

**LIST OF RESPONDENTS TO THE CONSULTATION PAPER ON
PROPOSED E-PAYMENTS USER PROTECTION GUIDELINES**

1. American Express International Inc, who requested for their comments to be kept confidential
2. Consumers Association of Singapore (“CASE”), who requested for their comments to be kept confidential
3. The Hongkong and Shanghai Banking Corporation Limited, Singapore Branch (“HBAP SGH”) and HSBC Bank (Singapore) Limited (“HBSP”), who requested for their comments to be kept confidential
4. Linklaters Singapore Pte Ltd on behalf of the Singapore FinTech Association
5. Network for Electronic Transfers (Singapore) Pte Ltd, who requested for their comments to be kept confidential
6. OCBC Bank, who requested for their comments to be kept confidential
7. PayPal Pte Ltd, who requested for their comments to be kept confidential
8. Sidley Austin LLO on behalf of Alipay Singapore E-commerce Private Limited, who requested for their comments to be kept confidential
9. SingCash Pte Ltd, Telecom Equipment Pte Ltd, Singtel Mobile Singapore Pte Ltd, collectively known as “Singtel”
10. The Association of Banks in Singapore
11. Visa Worldwide Pte Ltd, who requested for their comments to be kept confidential
12. Respondent 1 who requested for confidentiality of identity
13. Respondent 2 who requested for full confidentiality of identity and submission.
14. Respondent 3 who requested for full confidentiality of identity and submission.
15. Respondent 4 who requested for full confidentiality of identity and submission.
16. Respondent 5 who requested for full confidentiality of identity and submission.
17. Respondent 6 who requested for full confidentiality of identity and submission.

18. Respondent 7 who requested for confidentiality of identity
19. Respondent 8 who requested for confidentiality of identity
20. Respondent 9 who requested for full confidentiality of identity and submission
21. Respondent 10 who requested for full confidentiality of identity and submission

Please refer to [Annex B](#) for the submissions.

**FULL SUBMISSIONS FROM RESPONDENTS TO THE CONSULTATION PAPER
ON PROPOSED E-PAYMENTS USER PROTECTION GUIDELINES**

S/N	Respondent	Response from Respondent
1	American Express International Inc, who requested for their comments to be kept confidential	Requested for their comments to be kept confidential
2	CASE	Requested for their comments to be kept confidential
3	The Hongkong and Shanghai Banking Corporation Limited, Singapore Branch (“HBAP SGH”) and HSBC Bank (Singapore) Limited (“HBSP”), who requested for their comments to be kept confidential	Requested for their comments to be kept confidential
4	Linklaters Singapore Pte Ltd on behalf of the Singapore FinTech Association	<p>General comments:</p> <p>The members of the SFA (the “members”) are fully supportive of the introduction of the Guidelines and the resulting enhancements to consumer protection in the payment services field. This response does, however, request clarification on certain aspects of the Guidelines and proposes amendments to allow for a proportional approach in the application of the Guidelines by different types of responsible FIs (as defined in paragraph 3.1 of the Guidelines).</p> <p>Paragraph 1.4 of the Guidelines suggests that these may take effect ahead of the commencement of the new Payment Services Bill (“PSB”). It would be helpful if the MAS could clarify the expected timing for issuing the final Guidelines. The members are of the view that the Guidelines should take effect concurrently with the commencement of the PSB, to avoid any uncertainty regarding their scope of application (in particular given that the Guidelines use terms that are defined in the PSB, and that they will apply to certain responsible FIs that will</p>

be licensed under the PSB).

Question 1. Scope of Application

We share the MAS' view that the Guidelines will increase consumer confidence in the use of e-payments and will encourage wider adoption by the public of e-payments in Singapore.

Paragraph 2.1 of the Guidelines provides that these will apply to any responsible FI that issues or operates a protected account. The members would appreciate clarification on whether the Guidelines are therefore intended to apply solely in respect of the provision by responsible FIs of account issuance services as defined in the PSB.

