc accounted for the bulk of the scams. Modern scams often involve sophisticated methods that transcend traditional communication channels like SMS. Consistent with an equitable risk-sharing model, we propose that e-commerce platforms and social media services, which are integral to the consumer digital experience and scam operations, be included under the SRF at the initial stage. In light of the above, we are of the view that it is reasonable and logical that other key players such as the PAs, e-commerce platforms, social media service providers, etc also be included under the SRF.

S/N	Respondent	Responses from respondent
		Further, we submit that where a PA fails to perform their duties under the SSIR and allows SMSes with spoofed Sender IDs to be sent to a Telco, the PA should be responsible for any share of the losses incurred by scam victims. In addition, there could be instances where the primary security vulnerability does not originate from the Telco service itself. For example, where account holders use telecommunications networks for the purposes of carrying out a financial service that requires a higher form of security (e.g. for authentication purposes) to be implemented by the relevant FIs (e.g. banks), the security protocol chosen by the relevant FI is a factor beyond the control of Telcos. 3.5 Consider the MAS's recent announcement in July 2023 that it has required banks to phase out SMS OTP as a sole factor to authenticate high-risk transactions, against the trend of scams arising despite local Telco networks being secure and not compromised. The then Senior Minister and Minister in charge of MAS, Mr Tharman Shanmugaratnam had acknowledged the following: "local telco networks were secure and not compromised" …. "Nonetheless, the MAS recognised that malicious actors diverted SMS OTPs to perform fraudulent bank transactions, and inherent vulnerability of the SMS channel"… "The MAS has required banks to phase out SMS OTP as a sole factor to authenticate high-risk transactions." Hence, while Telcos provide the communication networks, Telcos do not control or influence the security protocols chosen by third parties (e.g. FIs for transaction authentication); in such a context, since those third parties (e.g. FIs) are responsible for determining and implementing authentication methods, they should bear the associated risks.
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** Singtel Mobile notes that Telcos will be subject to three duties under the SRF, which appear to be consistent with the IMDA's issued directions to the Telcos under Section 31 of the Telecommunications Act.

S/N	Respondent	Responses from respondent
		<u>Telcos to assist FIs, not responsible for compensation</u> Insofar as the duties of the Telcos are already set out as directions issued by the IMDA under Section 31 of the Telecommunications Act (IMDA's Directions), there should be no need to duplicate the same obligations under the SRF. Otherwise, notwithstanding that the Draft Guidelines currently propose that IMDA's Directions "will prevail if there is any inconsistency between the duties as set out in these Guidelines and IMDA's Directions", there could still be potential confusion as to whether there might be duplicate penalties under concurrent application of the two frameworks. Furthermore, the FIs are the custodians of the protected accounts that are implicated in the scams. In contrast, the Telcos are far from the heart of the scam: (a) Telcos typically have no direct relationship/involvement in the agreements/transactions between FIs and consumers (and, in principle, the protected accounts implicated by the scams are accounts opened with the FIs); and (b) the seemingly authorized transactions will ultimately be based on arrangements between the customer and the impersonated entity, to which the Telco has no privity. Accordingly, given the existing framework under Section 31 of the Telecommunications Act, the role of Telcos should be limited to compliance with telco-specific duties. Indeed, the framework under the Draft Guidelines recognize that the nexus is primarily between the FI and the consumer, where: (a) the consumer has to be an account holder or account user of a payment account, i.e. that is issued by an FI. Telcos are also not privy the account agreement; and (b) the FI should be the first and overall point of contact with the account holder/user. It is required to assess if the claim falls within the SRF's scope ("relevant claim") and inform a Telco only where the claim relates to the Telco duties under the SRF. For the reasons above, we submit that the Telcos participation in the SRF should be limited to assisting the FIs as appropriate (e.g. in investigations) as Telcos are already separately subject to penalties if they were to fail in their regulatory obligations to the IMDA.

S/N	Respondent	Responses from respondent
		Anti-scam filter One of the duties of the Telco proposed under the Draft Guidelines relate to the requirement to implement an anti-scam filter that filters SMS through the detection of malicious links for all SMS that pass through the Telco's network, regardless of whether the SMS originates domestically or internationally. We would highlight that as part of the regular and normal maintenance of our systems and networks, there may be instances where the anti-scam filter may be taken offline during scheduled maintenance in order to carry out essential upgrades or patching to ensure functioning of the filter. During such periods, the anti-scam filter will be temporarily unavailable. Furthermore, there may also be instances where the anti-scam filter may, for technical or other reasons, be causing issues with our wider mobile service network(s), which could potentially adversely affect customers. In such a situation, we may need to suspend the anti-scam filter for a period of time so as to ensure that customers may continue to use their mobile service until we complete necessary investigations and/or rectification actions. This is part of protecting the resiliency of the network and is essential in meeting our broader regulatory obligations to the IMDA in maintaining service uptime. In view of the above, so long as a Telco has taken steps to implement anti-scam filter tools, including those offered by reputable technology providers, and has duly ensured that they are maintained, the Telco should be treated as having discharged its obligations under the SRF.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** Singtel Mobile agrees that the FI should be placed first in line and be expected to bear the full losses if any of its duties have been breached. We agree with the principle of recognising the primary accountability that FIs owe to their consumers as custodians of their money. Independent and objective assessment It is also not clear how it may be established with reasonable certainty that an FI has fully complied with all its duties under the SRF, such that the liability cascades to the Telco under the SRF. It must be remembered in this

S/N	Respondent	Responses from respondent
		context that the Telco is only a carrier of messages or communications, but does not originate the same, nor is it in any position to control the same nor the contents of the communications. The obligations of the Telco under the SRF (as set out in Paragraph 5.11 to 5.13 of the Consultation and Paragraph 5.2 of the Draft Guidelines) are clear because they constitute the obligations that the IMDA has directed responsible Telcos to comply with. The IMDA can therefore function as the independent and objective assessor, clearly and definitively, whether the applicable obligations have been met by the Telcos, based on the existing metrics already available under the Telco regulatory regime. By comparison, the obligations of the FIs under the SRF (as set out under Section 4 of the Draft Guidelines) are drawn from yet another set of guidelines, i.e. the End-User Payment Guidelines. It is not clear how it may be assessed independently and objectively that the FIs have fulfilled all their applicable obligations. Under the waterfall approach, independent and objective assessment of the FIs' compliance with duties under the SRF will be crucial precisely because Telcos are far from the heart of the scam and not privy to the arrangements between the consumer and the FI when the protected account is affected – see the discussion above at paragraphs 3.9 et seq. As the Consultation Paper acknowledges, the Telcos only play a supporting role as infrastructure providers and are merely network carriage providers. Accordingly, we submit that the different operational realities of FIs and Telcos should be recognised – there should be an assessment framework that reflects these differences while maintaining fairness and equity. Limit for Losses/Claims Singtel Mobile notes that there is no specific cap or limit set for losses suffered by scam victims or the quantum of the claim as set out in the Consultation Paper and Draft Guidelines. This is of high concern as the users could potentially claim up to millions of dollars in losses in the aggregate, which is a substantial amount compared to the monthly subscription charges that consumers pay for their mobile service. This can result in a disproportionate financial burden. Typically, claims of these values will

S/N	Respondent	Responses from respondent
		require a fair period of dispute resolution, including detailed documentation and perhaps court adjudication. We therefore propose that a cap or a limit be placed in relation to the quantum of claims under the SRF. This will also be consistent with the Telecommunications Alternative Dispute Resolution scheme where the IMDA has introduced a limit – the same should be considered in the present context as well. It is also Singtel Mobile's view that recovery under SRF should be limited to vulnerable segments of the Singapore population, as we will further discuss below.
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper.** We provide our comments on the stages identified under the SRF: (a) "Claim Stage" – Singtel Mobile supports: the proposal that the 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; under this approach, it will also assess if the claim falls within the SRF's scope and inform a Telco only where the claim relates to the telco duties under the SRF. However, we would refer to our comments above on the need for independent assessment; (i) the proposal that it is the consumer's responsibility to provide records of communication with the scammer, including the date, time and sender of the SMS. It is important for such information to be provided by the consumer in order for the Telcos to be able to thoroughly investigate any claims under the SRF. (ii) "Investigation Stage" – we note that under the current proposed framework, Telcos (where the scam was perpetrated through SMS) shall endeavour to complete its investigation within 21 business days for straightforward cases, or 45 business days for complex cases. (iii) "Outcome Stage" – Singtel Mobile notes that it is the responsibility of the FI to provide the

S/N	Respondent	Responses from respondent
		consumer with a written reply of the investigation outcome and the assessment of the consumer's responsibility for the losses. We support this approach as the FI has a direct contractual relationship with the consumer, hence it is only appropriate for the FI to close off the claim with the consumer. (iv) "Recourse Stage" – we submit that it is unclear why there is a "recourse stage" where consumers can write to the IMDA if the consumer disagrees with the Telcos assessment on the breach of its duties. The Telco duties under the SRF are clearly set-up and described under the SRF. Where a Telco assesses that it has met the telco duties under the SRF, it also means that it has complied with the IMDA's directions. There is no clear basis for a consumer to disagree with the assessment, it is a matter of whether the Telco has or has not met the duties under the SRF. We are therefore of the view that it is unnecessary to have a "recourse stage" for Telcos.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** We would emphasise the importance of consumer participation in scam prevention and mitigation as part of an equitable approach to risk sharing. In this regard, we propose for a more targeted application of the SRF to specifically vulnerable consumer segments, such as the elderly who may be more susceptible to scams. Indeed, there are already extensive public awareness programs and initiatives by the Government, media, and industry (both in the financial and telecommunications sectors) that should have sufficiently equipped a significant portion of the population with awareness and appropriate tools, supporting a more focused application of the SRF. Furthermore, as discussed in our response above, the statistics clearly demonstrate that SMS-related scams now account for only a small percentage of scam cases. As the types of scams evolve rapidly, we believe that it is

S/N	Respondent	Responses from respondent
		important for other key players such as the PAs, e-commerce platforms and social media service providers to be included under the SRF at its initial stages. Singtel Mobile would be glad to support the Government's efforts in raising scam awareness amongst members of the public and would be open to collaborations between the Government and the telecommunication industry to further strengthen the public education campaigns to fight against such scams.
26	StarHub Ltd ("StarHub"), on behalf of the StarHub Group	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** Broader ecosystem needs to be considered: As the authorities would have already been aware, there are significantly more stakeholders/ players in the ecosystem than what is currently envisaged. The Telcos have been working very closely with IMDA over the years to implement various upstream measures over traditional SMS and voice channels to help combat against scams. As scams continue to evolve, scammers are increasingly turning to other popular channels, such as other messaging and social media platforms to contact victims. Such scams are common today. This is evidenced in SPF's published crime statistics which indicate messaging platforms and social media as key platforms by which scammers contact victims. Scams via SMS pale in comparison. We believe the proposed SRF should attempt to cover a broader and more relevant set of entities, such as operators of key messaging and social media platforms that are widely used in Singapore. This will more effectively address the scam landscape, in tandem with the trends and challenges we are facing today. It will also better reflect accountability and responsibility from all relevant stakeholders operating in the ecosystem. <u>Delivery of SMS messages:</u> For SMS delivery, we wish to highlight the there are other IMDA-regulated entities involved. Specifically, most SMS-sending organisations (including the FIs) do not deal with the Telcos directly when sending out SMS messages to customers. Rather, these organisations work with IMDA-licensed SMS aggregators, which play a pivotal role in the mass delivery of SMS messages to subscribers. In its consultation document, MAS / IMDA has also acknowledged the key role that such SMS aggregators play in securing the SMS channel.