In relation to the responsible FIs to whom the Guidelines will apply, we note that these will comprise a wide range of institutions including, for example, both established institutions such as banks and comparatively smaller fintech start-ups. The latter, in particular, may find it onerous to comply with the full range of proposed requirements under the Guidelines in respect of all payment transactions. To ensure a proportional compliance burden, we think it would be helpful to give responsible FIs the possibility of agreeing specific monetary thresholds with account holders above which the transaction notification and confirmation requirements and process for resolving erroneous transactions in the Guidelines will apply. We have set out further detail on this suggestion in our response to question 9 and 11 below.

The members also respectfully submit that it would be helpful if the MAS could align the scope of application of the Guidelines with that of the PSB, to keep the number of compliance thresholds to be adhered to by responsible FIs to a minimum. In particular:

- We note that the definition of "protected account" in the Guidelines is proposed to include (among others) any payment account that is capable of having a balance of more than S\$500 at any one time, whereas under the PSB, account issuers are proposed to apply AML/CFT requirements in respect of payment accounts that have an e-wallet capacity of more than S\$1,000 (in addition to

meeting other conditions). Although the members acknowledge that the two thresholds relate to regulatory frameworks with different objectives (one addresses the resolution of unauthorised and erroneous transactions, while the other counters money laundering and terrorist financing), for added simplicity and given that the difference between the thresholds is slight, the MAS may wish to consider setting these monetary thresholds at the same level.

- The MAS may wish to consider applying the monetary threshold in the definition of “protected account” in the Guidelines (currently proposed to be set at S\$500) both to payment accounts that are not a credit facility and to payment accounts that are a credit facility.

Question 2. Definitions

We note that expressions used in the Guidelines are proposed to have the same meanings as in the applicable Acts in which the expressions are referred to or used, except where they are expressly defined in the Guidelines. However, if the Guidelines will be issued under the PSB (once the latter takes effect), then for additional clarity and certainty, we think it would be helpful for the Guidelines to expressly state that capitalised terms are as defined in the PSB, unless defined in the Guidelines.

The members also respectfully submit that the defined terms “account holder” and “account user” should be used consistently in the final Guidelines. In particular, in the Guidelines as proposed, Paragraph 1.3 currently refers to liability of account users for unauthorised payment transactions, whereas Part A refers to liability of the account holder. We understand that these should be references to the account holder. In this response, we have employed the respective terms “account holder” and “account user” in accordance with our understanding of the MAS’ policy intention.

Our understanding of the term “authentication device” is that it does not include any debit card, credit card or charge card. If this is correct, it would be helpful to clarify this in the definition of “authentication device” for the avoidance of doubt.

Question 3. Where the account holder is not liable for any loss

We note that under paragraph 4.1, the account holder is not liable for any loss arising from an unauthorised transaction where (among others) an account holder shows that the account user has not contributed to the loss. We understand that this is distinct from the other situations set out in paragraph 4.1. We would welcome guidance on the circumstances in which an account holder can be deemed not to have contributed to the loss arising from an unauthorised transaction (for example, query whether this would cover a technical malfunction in a payment system).

Question 4. Where the account holder's liability is capped

In the members' view, additional guidance on when an account holder may be considered to have acted negligently would be helpful. In particular, it is currently unclear when an account holder will have acted negligently as opposed to recklessly (on recklessness, please also see our response to question 5 below).

We also note that the Association of Banks in Singapore's Code of Practice for Banks – Credit Cards (the "**ABS Credit Card Code**") takes a different approach to "limited liability" situations. The ABS Credit Card Code provides that, prior to notification of credit card loss to card issuers, the maximum liability for cardholders due to unauthorised charges is S\$100, unless the cardholder has acted fraudulently, or has been grossly negligent, or has failed to inform the card issuers as soon as reasonably practicable after becoming aware that his/her card has been lost or stolen. It would be helpful for the MAS to clarify how card issuers that are both ABS members and responsible FIs under the Guidelines should reconcile this standard under the ABS Credit Card Code with the provisions on "limited liability" in the Guidelines.