S/N	Respondent	Responses from respondent
		SMS aggregators are already required to comply with minimum IMDA-mandated regulatory safeguards, and it is both necessary and logical to include these aggregators in the scope of entities covered under the SRF, to ensure that they consistently comply with IMDA's regulatory requirements, to protect the end customers from scams. Without closing this loophole, if there are any breach of duties at the SMS aggregator-level, there is no mechanism under the SRF for consumers to seek redress from the SMS aggregators. <u>Phishing emails:</u> We note that the SRF also covers phishing emails. We acknowledge IMDA / MAS' position that this is outside the scope of responsibility for the Telcos, and in any case, Telcos are not privy to the content of the emails. However, it may not be clear to the public what responsibilities and recourse they would have if they became a victim of email phishing scams, as opposed to SMS phishing scams. As the SRF also covers phishing emails, IMDA may also wish to consider whether it is necessary for key email providers to be covered under the SRF, to raise awareness, and ensure that adequate protections are placed at the email delivery layer.
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** StarHub is in-principle agreeable with the three duties set out for the Telcos under the SRF, subject to our submissions herein. It is critical that such duties have clearly defined parameters established between the Telcos and authorities, in order to avoid confusion amongst the relevant stakeholders and avert disputes over compliance. While Telcos can take reasonable steps to fulfil our duties, exemptions for inadvertent breaches should also be allowed under certain circumstances. For example: (a) System outages which are outside of the Telcos' reasonable control (e.g., those caused by third parties and/or acts of God). The Government has acknowledged that: "*We cannot completely eliminate service outages, especially with the increasing complexity of technologies and networks. Instead, we expect operators to plan and design resilient networks, and put in place measures to ensure speedy recovery in the event*

S/N	Respondent	Responses from respondent
		of a disruption. This will minimise inconvenience to end-users should such disruptions occur."1 In the Telco contracts with customers, it is explicitly stated that services are provided on an as-is and where-is basis. Notwithstanding the Telcos putting in place resiliency measures and attempting to recover systems as quickly as possible, it is clear that there will be unavoidable downtimes and also scheduled maintenance windows for the Telcos' systems. The SRF should take into account this exception. (b) While Telcos have implemented an anti-scam filter solution, there is no perfect solution which can filter out all phishing links, which are constantly evolving. To avoid any confusion or unnecessary disputes with consumers, IMDA should clarify that the mere fact that a consumer has received an SMS phishing link does not automatically mean that the Telcos have breached their duty to implement an anti-scam filter. Further, consumers should also be reminded of their individual responsibility under the SRF to mitigate the occurrence of scams by practising proper cyber hygiene, and not share their credentials to a third party under any circumstance. The customer must share responsibility of his own acts and omissions.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** The business relationship between Telcos and their customers can be quantified by the amount of monthly subscription fees paid by each customer, which will typically be significantly lower than any actual scam losses that the customers may incur. Furthermore, per trite law there are also clear and enforceable contractual limits on the Telcos' liabilities in the service contracts with their customers. This is in stark contrast to the relationship between FIs and their customers, where the FIs have direct knowledge of each account holder's assets and the amounts that may be scammed are directly held by the FIs as custodians of the account holder's money. Consequently, it would not be reasonable for the SRF to require Telcos to bear the full amount of any SMS

S/N	Respondent	Responses from respondent
		phishing scam losses when we do not have visibility, possession or control of the potential quantum involved. There should be an equitable sense of proportionality in determining the amount of losses that the Telcos need to compensate to consumers under the SRF. The consultation paper makes it clear that a key purpose of the SRF is to "emphasise individuals' responsibility to be vigilant against scams". The amount of the scam losses that should be compensated by the Telcos should be assessed based on the overall facts of each incident. There may be circumstances where a consumer had not exercised reasonable due diligence in guarding against scams. For example, a customer may ignore notification alerts and knowingly allows scam-related transactions to take place on an ongoing basis. Even if a Telco has not fully complied with their duties under the SRF, a case-by-case analysis of the facts of each incident should be carried out before determining the culpability of the Telco in any scam-related incident. Furthermore: • The actual subscriber of the mobile service (i.e., the party that registers the service with the Telco) may be different from the party who is using the mobile line or who encounters the scam. • The scam victim may not even be a Telco subscriber, for example, the victim could be an MVNO customer. Where the affected party is an MVNO customer, the Telcos should not be responsible for any compensation of scam losses under the SRF as we have no contractual relationship with the MNVO customer. Any claim by MVNO customers should lie with the MVNOs directly. The SRF should not override the legal concept of privy of contract, which is trite law.
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper.** <u>Timeliness of investigations:</u> We are of the view that further clarity is needed on the following statements under paragraph 7.3 of the draft Guidelines: • "The account holder should report any unauthorised activity to the responsible FI as soon as practicable, and no later than 30 calendar

S/N	Respondent	Responses from respondent
		days after becoming aware of the seemingly authorised transaction." (Emphasis added). • "The account holder must furnish a valid email address and a police report within 3 calendar days from the date of notification of the seemingly authorised transaction to the responsible FI, in order to facilitate the claims investigation process" (emphasis added). It is unclear whether the requirement is for an account holder to report any seemingly authorised transaction within "3 calendar days", or "no later than 30 calendar days". We wish to highlight that timing is a critical element of the operational workflow. Any retention of logs showing the sender of the SMS, and whether the SMS has been scanned by the anti-scam filter will only be available to the Telcos for a limited period after the SMS was sent. This emphasises the need for timely reporting of any scams on the part of consumers. To facilitate the investigation, consumers also have the responsibility to report any scams to the police and the FIs as quickly as possible, and with the necessary information. Where the scam was perpetrated via SMS, the relevant information will also have to be provided to the Telcos as soon as possible to facilitate our investigations. There should be clarity who should be the party providing this information and the timelines. If Telcos are asked to investigate the claims beyond a certain period of time after the phishing SMS is sent, there can be no guarantees that the Telcos will be able to successfully retrieve information on the phishing SMS. Network information is purged periodically, in line with industry practice. <u>Investigations into claims:</u> We would like to clarify what the Authorities mean by "a responsible Telco should have governance structures and investigations processes, involving representatives who are independent from business units to assess and determine whether duties have been breached". For Telcos, the relevant duties under the draft Guidelines are network-based, and only the Telcos' network engineering teams have access to this information, and they would have to be involved in the investigation. Our understanding is that the network engineering teams are not "business units", and as such should be allowed to carry out any necessary investigations into the claims.

S/N	Respondent	Responses from respondent
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** As highlighted above, there are significantly more stakeholders in the ecosystem than what is currently envisaged under the SRF, such as operators of key messaging and social media platforms in Singapore. As the scammers have moved to such messaging and social media platforms as contact methods, it is necessary to consider expanding the scope of the SRF to include these stakeholders. For SMS delivery, SMS aggregators should be included as they also play an important part in the safe delivery of SMS messages.
27	Sylvia Lim (Personal Capacity)	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** The SRF only applies to responsible FIs and responsible Telcos (as defined in the SRF). It is logical to ask why messaging platforms and social media intermediaries are excluded from the SRF. According to the Singapore Police Force (SPF), messaging platforms and social media were the top two methods of contacting victims, with 6,573 cases involving messaging platforms and 5,368 cases using social media in the first half of 2023. These far exceeded cases using phone calls (3,908) or SMSes (920). The SPF also specifically noted that messaging platform WhatsApp was the most common channel for phishing scams.3 Furthermore, to most victims, it would matter very little to them whether they received a phishing link via SMS or a platform like WhatsApp. It would therefore be unfair for consumers to have SMS-enabled scams excluded, if the intermediary fails to meet certain minimum standards. While such platforms are not presently regulated, the Government should consider how to include such intermediaries in the SRF. This can be done and I note that such intermediaries fall within the scope of the Online Criminal Harms Act, which will come into force next year.

S/N	Respondent	Responses from respondent
		Another concern is the delay in drafting the SRF and urge the MAS and IMDA to consider having the SRF apply retrospectively to phishing scams from February 2022, when the MAS first informed banks that it expected financial institutions to "treat their customers fairly and bear an appropriate proportion of losses arising from scams".4 The MAS then announced that a framework would be published "within three months" and some consumers have continued to bear the financial losses during this time. As the duties set out in the SRF are not onerous on the banks, such a retrospective application would not be unfair or unjust.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** I welcome the category of high-risk activities and additional friction to mitigate scam losses. However, one concern is the widespread adoption of 'digital security tokens' among banks in Singapore, which has given rise to its use in phishing scams when online banking details are compromised. I urge the MAS to allow customers to opt for a physical security token instead, particularly for elderly and vulnerable clients. Despite the government's acknowledgment that hardware tokens are resistant to malware-enabled scams, personal experience and feedback from residents are that it has been difficult to obtain such tokens from banks, with some customers having been informed that these tokens were unavailable or phased out entirely. I therefore ask the MAS to require banks to provide physical tokens without delay, if requested by the customer. It is also important that a kill switch (as set out in FI Duty #4) is available across all channels including by telephone or in-person and that the details of reporting channels be prominently displayed on bank cards, websites and banking apps to allow customers to quickly locate such numbers and stop unauthorised transactions. The MAS should also consider implementing an additional duty on responsible FIs to conduct further customer verification for any transaction that is identified as being suspicious. Banks have extensive transaction monitoring and screening tools at their disposal and the best course of action for all parties is to prevent the unauthorised transaction from occurring. Without such an obligation,

S/N	Respondent	Responses from respondent
		a major concern is that the FI duties will become the default standard of conduct as banks will not have any regulatory or financial incentive to go beyond the scope of their limited duties. An obligation to conduct further verification or "hold" suspicious transactions is not an onerous one. Banks can leverage technology to do this, and are already doing so.5 Such transactions could include, among others: (a) Repeated transactions to a new transferee; (b) Transfers of unusually large sums; or (c) Other transactions out of the usual course of business of the bank customer. (d) The MAS should also require all banks to provide customers with the option to ring fence funds that cannot be digitally transferred out of their accounts. The move by DBS, OCBC and UOB to provide this option is a practical one and I urge the MAS to make this mandatory for all banks inSingapore.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** A significant concern is that the waterfall approach may be construed as shielding banks from potential claims if the bank has fulfilled its duties in section 4 of the Draft Guidelines on Shared Responsibility Framework. To this extent, the clarification in paragraph 11.10 of the CP that dispute resolution bodies may consider duties beyond section 5 of the CP is welcome and necessary. The SRF should not set legal standards for banks and customers, but be seen as a quick remedial measure to compensate customers in certain limited circumstances. It would be helpful to set out the other factors that dispute resolution bodies may consider when adjudicating disputes, in the interests of transparency. This would allow consumers to assess the viability of a claim before commencing an action. Such factors could include, for example, whether the customer was elderly or vulnerable, whether the victim was put on notice of the scam at any point and / or whether any mitigating measures were taken.
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper.**

S/N	Respondent	Responses from respondent
		The 21 and 45 business day limits for investigations by responsible FIs and Telcos are a positive development. Such time limits are important to ensure that victims receive compensation promptly as they may have limited access to funds during this period. While I note this remains the subject of a separate consultation, the proposed amendments to the E-payments User Protection Guidelines (EUPG) are also a positive development. In particular, section 7 of the draft Revised EUPG that sets out the duties of FIs during the dispute resolution process are important. This is progress and the MAS should further consider how to safeguard victims during a dispute resolution process with an FI, given the unequal resources and bargaining power between the FI and the average consumer. However, I also urge the MAS to require pay outs to be made under the SRF without onerous settlement terms. I have received feedback that some residents have been asked to sign onerous non-disclosure agreements (NDA) before receiving pay outs. Pay outs under the SRF should be made without requiring customers to sign any waiver of their rights or NDAs.
		Question 9. **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.** The proposal for major payment institutions providing account issuance services to be members of FIDReC is a welcome development, particularly in light of the MAS proposal to increase to the stock cap and flow cap under the Payment Services Act 2019. FIDReC is an important, low-cost option for consumers to resolve disputes. With more transactions (and consequently, scams) involving e-money, this is a positive development for consumers.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** It is acknowledged that combating scams is complex and requires the balancing of the interests of multiple parties, including financial institutions and consumers. However,

S/N	Respondent	Responses from respondent
		there is concern that the SRF does not go far enough to safeguard the interests of bank customers. According to the SPF, phishing scams made up only 13.4% of scam cases in the first half of 2023. This was down from 17.1% in the first half of 2022. This means that most scam victims will go uncompensated as they do not fall within the scope of the SRF. With scammers becoming increasingly sophisticated, creating new frameworks for different scam typologies will mean that the regulatory landscape will constantly be playing catch-up. Legislating duties for responsible FIs will also be challenging for more complex scams like love scams and malware scams, which are becoming more common. For this reason, I reiterate my call for the Government to consider the CRM as explained in paragraph 1.3 above as well as more proactive transaction screening and monitoring (per paragraph 3.3) on the part of banks. A simpler and quicker solution is needed to ensure consumers are adequately protected and fairly reimbursed. While not directly within the scope of the CP, the MAS should also consider reforms to the FIDReC dispute resolution mechanism to better assist scam victims. For example, the limit of S$100,000 for adjudication needs to be relooked, along with the estimated timing for an adjudication of 6 months. A higher threshold of S$200,000 (the FAST transfer limit) should be considered and increased funding for FIDReC to allow claims to be processed faster.
28	Tan Eng Teck	**Question 8.** **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper.** How to ensure financial institutions judging or investigating each and every case in a neutral and fair way that is not incline to their own institutional benefit? same to telcos. Suggestion 1. FIs and Telcos must employ professionals from gov appointed source who responsible for the gov body and not the FI. It's like independent director in a company. Suggestion 2. When a case involve up to a certain amount of money lost, it automatically need to involve gov supervision body during the process of investigating. Suggestion 3. FIs and Telcos need to update the victim in all cases within a certain period of time frame regarding the investigation process and how they likely to judge the case. Not just remain uncontactable.

S/N	Respondent	Responses from respondent
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** All FIs and Telcos should invest together into a large pool of advance technology in this particular knowledge. Always stay ahead of the bad guys in term of knowledge and management TOGETHER and not alone or individually. They can consider hiring people from within the scam or fraud syndicates.
29	Tan Geok Lan	**Question 10.** **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** MAS's proposed Shared Responsibility Framework (SRF) Focus is off the Bullseye. This proposed initial framework mainly does not address all Authorised Push Payment (APP) scams (made up of about 70-80% of total scams based on SPF's 2022 statistics) which it differentiates from the phishing scams (that has both authorised and and unauthorised components). Minister Alvin Tan has mentioned the framework focus on the phishing scam as a start. This differentiation actually leads to distractions and complications in the implementations and the disarray of objectives. In addition, the glaring issues on the continuous abundant supply of mule accounts are not addressed nor are the "actors" (banks and mules) been made to hold direct responsible (which are unfair, with the exceptions of the mules whose accounts were used without consent). This is puzzling why the proposed SFR took 3 years to prepare (the actual proposal on the framework started in late 2020/early 2021, way before OCBC's phishing scam made the headlines in January 2022), and the aspects it address are so off the marks based on the objectives set. It is almost perfunctory. It left so many questions unanswered eg. It did not address the lapses/lax in AML practices by FIs and Singapore authorities in terms of international standards, which lead to the abundant supply of mule accounts as evidenced by the recent 2.8 billion ML case for the last few years. This major flaw in the Singapore's financial digitised ecosystem allows the bad characters to exploit is glaringly ignored if only the SRF only target the phishing scams (non-authorised). The main flaw in this framework is why the need to differentiate phishing scam from other types of scam?

S/N	Respondent	Responses from respondent
		One cannot help but suspect this is a distraction or delaying strategy to protect the FIs and those organisations such as telcos and social media owners who play complicit roles in the scams. It is clearly a wrong direction or a roundabout way to a solution. I beseech the SRF committee to ensure the framework to be simple but comprehensive to implement without compromising justice, compassion and fairness to scam victims. In fact, this draft is entirely unfair to all APP scam victims, which made up the majority of the scam victims and this actually deepened the agonies they suffered. This is clearly different from UK's framework which fundamentally addresses All APP scams as the lawmakers understood the definition of APP scam "APP scams happen when someone is tricked into making a payment to criminals posing as a legitimate organisation such as a bank, HM Revenue and Customs or the police. Scammers may also pretend to be selling goods or services that do not exist.
30	Tanla Platforms Limited	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** The SRF specifically targets phishing scams with a digital nexus in Singapore. These are defined as scams in which consumers are tricked into revealing their credentials on fake digital platforms, leading subsequently to "seemingly authorised transactions". For other types of scams, the SRF clarifies that the victims are free to seek recourse through existing channels. This focus on addressing a specific type of problem is understandable. However, it may be overly restrictive to address only the subset of phishing scams (in SMS) where the credentials are captured on an imposter website. Similar phishing attempts, but with a link to WhatsApp chat or a (fake) customer service number should be identified and disabled too because the larger objective of the SRF is to "preserve confidence in digital payments and digital banking in Singapore". The users may be unable to distinguish between subtypes of phishing techniques (Annexure 1). Being constantly targeted by scam messages, even when the messages are flagged as such on their devices, and being regularly reminded to be careful can also make them jittery. The confusion and anxiety so created is enough to erode trust in the online banking system. What is worse, the anxiety enables the scammer to trap the victim into taking the wrong action! Fortunately, the techniques that work against phishing scams with a digital nexus are also

S/N	Respondent	Responses from respondent
		effective against other variants. Therefore, MAS and IMDA may consider encouraging responsible FI's and Telco's to address the larger set of SMS-based phishing attacks through the SRF. Also, they may require Telco's to block all malicious messages in their networks, rather than on users' devices, thus guaranteeing universal coverage and protection.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** **Question 6.** **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** The SRF emphasizes the critical roles that Financial Institutions (FIs) and telecommunications companies (Telco's) play in protecting users, including their responsibility to compensate victims in cases of non-compliance with MAS and IMDA directives. However, this responsibility should fundamentally begin with a collaborative effort to identify and neutralize scams in real-time and to bring the perpetrators to justice. This collaboration should extend beyond mere regulatory compliance. For instance: 1. Real-Time Alerts and Transaction Monitoring: Telco's can provide real-time alerts to concerned FIs about potential phishing activities. FIs can then implement additional checks to prevent fraudulent payments or delay the transactions to allow investigations to catch, especially where the beneficiaries are private individuals or unregistered businesses. Where the recipient of funds is a large company, they can require additional verification before service delivery. 2. Collaboration with Technology Partners: Upon detection of a phishing link, Telco's or their solution providers should collaborate with partners like Google or WhatsApp to render the link inaccessible to all recipients, whether received via SMS or other channels. This broad-based approach can significantly reduce the reach and impact of phishing attempts. 3. Engagement with Law Enforcement: Law enforcement agencies should receive real-time reports of phishing attempts, increasing the likelihood of apprehending the culprits while they are actively engaged in the scam. Additionally, the permissioned distributed ledger