In respect of the situation where an account holder reports the unauthorised transaction to the responsible FI later than the next business day from receipt of the relevant transaction notification but within a period acceptable to the responsible FI, it would be helpful for the MAS to clarify what the responsible FI would be

permitted to treat as an acceptable period, and whether this period would need to be specified in the account agreement with the account holder.

Question 5. Where the account holder is liable for actual loss

We consider that additional guidance on when an account holder may have acted recklessly would be helpful. While the proposed Guidelines do clarify that recklessness would include the account holder or account user deliberately not complying with any duty in the Guidelines, it would be helpful for the MAS to provide further guidance on the meaning of recklessness in the context of the Guidelines.

We note that the ABS Credit Card Code makes a cardholder liable for 100% of outstanding unauthorised charges if he/she is involved in fraud or has acted with gross negligence. It is unclear in which respects recklessness would differ from this existing industry standard. It would be helpful for the MAS to clarify how card issuers that are both ABS members and responsible FIs under the Guidelines should reconcile this standard under the ABS Credit Card Code with the provisions in the Guidelines relating to recklessness of the account holder.

Question 6. Liability for losses arising from unauthorised transactions

We take the view that additional evidential provisions should be incorporated into the Guidelines to make it clear with whom the burden of proof lies (i.e. the account holder or the responsible FI) in any situation where an unauthorised transaction has occurred. While the Guidelines currently do indicate with whom the burden of proof lies in certain situations (e.g. a responsible FI must show that an account user's recklessness was the primary cause of the loss arising from any unauthorised transaction), in other situations, additional clarity on the evidential process would be welcomed. For example, in the "negligence" situations, where the account holder is liable for no more than S\$100, it is currently unclear whether the onus is on the responsible FI to prove the account user's negligence.

Question 9. Information and facilities provided by the responsible FI

As per our response to question 1 above, it would be helpful to allow responsible FIs to reach a specific agreement with account holders on the monetary threshold above which the transaction notification and confirmation requirements (referred to in paragraphs 6.3 and 6.4 of the Guidelines) will apply. As a practical matter, applying these requirements in respect of all payment transactions, irrespective of their value, may be unduly onerous for the relevant responsible FI. From a policy perspective, there is also a risk that providing transaction notifications, and requiring the account holder to provide confirmations, even in respect of the most low-value transactions could be counterproductive, as it could instil a habit in account holders of not scrutinising notifications and confirmations.

We would also welcome clarity on which party (the responsible FI or the account holder) should be expected to bear the cost of SMS notifications provided by the responsible FI and of other SMS messages sent pursuant to requirements in the Guidelines. Alternatively, it would be helpful for the MAS to confirm whether the allocation of this cost can be agreed by the parties in the account agreement.

Question 10. Claims investigation and outcomes.

We note that a responsible FI is not required to credit the account holder's protected account with the total loss arising from an unauthorised transaction where the responsible FI has good reasons to believe that the account holder (or in the case of a joint account, any account holder) is primarily responsible for the loss, and has communicated its reasons to the account holder. In this context, it would be helpful for the MAS to provide guidance on when the account holder will be "primarily responsible" for the loss, and in particular, whether this determination requires the responsible FI to prove the account holder's responsibility in accordance with a particular standard (e.g. on the basis of reasonable evidence obtained by the responsible FI).

We would also appreciate clarification on whether, when a responsible FI credits the protected account with the value of the unauthorised payment, this amount must also include any charges and interest payable by the account