S/N	Respondent	Responses from respondent
		technology, that was implemented in India has witnessed a reduction is scam and has also been successful in preserving evidence and notifying stakeholders of phishing attempts in real-time. This technology can be suitably extended to support the operational workflow for claims under the SRF, ensuring a more efficient and secure process."
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** The principle that the responsible Financial Institution (FI) should bear full losses in case of any breach of duty is a significant step towards ensuring accountability in the digital banking ecosystem. However, this approach necessitates a more collaborative decision-making process involving both F'Is and telecommunications companies (Telco's). 1. Shared Responsibility and Decision-Making: Given that FIs are expected to bear the primary financial burden of breaches, it is logical and fair for them to have substantial input in selecting anti-phishing solutions implemented by Telco's. This involvement ensures that the chosen solutions are effective and tailored to the specific security needs and risk profiles of the FIs. 2. Funding Mechanism for Solutions: The funding for acquiring and operating anti-phishing solutions by Telco's should ideally come from the FIs. This arrangement not only aligns with the principle that those who derive efficiency benefits from digital processes should fund the security required to use of the channels, but also grants FIs decision-making power in selecting these solutions. 3. Alternative Funding Models: If it is decided that FIs should not bear the full cost, an alternative could be the creation of a pooled fund. Contributions to this fund could come from FI's, Telco's, and other stakeholders, with the fund being managed primarily by the FIs. 4. Demonstration of Effectiveness: Telco's should be required to demonstrate the effectiveness of various anti-phishing solutions to both regulators

S/N	Respondent	Responses from respondent
		and FIs. This process should involve a comprehensive evaluation against benchmark criteria, ensuring the effectiveness, cost-efficiency, and alignment with the FIs' security requirements. A transparent and evidence-based selection process is crucial for building trust and ensuring effective use of resources. 5. Regulatory Oversight and Collaboration: Regulatory bodies like MAS and IMDA play a pivotal role in overseeing and facilitating this collaborative process. Their involvement is crucial in ensuring that the collaboration between FI's, Telco's, law enforcement, and other stakeholders, such as take-down service providers, leads to a more resilient and secure digital banking ecosystem. In conclusion, a collaborative approach within the proposed waterfall model, with shared decision-making and responsibility, is essential for enhancing the security and integrity of Singapore's digital banking system. Such collaboration must involve not only FIs and Telco's, but also law enforcement and other stakeholders.
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper.** The proposed operational workflow for claims under the Shared Responsibility Framework, as outlined in Section 7 and Annex B of the consultation paper, provides a solid foundation. Integrating a (permissioned) distributed ledger into this workflow can significantly enhance its efficiency and effectiveness. 1. Real-Time Data Recording and Publication: Recording and publishing data on all phishing attempts in real time is crucial. This approach not only aids in building robust prevention strategies but also supports law enforcement in tracking down perpetrators. The immediate availability of such data ensures a proactive stance in combating phishing. 2. Comprehensive Data: Comprehensive data on phishing attempts, whether successful or not, constitutes essential background information and evidence

S/N	Respondent	Responses from respondent
		necessary for processing claims. This repository of information would be invaluable in assessing the context and legitimacy of each claim, fostering trust and transparency among all stakeholders. 3. Enhancing Efficiency: The implementing smart contracts can automate several aspects of the claims process, enhancing efficiency and reducing the potential for human error. This can coexist with human oversight at critical decision-making stages to ensure that the nuances of each case are adequately considered. In conclusion, the integration of a permissioned distributed ledger into the operational workflow for claims under the Shared Responsibility Framework offers a forward-looking approach. It not only speeds up the process but also ensures accuracy and integrity in record-keeping and decision-making.
31	Trust Bank Singapore Limited	**Respondent has requested for submissions to be kept confidential.**
32	You Technologies Group (Singapore) Pte Ltd	**Question 5.** **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** The recent Circular to raise the stock/flow cap for e-money issuers included additional anti-scam measures not within this consultation paper. (E.g. limiting of top-up sources and wallets linked to each top-up source) We would like to clarify if the duties of a responsible FI under the SRF be eventually aligned with the Circular's Annex? Or would these incremental requirements in the Circular not be considered when determining an FI's responsibility under the "waterfall" approach?
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** In relation to the Authority's proposed timelines to complete investigation under 11.7 of Annex B, we would like to seek further guidance on how the 21 and 45 business days requirements can be apportioned between FIs and Telcos, as well as whether FIs can apply their own interpretation of what constitutes to 'simple' and 'complex' case.
		Question 9. **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.**

S/N	Respondent	Responses from respondent
		We are supportive of the Authority's proposal in relation to being members of FIDReC.
32	ANOM1	**Question 6.** **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** I would like to add that telcos should be obligated to ensure all SIMs are issued with a PIN or at least, a SIM in which a PIN can be created. In addition, all telcos should have a 24hr hotline or at least a website for reporting lost or stolen phones. My phone was recently pickpocketed while I was in Kuala Lumpur. My Telco, SIMBA, and a few others, do not issue SIMs with PINs. It also does not have any easy means for reporting lost or stolen phones. As my SIM was unlocked, the pickpocket could have easily transferred my SIM to another phone and spoofed my identity. Apps like WhatsApp uses 2FA SMSs and my account could have easily been transferred and used to scam others. And because there was also no way to easily contact SIMBA other than their less-than-useful chatbot on their website, I had to fly back to Singapore the very next day just to get a replacement SIM so as to ensure my phone number would not be misused. I do hope you will be able to take the suggestions into consideration.
33	ANOM2	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** Given that most consumers use a so-called smart phone as their platform, and as such it supports all kinds of communications, like browsing, calls, SMS, MMS, chats and much more, in parallel accessing their accounts, **it is not clear why the scheme would exclude 'non-digital means (i.e., phone calls ..' as per 4.4(b).** MAS/IMDA may want to take into consideration that due to the other useful measures and controls, scammers and phishers have switched to **landline and office line** substantially more than before. Excluding these type of raising threats may leave out a substantial part of the scope, especially for the elderly who are among the main targets. MAS/IMDA may want to specify exactly what a 'non digital phone call' would be versus a 'digital phone call'. The same applies for text messages, especially in light of 4.3 where SMS text (as a form of text message) is clearly stated as example of the attack vector and probably the key element, because without the initial call/message the whole phishing attack would not take off.

S/N	Respondent	Responses from respondent
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** MAS/IMDA may want to explain 'high risk cool of in FI Duty #1 in more detail. FIs tend to send mails and SMS nowadays for the smallest amount and transaction, but also allow the user to set thresholds. It seems thus not clear when the 'high risk' would kick in and basing it on a message to the consumer by the FI does not seem a useful measure. As scammers work automated, it is very easy for them to transact small, non-triggering amounts in bulk and thus still reach high amounts, just like they do in exfiltrating huge data sets when attacking data bases. FI Duty #3 seems for many FI already a practice and has lead already to fatigue. It is not clear how 'real time' the alert would be anyway if it is per email. The consumer may not be online all the time. It would be more useful if this Duty would address the actual transaction, namely if a transaction to a new entity or new destination occurs, as it is rather unlikely that the scammers bank account etc. where he/she sends the money is already on the list of the victim. It would seem better to receive an OTP for new destinations, instead of swamping consumers with mostly meaningless messages, and expecting the consumer to go through each one and spot a scam.
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** Regarding the telco duties, a very efficient way to block any scam is to know the caller/sender. It would thus be of paramount importance that IMDA mandate that charging customers for showing caller-ID (and this comparing with the contacts on the phone etc) is not allowed anymore and must be a free service. If such a critical security component is not mandated, it is much more likely that scams continue to raise and the cost to the telco might in the end be higher. This is not only critical for scam and phishing, but an essential starting point for digital trust. It should not be the case that consumers must pay for the most basic security components in a push by MAS/IMDA to digitalise everything. This applies especially as technically savvy people are not even given the option to use alternatives like tokens, all the security and all apps are now focused on the one smart device, even the digital token.
		Question 10.

S/N	Respondent	Responses from respondent
		The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape. IMDA/MAS may want to also consider extending the scope to SingPass linked apps and lead the way there. Nowadays, even to go to swim in a public pool, one cannot pay cash and moreover needs an activeSG account linked to Singpass, and while swimming put the phone with all the security and apps and all .... yes, where? And in order to top up for swimming or gym, I must use the same security as to access my entire life savings in CPF. A two-layer security would be much more useful, such that the verification of the consumer is disentangled from the 'all or nothing' kind of access. There should be a type of credentials for small transactions and one for what you previously called a 'high risk' level. Thus, even if the phishing is attempted, which always appears as small amount and then exploits the 'all or nothing' to elevate to high sums, it cannot cross the barrier. Imposing actually good, sound and useful security on FI and telcos seems a much better solution for all than finding so many workarounds and waterfall responsibilties etc etc. as outlaid in the consultation and in many other schemes, which avoid the root problem. Singapore, known as a safe and secure country in the physical world, may want to be at the forefront to extend the same to the digital world by addressing the root of the problem and a rigorous penalty scheme. We are living in the 21st century and IT is not an infancy toy anymore; with the current approach of digitalisation and the attempt to push for Digital Trust, the workaround attempts outlined in the consultation paper seems to send the clear message that MAS/IMDA themselves don't believe a proper IT security is possible and that Digital Trust may not be on the horizon yet.
34	ANOM3	**Question 5.** **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** “12-hour cooling off period upon activation period of digital security token" Under the framework, the “Duty 1” of FI is to have a 12h cooling off period upon activation period of digital security token. Correct me if I am wrong, but I am under the impression that this measure only covers the 12h

S/N	Respondent	Responses from respondent
		period after scammers' attempt to take over the consumer's account by activating the digital token on a separate device. Am I right to say that it doesn't cover our normal everyday activity, meaning if I want to increase my transaction limit on any day to $200,000 and transfer it to some random guy, I can do so immediately without any restriction? If that's the case, I would like to suggest that we extend this 12h cooling off period to even the everyday, regular use of the banking app (not just for the 12h period when the digital token is activated on a separate device), as it will really be effective in helping ordinary consumers fight off scammers. Some scenarios: (A) Scammers often use scare tactics on victims, such as threatening victims to pay up immediately, otherwise their loved ones would be harmed; or to ""pay up immediately to avoid larger penalties/jail"". Under such circumstances, victims may not be able to think straight/clearly and would attempt to immediately transfer money to the scammers. (B) What if my device gets hacked into and scammers are able to remotely control my device? Of course, the current practice by the banks is to restrict access to the banking apps should unverified apps be found. But this is not foolproof. Scammers will get more sophisticated over time. So what if, despite all the current FI/Telco measures, they are able to gain control over our devices/banking apps via "verified apps" or some other means? In fact, UOB TMRW already has a 12h cooling off period any time we "add new recipients" while OCBC Digital app has a 12h cooling off period whenever we "increase transaction limits". However, UOB/OCBC (and all the FIs) can and should extend this 12h cooling period to include all the baseline set of high-risk activities such as "add new recipients", "one-time transfer of funds to non-registered recipients" and "increasing transfer limits". This, I believe, can go a long way towards protecting account holders from potential losses. With this feature, victims in scenario (A) would have time to consult their family members/friends/authorities before their money gets transferred out.