		<p>holder as a consequence of the unauthorised transaction.</p> <p>The members would appreciate guidance from the MAS on the exceptional circumstances in which a responsible FI may conduct an extended investigation.</p> <p>Question 11. <u>Specific duties in relation to erroneous transactions</u></p> <p>We consider the process set out in the Guidelines for resolving erroneous transactions to be broadly appropriate. In our view, however, responsible FIs should only be obliged to engage this resolution process for those erroneous transactions which exceed an agreed monetary value threshold, as suggested in our response to question 9 above.</p> <p>We would also appreciate clarification on how the MAS expects this resolution process to work where the wrong recipient's financial institution is a foreign entity rather than a responsible FI in Singapore (noting in particular that foreign entities will not be subject to the Guidelines).</p>
5	Network for Electronic Transfers (Singapore) Pte Ltd	Requested for their comments to be kept confidential
6	OCBC Bank	Requested for their comments to be kept confidential
7	PayPal Pte Ltd	Requested for their comments to be kept confidential
8	Sidley Austin LLO on behalf of Alipay Singapore E-commerce Private Limited	Requested for their comments to be kept confidential
9	Singtel	<p>Question 1. <u>Scope of Application</u></p> <p>Singtel supports the implementation of proposed e-payments user protection guidelines. We note that the guidelines will go further in enhancing user confidence in electronic payments and electronic commerce in Singapore.</p> <p>Singtel offers Dash, a mobile mobile payment solution that allows users to make payments to peers, overseas beneficiaries and for goods and services. We have already implemented many of the proposed measures, including</p>

- Providing immediate receipts for payments made
- Requiring credentials in compliance with the Technology Risk Management guidelines
- Providing users with the flexibility to set their own payment limits / caps without passwords etc

Nonetheless, we have also provided our comments to the proposed measures in here.

Question 2. Definitions

In relation to the definition of ‘protected accounts’, these seem to exclude situations of the CEPAS SVFs today that are widely used, i.e. the Nets Flashpay or the EZlink SVFs. This means that a user is deemed not responsible to protect such SVFs; we ask whether concurrently, it means that the entire set of e-payment user protection guidelines will therefore not apply to users and the related FIs of the Nets Flashpay and Ezlink SVFs. If this was the case, the MAS may wish to introduce requirements for such FIs to duly inform their users that the protection guidelines will not apply to these SVFs.

However, we also note that there are instances where a single user (i.e. identified by his or her NRIC number) can hold multiple such SVFs, e.g. multiple EZ-link cards, each of S\$500 max value, and link them together in a single ez-link account. There is no limit to the number of ez-link cards each customer can add to his/her ez-link account. Therefore, the MAS would need to consider whether such linked accounts that aggregate multiple stored value cards – each with its own balance capped at \$500 but collectively can have no limit – are still excluded from the ambit of protected accounts. If this is the case, then there is a serious need to point this out to the public to ensure that they are aware of the risks involved.

Question 3. Where the account holder is not liable for any loss

Singtel notes that the situations have been comprehensively identified and listed. We do wish to submit the following comments.

To offer no liability, there should be specific circumstances and situations involved. Hence, we do not support the example in 4.1 (f) which now recommends a user only need to show or claim that they have not contributed to

		<p>losses, that they have complied with Part B. This allows the user to claim a myriad of activities under “not contributing to losses”. In fact, FIs should reserve the right to ascertain if such claims are true. The user should be required to present ample supporting evidence to justify his/her stance. For cases where there is a significant degree of uncertainty /, amount of loss and/or the account holder wishes to pursue his/her claim despite being unable to present ample proof, may we propose for the FI to have the option of either:</p> <ul style="list-style-type: none">(a) engaging an independent forensic investigator to analyse the holder’s account and all known devices used to access the account (may likely require the account holder and users to temporarily surrender their devices to the investigator), or(b) requesting the account holder to engage such a forensic investigator at his own expense to carry out such purpose <p>In relation to fraud and negligence by merchants, generally, a payment service provider will onboard merchants after carrying out due diligence. However, in the case of the actual sales and purchase of goods and services, the contracting is directly between the user and the merchant. The merchant will spell out the contractual terms and conditions of purchase and a user needs to accept those before payment is accepted for the goods and services. When a user accepts the merchant’s terms and fulfilled the purchase using the account, the transaction is deemed “authorised”. As stated in 4.6, the account holder will be fully liable for such cases, unless there is proof that the merchant is defrauding the account holder/user through such purchases. It is therefore not feasible to expect that the FI provides for these as a no liability situation for a user. In fact, we caution the MAS against presenting conditions which users can rely on simply to avoid payments to merchants that would otherwise be legitimate.</p> <p>In relation to invalid or faulty, forged authentication devices. in many cases, a user may claim a device was faulty and a transaction happened as a result. The FI should be allowed to investigate and ascertain that this is true before the user can expect liability to be waived.</p>
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