S/N	Respondent	Responses from respondent
		Similarly, in scenario (B), if hackers somehow gain access/control of my phone remotely, they would be unable to transfer out all my monies immediately. The hackers will still have to wait 12h...giving me time to contact my banks to freeze my accounts. [I would like to also suggest giving consumers who need to regularly transfer large sums of money or to frequently add new recipients, the option to deactivate this 12h cooling period feature if they wish, at their own risk ("deactivate" will only be effective 12h from time this deactivate option is selected).]"
35	ANOM4	**Question 5.** **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** Refer to FI Duty #2 and FI Duty #3, it is understood that the FI is considered fulfilled its SRF duties as long as the notification alerts is send by the FI to the consumer. However, it is not clear which parties is responsible in the event that the notification alerts is send from the FI but is delayed/ not received by the consumer. Some of the examples are listed below: 1. The Telco service provider used by the consumer is having a cellular/ data network outage. 2. The consumer is in a poor network coverage location such as basement carpark, underpass, outside of the main island (e.g. Lazarus Island, St John Island) or MRT/ expressway tunnels. 3. The consumer is travelling (on Plane) or overseas which is unable to receive local SMS notification alert or not subscribed to the data network services. The consumer might not be aware when there is a network outage or they are in a poor network coverage locations. In additional, some of the FI no longer use SMS to notify consumer and instead they use in-app notification where there could be a dispute in the event of Telco network outage or consumer are in a poor network coverage locations where the in-app notification timestamp will be displayed at the time of transaction but the consumer only received the notification when the Telco network service is available. The FI could assumed that the consumer received and ignore the notification.

S/N	Respondent	Responses from respondent
		Refer to Case Study 9 – Responsible FI did not send notifications for some transactions A: (FI - Sent Notification, Consumer - Received = Consumer Responsibility) - It is noted that the consumer did not notice the transaction notification alerts sent on the first 9 transactions and therefore the consumer will bear the losses for all the 9 transactions. B: (FI - Failed to Sent Notification, Consumer - Never Receive = FI Responsibility) - It is noted that due to a system issue encountered by the responsible FI, the 10th SMS transaction notification was not sent and therefore the responsible FI is expected to bear 100% of losses for the 10th transaction. C: (FI - Sent Notification, Consumer - Never Receive = ?? Responsibility) Based on the examples (1,2,3) listed above. It will be good if more details can be provided on the responsibility for item C mentioned above."
36	ANOM5	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** The scope of industry stakeholders defined in the paper is too narrow. (1) It should not be limited to FI and Telcos. Industry players like Apple, Google, Meta, X, Telegram and WhatsApp should be held responsible for scammers who use their platform for scamming. (2) The paper did not address this very important and prevalent issue. There should be processes to take down scammer accounts which can be activated by the public immediately to arrest scam attempts at the earliest possible time. If there is no financial responsibility imposed on these providers, then these providers will save $$$ and continue to let scammers operate on their platform. (3) "banks have announced that they will take a more forward-leaning approach towards assessing goodwill payments for customers affected by malware scams" This is insufficient. Most malware scams succeeded because banks

S/N	Respondent	Responses from respondent
		did NOT implementing a proper 2 factor authentication. Basically compromise the mobile phone and the scammer/hacker can access all the person's bank account. Banks are also not doing a lot of things that makes scamming harder to succeed. (4) It is proposed that MAS mandate that banks must make their customer to choose the following: (i) whether he/she wants to allow internet banking (ii) whether he/she wants to use hardware token for their internet banking account (iii) whether he/she wants to allow non-Singapore IP addresses from accessing their internet banking account Banks should not default any of these options. Rather they should let customer decide. When bankers are to advise, they are to advise on the SAFEST possible choice (ie. not most cost savings for the bank)
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** Duties of FI ==> Please refer to the above for things that FI can do beside notifications and cool-down period.
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** Duties of Telcos ==> Why is it limited to only SMS? (a) For malware, they need to send the stolen info to some website. Shouldn't Telcos be expected to block these sites? For that matter, there should be a public site for people to submit scam websites so that Telcos can immediately block it and prevent scam at earliest possible time. (b) Many of us are receiving robo scam calls pretending to be from Singapore Government. Shouldn't the Telcos be responsible for preventing these calls?
		There should be some form of punishment for FI and Telco if they breach SRF duties even if there is no loss in customer $$$. Basically, the government cannot just put out the SRF and then push the responsibility to FI and Telcos. Government need also to audit the FI and Telco."
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the**

S/N	Respondent	Responses from respondent
		Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper. For "Scams not perpetrated via SMS", responsibility of losses should be liberated (in court or negotiations) based on investigation findings. It should not be "Customer bears the loss in full." There are too many possibilities (e.g. some contentious process of the bank…etc) and so it is not fair to specifically pinpoint the customer.
		Question 9. **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.** I strongly support this MAS Proposal.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** Please look into crypto as that will be the future of the Internet payment.
37	ANOM6	Duties of a responsible FI, should include a mandatory 3 day hold on all foreign transfers originating from a retail account. A reasonable person would conclude that any foreign transfers out of Singapore (especially large) are out of the ordinary. Maximum transfer size limits have always been implemented for retail accounts. The default setting should be set at zero for outgoing foreign transfers and the change to that setting should be duly notified. FI should take extra steps to inform the elderly, the tech-illiterate and responsibly hold such change until informed to do so by the account holder or at least 3 days. This would give sufficient and reasonable time for a response. Responsible FIs can of course provide a service for accounts that make frequent overseas transfers but the default should be no outgoing foreign transfers without precedent of such recipient.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** Duties of a responsible FI should include a mandatory 3 day hold on all foreign transfers originating from a retail account. A reasonable person would conclude that any foreign transfers out of Singapore (especially large) are out of the ordinary. Maximum transfer size limits have

S/N	Respondent	Responses from respondent
		always been implemented for retail accounts. The default setting should be set at zero for outgoing foreign transfers and the change to that setting should be duly notified. FI should take extra steps to inform the elderly, the tech-illiterate and responsibly hold such change until informed to do so by the account holder or at least 3 days. This would give sufficient and reasonable time for a response. Responsible FIs can of course provide a service for accounts that make frequent overseas transfers but the default should be no outgoing foreign transfers without precedent of such recipient.
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** Responsible Telcos should by default remove all clickable links from SMS. They can of course provide a service that allow companies and persons to advertise via SMS.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** The waterfall approach fails to recognize that neither of 3 parties are truly responsible for the loss. A crime has been committed, laundered and co-mingled with either business, investing or gambling proceeds.
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper.** The operational workflow assumes that money lost are unrecoverable or traceable. It should be mindful of international practices so as to not lessen Singapore's claim to assets seized internationally by global enforcement or locally or have the perception that seized assets are not in fact belonging to victims in Singapore.
		Question 9. **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.** There should not be any difference in the duties that a responsible FI may have. No retail money should transfer overseas unless there is an explicit instruction. The unique case of foreign retail investment should allow for an expansion of an watchlist. Only legitimate companies will challenge inclusion. FIDReC is well poised to manage this as it reduces their case load.

S/N	Respondent	Responses from respondent
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** The shared responsibility framework should evolve into a prevention framework whereby there is a collective prevention and claim for all innocent parties. Ideally, the loss should be held first by FI, but such losses are insurable given the expanded duties as discussed and other steps taken. There is nothing unfriendly in the discussed duties, it is a question of perspective.
38	ANOM7	**Question 5.** **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** Disagree on the type of scam proposed to be in the scope. Because the operi modus of such scams (proposed to be in scope) are such that the consumers are required to undertake a number of steps including but not limited to entering his/her account credentials. In such cases, they are indirectly a willing party to this scam and undermines the same principle that years of public education to sensitise consumers to exercise caution and not click on dubious links and/or enter their account credentials. Everyone should be held accountable for their own actions instead of expecting others to pay for their own negligence and/or wilful actions.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** **Question 6.** **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** Agree that the proposed duties and anti-scam measures set out for financial institutions and Telcos that should be implemented to protect consumers against scams regardless of whether this framework is implemented.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** Disagree that the responsible FI should be placed first in line and is expected to bear the full losses if any of its duties have been breached. The overarching principle should be that the consumer should also be made

S/N	Respondent	Responses from respondent
		accountable for their own negligence. Also, when the FIs and/or the Telcos are made to bear such losses for the consumers, the consumers will no longer be incentivised to exercise appropriate caution to click on dubious links and entering their account credentials. This proposed approach severely undermines the principle of personal ownership and responsibilities. Over time, it further reinforces weak public digital behaviour and conduct. This proposed framework is like we put the responsibilities on the school and teachers by fining them when students play truant. If the government really wants to push forward with this "shared" framework to assist the consumers to defray the losses from such scams, consumers must be made to pay at least 50% of the losses.
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper.** The FIs and/or Telcos should not be involved in the process of handling and investigation of the claims made by the consumers as their involvement lacks independence. Also, they are restricted due to the privacy laws and other regulations to obtain information/documents from other parties involved as part of their investigation process. This role should be undertaken by an independent party with enforcement powers e.g. the police, etc.
39	ANOM8	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** The responsibilities of required by the FI is wholly inadequate given the current framework is responding directly toward the phishing scams popular in 2021 and only requires FIs to do the bare minimum expected of them today. However, in 2023, 2 years after this proposed framework was initially announced, we are well aware that scam landscape moves significantly faster than our legislative processes. Hence, it is necessary that we ensure that the framework is dynamic and incentivises the FI to invest in the required systems to effectively detect and prevent fraud. While the consumer must bear a certain degree of responsibility in this process, having a capped loss of perhaps a percentage amount of the scam loss will act as a sufficient deterrent in avoiding forms of moral hazard. With the FIs eroding the security tools put into place in

S/N	Respondent	Responses from respondent
		the past such as physical tokens or even bank books for our vulnerable members of society simply to cut costs, the scope of any SRF should be widened to ensure that these members are protected in a variety of scam types to maintain a healthy banking ecosystem. I am unconvinced that FIs can be trusted to self-regulated with the rise of malware scams.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** The responsibilities listed here are very static and are sorely lacking compared to regulations in other countries. Under this framework, scammers can continue to exploit mobile phones as a single vulnerable point and the FIs would be deemed as fulfilling all their responsibilities. Duties should include forms of real-time transaction analytics, AI fraud detection and other technologies that are in the market and are actively being adopted by top FIs in other countries. The current framework is weak, heavily favouring the FIs and is not comparable with frameworks adopted by mature governments such as the EU.
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** Incorporating non-FIs in the framework is a step in the right direction but given this is a situation arising from the actions of the banks and their reluctance to invest sufficiently in fraud detection, FIs should continue to the primary focus of the framework.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** The waterfall approach is pointless given the weakness of the framework in the earlier sections as all responsibility would likely continue to fall to the consumer. I would suggest that the scope is expanded to cover scams fully and that a formula should be put out to share scam losses between all parties involved to ensure that there is no moral hazard in the framework. Provisions can be put into place where it is clear that the consumer is highly negligent and where the institutions involved have adequately advised the consumer for the losses to be fully borne by the consumer.
		Question 8.

S/N	Respondent	Responses from respondent
		MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper. A responsible FI cannot be trusted to operationalise the proposed workflow without further guidance and oversight from MAS. There is no incentive for the responsible FI to be fair and transparent in their dealing with the consumer and they may impose unfair terms to the vulnerable consumer prior to the recourse stage. Responsibilities need to be clearly laid out in much greater detail than listed with clear timelines and ideally an independent party should be involved from the initial stages. In my experience, a certain national bank has been evasive and uncooperative with a scam victim with unprofessional handling of the recourse process and took significant time to hand over basic information that is available on all our ibanking apps.
		Question 9. **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.** Including more institutions is good but more needs to be done to ensure the transparency and fairness of FIDReC. Consumers need to be enabled to have greater faith in the fairness of the organisation and this can be done by having a board of directors that are not heavily connected to the FIs under its purview and a more detailed breakdown of cases and results handled by them. FIDReC should also be enhanced to allow more vulnerable consumers to be better protected and guided through their processes.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** Ideally, the SRF should be dynamic and covering all scam variants through broad guidelines given the purpose of such legislature is to enhance the trust consumers have in ePayments. In its current form, the direction appears to be telling consumers to feel protected against phishing scams but continue to have your life savings at risk for all other matters. If a comprehensive framework is not feasible, kindly

S/N	Respondent	Responses from respondent
		consider provisions for retrospective action to be made possible to incentivise FIs to move quickly in responses to new scam variants. For instance, with the recent Malware scams, OCBC was much faster than other FIs in rolling out their fraud prevention measures relative to other banks who took a few additional months. If we could hold banks fully responsible for fraud losses that could have been otherwise prevented if they took speedy action, this would be a step in the right direction for the ecosystem.
40	ANOM9	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** Whilst we try to educate our aged parents to be discerning and vigilant, it can be challenging to 'update' them on the latest modus operandi in a timely manner. We will therefore not install any online banking or payment apps on our parents' mobile phones and will instead install the apps on our mobile phones to help them in their banking and payment transactions. Unfortunately, this is not feasible as FIs do not allow us to have more than 1 app in each mobile phone. For instance, (a) I have a DBS account and (b) my mother has her own DBS account. I cannot download 2 DBS apps on my mobile phone to authorise payments from my own account (a) and from my mum's account (b), for our respective purchases. Pls allow each mobile phone to install more than 1 app from the same FI or consider a 'caregiver' authorising arrangement similar to Healthhub app concept so we can help our parents minimise the risk of falling victim to scams.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** Notification alerts via apps require data access. There could be instances when victims are overseas with no data roaming service. The SMS channel should therefore not be decommissioned.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** SRF focuses on responsibility per incident. FIs should also be assessed and complemented/sanctioned publicly

S/N	Respondent	Responses from respondent
		based on their overall track record and control proactivity. FIs have the resources and surveillance mechanism to keep track of the latest trends and suspicious activities. They charge fees and earn margin from funds placed with them. They have an obligation to implement controls and protect customers' funds. Rather than devoting resources to Legal and Compliance teams to deflect responsibility (and tick the SRF boxes), FIs should allocate budget for customer education and implementation of controls to address the latest scams. This is one of the accessible KRI/KPIs that should be taken into account to help consumers decide which FI to keep their funds with and motivate FIs to be more proactive.
41	ANOM10	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** Don't think it is wise to rely on the FIs and Telcos to adopt it voluntarily. These entities are too powerful and do not respect the Government. Should go for legislative powers.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** FIs should be held to higher standards over Telcos when they hold the key to our savings. FIs should be motivated by legislation to improve their digital infrastructure. FIs should provide physical tokens to those who opt for it such as the elderly instead of saving costs.
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** Duties expected of Telcos are reasonable but not so sure if they will comply and the penalties. Should educate the public more on IMDA's regulatory powers. Telcos should not charge for caller ID, which would help consumers to identify scam signs.
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper.** Great ideas. They should be held accountable and not be on a voluntary basis. Not sure what legislative powers the

S/N	Respondent	Responses from respondent
		Government have over FIs and Telcos to get them to comply.
42	ANOM11	**Question 5.** **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** FI and relevant stakeholders should also engage in anti scam education measures and encouraging their customers to do so through their core offering. For instance, having consumers (especially those in high risk of being scammed - ie high concentrated amount in their saving accounts) to open separate bank accounts or debit cards used solely for online purchases can reduce their risks considerably by decentralising their savings best egg.
43	ANOM12	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** Service providers offering e-wallet services or e-payment accounts: Hope it extends to platforms such as Shopee's MARI, StanChart's Trust Bank. Despite the losses that consumers faced in buying prepaid packages, the regulators have continued to apply light-touch oversight even though these are also "wallets" or "store value" mechanisms. Perhaps similar onus should be put on such service providers or vendors (eg, I take a photo of the job sheet after each hairdressing visit under a prepaid package just to provide a back-up record in case the biz owner decides to "consume" the remaining balance to cheat or short-change customers).
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** ABS/MAS could do better to require Hotlines to announce the option number at the start of the system-recorded message. UOB hotline rambles on before giving the report scam option number without understanding that the victim may already be frantic and in panic mode. All FIs must be compelled to issue a physical token as diversification of device is one method of thwarting scammers as the OTP is generated by the user and is not visible to the scammer/hacker's mirrored screen. Better yet, Assurity physical token could be improved with additional buttons to pre-link to selected FIs (Button 1 for Bank A A/c 1 selected by user, Button 2 for Bank B A/c 2, Button C for Bank C A/c 3). All FIs should be required to default the alert quantum at 1 Singapore cent and then let users log-in to up the limit (now, it could be defaulted

S/N	Respondent	Responses from respondent
		at $1,000 and users have to log-in to reduce it to 10 cents).
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** Telcos should be obliged to "whitelist" all Govt entities' telephone numbers as I discovered that important telephone calls from Hospital Clinics to my HP were tagged as "Scam calls" because some user previously/mischievously tagged such caller numbers as "scammers". Telcos should NOT mask the caller ID on land lines as "Private" because that is preventing me from reporting land line telephone calls via the ScamShield app. For prepaid card holders (usually used by the elderly or the low-paid workers), all incoming SMSes should be FREE so as to alert account holders in case of unauthorized spendings or withdrawals. Am not sure if AI technology could be applied to detect if the link embedded in e-mail or SMS or WhatsApp chat when clicked upon would link to malicious activity (e.g., blinking icon is not good enough) - the telco should auto-disable and auto-terminate such clicked link and send Red Alert to user to shut down HP or PC immediately or at least xx hours.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** Waterfall" approach is fair enough. But users should also bear full responsibility if they have been negligent - eg, shared passwords, too simple passwords, allowing others to use their devices or their user names/accounts. One area that requires attention is the elderly who may be dependent on caregivers or institutional staff to help with banking transactions (maybe once such HP/device owner is medically tagged as vulnerable but before the stage of LPA donees stepping in, the FIs could allow such medically tagged persons to register a specified caregiver with ID/face/fingerprint identification fully captured for future tracing/enforcement and/or immediate 2nd-level verification by the HP/device owner through a video call if the amount is above $xxx/txn or an aggregate $yyy/day).
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the**

S/N	Respondent	Responses from respondent
		Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper. The service provider of e-payment or e-wallet facilities should be auto-looped in by the FI (eg, Grab Food/Taxi, FoodPanda, Shopee, Comfort Taxi, etc) should be roped-in by FI upon receipt of scam/hacking/phishing report. Then these platform owners should also do the necessary to protect the victims' accounts on their e-commerce platforms. FIDReC seems unapproachable to inquiries - could do better to be reassuring and helpful (rather than send callers on wild goose chase). Is FIDReC charging high fees to victims upfront or should FIDReC recover their charges upon successful clawback?
		Question 9. **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.** Yes, any entity that stores money (be it inn the form of credits, dollars, prepaid, store-value) should all be members of FIDRec so as to improve their awareness and their focus on governance and strong web/app design. Also, there is too much splintering of govt depts involved in cybercrime - is Govt trying to create jobs to boost employment numbers? Whilst I appreciate each of them specializes in certain focal/expertise areas, they should be consolidated under one cyber-security umbrella (e.g., GovTech) to operate in similar manner to OneService for municipal issues.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** Govt should mandate that the major ISPs and device manufacturers do NOT offer the default option of "saving passwords" or updating their software/firmware to auto-copy screens (this was what happened after I updated my Samsung firmware about a year ago - which totally freaked me out). Where organizations have breached Data Protection (eg, Ageing Asia Pte Ltd who committed such a brazen violation) or caused users' data to be breached due to a variety of reasons (eg, weak governance, improper choice of sub-contractors, malicious or careless employees in Singtel and Singhealth, etc) and a fine was imposed by the regulator, then 80% of the fine should be distributed to all the affected names with 20% retained by the

S/N	Respondent	Responses from respondent
		regulatory/enforcement authority - even if it means only $0.30 credited, it serves as a record and reminder to the user to be extra wary as his/her details were already leaked).
44	ANOM13	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** Recommend scope should also include organisations/companies that provide mobile application services. They need to be responsible for the security of their application in the event someone hacks the software and is able to communicate to a person through an existing (trusted) chat thread or should 1 day, banks/telcos make use of such communications applications (e.g. Whatsapp) as their primary mode of communications to replace the SMS. If I follow your logic of making Telcos responsible in timely notifying the user, then that is the same basis I am recommending including such software companies. If you go on the path of holding banks and telcos responsible only, and it is for them to go after such software companies for any breach, then you are likely going to end up with companies feigning ignorance that they should be responsible, especially in the scenario described above where someone is able to break through and chat using an existing thread you have with someone (e.g. with your mother).
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** Recommend that the FI should also provide a channel for the consumer to add an additional path to notify someone else (e.g. a trustee such as children of the aged) if such security tokens are activated and these alternate paths should take a longer time to be changed, beyond the 12 hours, e.g. 3 days such that the scammer cannot immediately delete these people to be notified.
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** Recommend Telcos also be made to deploy advanced systems such as AI to detect patterns of these rogue SMS messages.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** Agree on the waterfall and recommend it should also include the software companies I described above in

S/N	Respondent	Responses from respondent
		section 1. That should be right after the telcos. In addition, I would recommend including the entity(s) that designed and approved the enterprise architecture of these digital systems and corresponding workflows. Well, it could very well be the bank but what if the bank performed consultation with consultant firms or even CSA and they blessed the design? By enterprise architecture I am referring to the TOGAF standards equivalent. These entities should come right before the bank in the waterfall sequence as that is the source of today's problem in my opinion. Let me explain. The consumers had no real say wrt to the digitalisation push by both the government and the banks which has brought us to where we are today, on the relentless push for digital first for the sake of digital without due consideration of financial safety/security. Think back to the days when there is only web portal and SMS OTP with no mobile app. The scammer needs to invest in a lot of social engineering and there are opportunities for banks to safeguard at the various steps. Scammers are also forced to potentially show up at the bank with the victim (reference today's news report on UOB staff stopping a scam when they sense the person accompanying the old lady was not who he said he was). Minimally you would get CCTV and facial recognition for our good SPF lads to chase down in our well ring fenced SG boundaries. Taking a leaf from CSA, it is apparent that there was no equivalent of cyber security by design (as a concept) when it came to rationalising the concept of 2FA/MFA in the critical business workflow in the mobile application. Who approved such a design that the SMS OTP / digital token can be in the same mobile device, which to me runs in the face of the fundamental concept of 2FA/MFA. Where is the air gap? What were the consideration of the entity(s) in approving such an enterprise design/workflow to allowed in the first place? Yes I am kind of alluding to the phasing out of the physical tokens which again, consumers had no real say to block. There must be apportioned responsibility for the folks who design and approved the enterprise architecture. The consumers didn't design nor approve the business, data, application and infrastructure architecture in the whole enterprise architecture. Why should they bear 100% liability in certain scenarios when the enterprise architecture had created the latent condition (for an accident to happen) in the first place which were not the consumers' doing?
		Question 9.

S/N	Respondent	Responses from respondent
		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. If your payment institutions are separate entities that have business dealings with the FIs, would this not constitute conflict of interest? Why would they rule against the FIs which they have a contract to provide other services?
45	ANOM14	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** With reference to section 4.4 (a) scams where victims authorise payments to the scammer will be excluded from SRF. Despite the crime can equally happen in the non-digital world, we must take into consideration of the source of information is derived from digital platform whereby there is no authentication done by the digital platform. I am referring to rental scam. This Shared Responsibility Framework only cover those losses made via FI's platform. What about those rental scam victims?
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** The duties of responsible FI seem to be focus on digital token activation and transactions real-time notifications. Based on news, it seems that many fraudulent transactions are done at night and not many users can immediately read their notifications due to other commitments. Therefore, I would like to suggest responsible FI to set a time limit for fund transfer delay and provide funds transfer instruction notification alerts based on real-time basis. E.g. User set a "Funds Transfer Delay" of 6 hours. He transfers $10,000 on a FI platform at 11am. He receives the notification alert of the funds transfer instruction at 11am and the funds will be transferred out from his bank account at 5pm.
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** Grey area in term of notification alert in real-time - duties falls under MNO or Telco or FI. Responsible Telco and FI will deem that they have sent out the notification alert in real-time basis. However, victims might be at a location whereby the cellular connectivity is poor.
		Question 8.

S/N	Respondent	Responses from respondent
		MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper. I think it is more efficient to set up an independent department to handle the claim process so that liaising would be less stressful on FI and victims. In reference to diagram 2 on outcome stage for scams perpetrated via SMS, despite responsible FI/Telco inform victim of outcome of investigation, keeping responsible Teleco/ FI in the loop might have time lapse informing the victims which will further distress the victims. "Scam Claim" department will be better (on-the-job) trained on the information required in liaising with all parties from the experience.
46	ANOM15	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** 1. We note that the draft Guidelines on SRF states at footnote 1 that "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 responsibility sharing set out in these Guidelines do not apply to transactions on credit cards, charge cards and debit cards issued in Singapore." We note that the ABS Code of Practice for Banks is currently meant to apply to banks, and does not seem to apply to other responsible FIs such as payment service providers hence we would appreciate MAS' clarification on the applicability of the ABS Code of Practice for Banks - Credit Cards for non-bank responsible FIs. In particular, for phishing scams perpetuated through the debit cards of payment service providers, is it intended for the SRF or the ABS Code of Practice for Banks - Credit Cards apply? 2. We note that paragraph 4.2 of the CP on Proposed SRF states that "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." We would appreciate MAS' clarification on whether customers of responsible FIs who are foreign residents and receiving the services overseas would also be within the scope of the SRF.
		Question 5.

S/N	Respondent	Responses from respondent
		MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper. We note that FI Duty #1 requires that FIs impose a 12-hour cooling off period upon activation of digital security token during which 'high-risk' activities cannot be performed. This seems to presuppose that a digital security token is issued by FIs. We would appreciate MAS' clarification on - (a) Whether it is MAS' intention to require all responsible FIs to issue such a digital security token to their consumers; and (b) If not, whether and how would the 12-hour cooling off period would apply to FIs which do not issue digital security tokens to their consumers.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** We agree that FIs do hold an important role in addressing scams as custodians of consumers' money and should take on the responsibility to the extent that the FI's lapse(s) results in a phishing scam being successfully perpetrated. However, where both the responsible FI and the responsible Telco have breached SRF duties, especially where the responsible Telco's breach contributes significantly more to the consumer's loss, there should be a more proportionate method in allocating the loss between the responsible FI and the responsible Telco to ensure that both parties' duties are fairly recognised and that each party is held accountable for fulfilling their responsibilities. This will better help to ensure that all responsible parties put in their best efforts to perform their duties in supporting the multi-layer strategy to combat phishing scams.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** We appreciate the clarity provided by the proposed operational workflow and timeline. We note, however, that the process may require the account holder to provide information and would like to clarify on how the timeline in the proposed operational workflow should be implemented if there is a lag from the account holder in providing the required information to the responsible FI for its assessment of the claim. For clarity to consumers, we recommend that the 21 business days for straightforward cases and 45 business days for complex

S/N	Respondent	Responses from respondent
		cases should commence from the date that all required information is provided by the account holder. Alternatively, the timeline can commence from the initial date that the claim is first made, but the FI should be allowed to pause the time when it is pending the account holder's response.
		Question 9. **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.** We are supportive of major payment institutions being members of FIDReC as it provides another avenue for fair dispute resolution. We note, however, that major payment institutions may also provide payment services other than account issuance services and would appreciate MAS' clarification on whether disputes relating to payment services other than account issuance services provided by a major payment institution would also be subject to the jurisdiction of FIDReC.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** We agree that currently in the majority of cases, the responsible FI, responsible Telco and/or the victim should be allocated liability for the digitally-enabled scam. However, given the growing complexity of digital payments and transactions and digitally-enabled scams, the SRF should also consider whether there is any scope for including other parties (aside from the responsible FI, the responsible Telco, and the victim) which may be involved in the process to be allocated liability in the future.
47	ANOM16	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** We respectfully propose that the scope of banks be clarified to include local banks and qualifying full banks, in addition to full banks.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** In relation to the duties of Responsible FIs in Paragraph 5.4, beyond the 12 hours, we respectfully propose for FIs to implement additional filters to alert the FIs to take actions or restrict consumers to physical banking if out-

S/N	Respondent	Responses from respondent
		of-the-norm activities (for example, multiple transfers out of bank account within a short amount of time such as 30 minutes) occur. In relation to Paragraph 5.7, we are of the view that the kill switch function may cause difficulty in authenticating the user of the kill switch. FIs can perhaps consider allowing users to have different credentials to activate the kill switch.
		Question 6. **IMDA invites comments on the duties of responsible Telcos in Section 5 of the consultation paper.** In relation to the duties of Responsible Telcos in Paragraph 5.12 and Paragraph 5.13, we respectfully propose for Telcos to send an additional SMS i.e. Real-time alert to warn users that the preceding SMS could be a scam. The alert can be triggered based on keywords identified in the previous SMS.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** We further propose that there should be mandated periodic checks or audits by an independent party/function on the teams that assesses consumer claims.
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper.** Please find below our comments on the proposed operational workflow: - We respectfully seek MAS' clarification if all cases indicated under Annex A can be categorised as "straightforward" and "complex" cases would be those that do not fall under Annex A. - We respectfully propose that there should be implications/consequences where the investigation periods for cases have lapsed for both the consumer and responsible FI/Telco. For example, when the onus is on the consumer, but they do not cooperate within the timeframe, the case can be taken as defaulted. When the onus is on the FI/Telco, and they do not progress the investigation within the timeframe, the FI/Telco should payout to the consumer the losses suffered.

S/N	Respondent	Responses from respondent
		- If the responsible FI is an SPI/MPI providing e-money payment services and does not bear the responsibility of the consumer's loss, we note that the consumer has limited recourse as the responsible FIs are not members of the FIDReC.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** We respectfully suggest having a reimbursement process, including setting out a standard reimbursement timeframe once the investigation is completed and obtaining the consumer's acknowledgement. The shared responsibility framework can also consider enhancing the awareness of scams to users to mitigate the risk of evolving scams. For example, payment services such as Grab, Youtrip, Paypal etc can include a pop-up notification or disclaimer on their websites, mobile applications or via email to users to remind them about the evolving scams.
48	ANOM17	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** Under the SRF, the losses incurred by consumers in scams are highly dependent on timely notifications from FIs. To ensure that consumers are notified promptly, can a FI use multiple methods to notify its clients simultaneously
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** a) Due to the complexity of SMS transmission or other mechanisms of push notifications, consumers may not be able to receive the notifications or experience delays due to poor network coverage or their own mobile device problems. Can a FI be exempt from liability if it can demonstrate that it has taken reasonable steps to send notifications? (Case 8 and 9) b) In the case of a consumer being scammed due to a spoofed sender ID SMS, the FI should take full responsibility because it failed to notify its client in a timely manner, despite having already registered the Sender ID to SSIR and taking other measures to protect the consumer. However, does the SSIR or Telco also have a role to play in ensuring that the consumer is protected and may is responsible for their

S/N	Respondent	Responses from respondent
		failure to safeguard the connection from aggregators? (Case 13 and 14)
49	ANOM18	Note: Separate responses was provided to MAS.
50	ANOM19	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** May I suggest SMS be one of the default real-time notification mode or giving account holders a choice– SMS, Email and/or In-app Notification. b) Real-time notification alert is meaningful only if the account holder is in control of his handphone When online banking, security token for OTP and transaction alert are all on the same device (the handphone), the alert is meaningless when the account holder has lost control over his handphone to a scammer. It is like hanging the key and password next to the safe that is monitored with a faulty CCTV. Account holders are the first line of defence to secure their accounts against scam. A physical token gives them the sole control over their accounts during online banking. In the event that the handphone is compromised in a moment of inattention, the scammer will not be able to perform online banking without the OTP from the physical security token. A physical security token also empowers account holders who choose to exercise more caution by having separate devices for different purposes. May I appeal to MAS to strongly encourage the banks to give account holders the option to have/continue the use of physical security token for online banking.
51	ANOM20	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** Para 4.6 of the Consultation Paper ("CP") 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)." a. Is there an expectation for all banks to have a framework for goodwill payments (for example, in financial hardship cases) when the loss did not arise from the fraud or negligence of the FI or its employees or agents? b. Paragraphs 4 and 8 of the CP state the types of scams covered and the related approach. However, we note that these are not indicated in the draft guidelines. For clarity, we propose to state the same information in the draft guidelines.

S/N	Respondent	Responses from respondent
		Footnote 1 of the draft SRF guidelines states that: "1 The Guidelines applies to accounts opened with the retail segment or entity of the responsible FI". We have interpreted this footnote to mean that only sole proprietors that reside within the retail segment of the bank will be governed under the SRF Guidelines. Where sole proprietors reside under the bank's wholesale segment, we would assess any disputed transactions based on the bank's internal procedures or guidelines, unless otherwise clarified by MAS.
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** 1. Regarding FI duties #2 and #3 to provide notifications on a real-time basis, do these duties override a customer's chosen notification preferences e.g., if a customer has chosen not to receive any notifications, does the FI still have the duty to notify of such high-risk activities? 2. In the event that the FI have fulfilled our duties but there are lapses from Telco, we assume that FI will not be responsible for the losses. Please confirm our understanding.
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper.** 1. If an opinion is made by an adjudicator as to telco's liability in the course of a FIDReC hearing/decision, will the customer be able to take said opinion to IMDA or the telco? Bearing in mind the confidential nature of FIDReC proceedings. 2. Apart from a responsible FI being the first and overall point of contact with the consumer, will the Regulator set up an ombudsman to facilitate the handling of claims that could involve more than one FI.
		Question 10. **The Government welcomes comments on how the Shared Responsibility Framework should evolve, taking into account the changing scams landscape.** 1. With reference to Annex D of the CP, noted that "Australia announced in May 2023 that there will be a mandatory co-regulatory code developed by the Australian Competition and Consumer Commission that

S/N	Respondent	Responses from respondent
		involve banks, telcos, and big social media platforms to mitigate scams." In a similar light, will MAS consider social media platforms (e.g., WhatsApp, FB, IG, WeChat) as part of the responsible parties to be liable for the losses, in addition to the responsible Telcos? 2. The SRF must not lull consumers into a false sense of security. It should be the ultimate safety net for consumers and not the first port of call. 3. If not already considered, could the Government consider upstream digital financial literacy/ cyber hygiene programs in primary, secondary school education; and, as part of community education programs for the elderly. For instance, people must be aware that they need to upgrade the minimum operating system of their phones; download anti-virus software etc.
52	ANOM21	**Question 5.** **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** Under FI Duty #1 point 5.3, do FIs have the flexibility of imposed a stricter cooling period which is longer than 12 hours? If so, suggest to rephrase to 'F1 Duty #1 : Impose a minimum cooling off period of 12 hours upon activation of digital security token during which 'high-risk activities cannot be performed.' Suggest to align with the definition in the proposed enhancements to the E-Payments User Protection Guidelines ('EUPG)' where it states that when a digital security token is activated, a responsible FI should : (a) impose a minimum 12-hour cooling off period, during which high risk activities cannot be performed…..". Under FI Duty #1 point 5.3 , do FIs have the flexibility of imposed a stricter cooling period which is longer than 12 hours? If so, suggest to rephrase to 'F1 Duty #1 : Impose a minimum cooling off period of 12 hours upon activation of digital security token during which 'high-risk activities cannot be performed.' Suggest to align with the definition in the proposed enhancements to the E-Payments User Protection Guidelines ('EUPG)' where it states that when a digital security token is activated, a responsible FI should : (a) impose a minimum 12-hour cooling off period, during which high risk activities cannot be performed…..".

S/N	Respondent	Responses from respondent
		Under FI Duty #4 point 5.7, do the blocking of accounts refer to the retail banking account or the digital banking account? Also, are there any baseline guidelines on the types of channels available for customers to perform the kill switch? Under the proposed enhancements to the E-Payments User Protection Guidelines, the kill switch is defined as 'a self-service promptly block his account from digital access'. Suggest to align the definition in the SRF and enhanced EUPG for consistency."
		Question 9. **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.** Referring to points 7.1 (a) and 7.2, in the event that the FI has fulfilled all its SRF duties and the Telco has breached the SRF duties, it may be more efficient to define the engagement process for the Telco to front the victim for such scenarios and inform the victim directly on the status of the investigation. The FI involved may be kept in the loop on the outcome of the investigation. Reason is that the FIs are not privy to the telco's internal SLA and processes for such scam investigation and goodwill payouts.
53	ANOM22	**Question 5.** **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** Responsible FIs have duty to provide notification alerts on a real-time basis for activation of digital security token, high-risk activities and outgoing transactions. However, there are dependencies on Telcos as infrastructure providers to ensure service availability for the delivery and receipt of notification alerts (via SMS, email or push notification) by FIs and account holders real-time. In this regard, the Bank would like to seek MAS' consideration to include such dependency as one of the duties of responsible telcos in Para 5 of the draft SRF guidelines.
		Question 7. **MAS and IMDA invite feedback on the "waterfall" approach for sharing responsibility, outlined in Section 6 of the consultation paper.** All responsible parties have collective responsibility as industry stakeholders in dealing with scam threats. We are of the view that it would be more appropriate to assign the sharing of losses based on the parties that have

S/N	Respondent	Responses from respondent
		breached the SRF duties. This will encourage accountability and have a positive effect in the prevention of scam. In cases where both parties fail in its duties, then joint responsibility should be assumed.
		Question 8. **MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper.** The Bank noted that Responsible FIs will be the first and overall point of contact with the customer and the timeline to complete investigation of any relevant claim within 21 business days for straightforward cases, or 45 business days for complex cases. In this regard, the Bank would like to seek MAS' consideration to establish a timeline for telcos to provide the Responsible FIs with their investigation outcomes (for cases where scams were perpetrated through SMS) to allow the Responsible FIs sufficient time to conclude the assessment and provide a written reply to the account holder by the stipulated timeline.
54	ANOM23	**Question 9.** **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.** We understand that FIDReC supports a wide range of use cases between FI and consumer concerns. The participation of MPI's with FIDReC should be limited to scam related mediation as per the SRF scope for starters. Nonetheless, we are supportive of this proposal.
55	ANOM24	**Question 4.** **MAS and IMDA seek comments on the scope of the SRF in Sections 3 and 4 of the consultation paper.** We seek to clarify the definition of "consumers" mentioned in 3.2, particularly, whether it is meant to only include individuals or does it also cover corporate entities. Unlike individual customers, the applicability and implementation of FI duties set out in subsequent sections may be difficult to fulfil for corporate customers. As a practical example, corporate entities may have multiple administrators for a single payment account which may give rise to practical challenges such as whether the "kill switch" should be made available to all administrators etc. Although not impossible, the likelihood of a corporate entity succumbing to phishing scams is lower as corporate entities typically have their own risk and control mechanisms to mitigate against such

S/N	Respondent	Responses from respondent
		fraud risks (for instance, by having a multi-layer approval matrix for high-risk transactions).
		Question 5. **MAS invites comments on the duties of responsible Financial Institutions in Section 5 of the consultation paper.** We wish to clarify that, for a financial institution to meet the requirements of FI duty #4, it is not necessary for the 24/7 reporting channel to be staffed (manned by an individual) around the clock, provided that there is an avenue for such reporting. This is because implementing such a practice would impose a substantial operational burden and cost. If this is not the expectation, it is presumed that the specified timelines in table 4 of the proposed EUPG would then still apply.
		MAS and IMDA seek comments on the proposed operational workflow for claims brought under the Shared Responsibility Framework, outlined in Section 7 and Annex B of the consultation paper. We seek clarification on whether FIDReC would offer a platform for financial institutions (FIs) to notify a responsible Telecommunications company (Telco) when a claim is submitted. Specifically, in the absence of FIDReC, is there an expectation for FIs to individually contact each Telco for every claim? If this is indeed the case, Tenpay Global suggests the creation of a dispute management platform encompassing FIs and Telcos. Such a platform could enhance the efficiency and effectiveness of fraud management frameworks, as well as alleviate the challenges faced by distressed consumers who have fallen victim to phishing scams.
		Question 9. **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.** We have no 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. However, if the earlier suggestion (as mentioned in question 4) regarding the establishment of a dispute management platform proves unfeasible at this juncture, we propose that Telecommunications companies (Telcos) also become part of FIDReC. This approach would involve a single entity overseeing the entire process of disputes, ranging from the claims stage to resolution, thereby streamlining

S/N	Respondent	Responses from respondent
		the entire chain and improving the experience to the consumer.