In relation to situations where payment was initiated after the FI was informed by the user of a breach or loss of the device – there needs to be a bridging period for the FI to be able to deactivate the device. These actions cannot happen immediately and the FI cannot be held responsible if the payment was still initiated during the bridging period. A reasonable period will be 24 hour(s) and the FI should be allowed to state the circumstances under which the report or informing is done – e.g. designated hotline, specific information. A user cannot call a non-designated hotline or simply leave voice messages or email messages for such cases.

Question 4. Where the account holder's liability is capped

Singtel believes that there should not be a fixed value for the liability cap but that FIs should be permitted a range of values, depending on the measures that they take. For example, we allow customers to set different limits for payments without PINs. So customers have to actively set the cap they want otherwise a default limit will apply. So where mitigation measures are given to users, it may not be necessary to set the same liability cap across FIs

Further, the situations in 4.3 (a) and (b) are not acceptable on grounds that these are clearly situations that could have been avoided and prevented by the user themselves. To cap the user's liability when they misplaced the authentication device or when they failed to report an unauthorised transaction within the required timeframe basically encourages a callous attitude towards treating payment transactions with care. Liabilities under these circumstances should not be the burden of the FI.

Question 5. Where the account holder is liable for actual loss

Whilst the scope of liability for actual loss is reasonable, we also highlight that there are cases of frivolous complaints resulting in time and resource expended to investigate only to conclude that the user is liable. Under such circumstances, FIs should be allowed to recover fees apart from having the user being liable for the actual loss itself. This is particular significant if the user has not taken the necessary measures to protect its own account resulting in fraudulent usage more than once, with the FI

having to carry out extensive investigations.

Question 6. Liability for losses arising from unauthorised transactions

Singtel notes that the MAS intends for the user to enjoy the lower of any caps in liabilities, whether that lower cap exists as part of the account agreement or in the scheme.

Whilst this appears reasonable, there is again the risk that the users are lulled into a sense of complacency. This should not be the case. Therefore, we propose that if the MAS is already proposing situations where the users cannot be held responsible and a limitation in liability amount, then these are sufficient as end-user protection mechanisms.

Question 7. Reporting duties of the account holder

Singtel agrees with the users' responsibilities identified in 5.1 to 5.7.

We also agree that the user should undertake the reporting obligations outlined in 5.8 and 5.9. Basically, an FI will first and foremost hold the contracting party responsible. So the person who contracted or subscribed to the service [and accepted the terms and conditions] will have to provide the contacted details.

Agree that if user does not provide updated or correct details or does not check messages or notifications, then the FI is not responsible for complying with liability caps. Given that that the user is expecting to have its liability capped, then it is only reasonable that the user provide all the minimum information listed within 1 calendar day or 1 business day, depending on the FI's own operational procedures.

In terms of the proposal in 5.10 on police reports, police report(s) should be encouraged and it should be right upfront when the user suspects fraudulent or unauthorised usage. In fact, to ensure that the matter is also accorded proper treatment by law enforcement authorities, FIs should be allowed to request that and only proceed when the account holder lodges a police report and furnishes a copy of the police report to the FI, along with other required information for investigation. This should also apply regardless whether it's the first time the

user is seeking a claim on grounds that these matters could be criminal in nature and should not be treated as merely a dispute between user and the FI.

Generally, reporting should be carried out by the user itself. Where the user requires information for supplying to the police and where there are no legal constraints on supplying, the FI would provide the required information

Question 8. Duty to protect access codes and protected accounts

Singtel agrees with the users' responsibilities identified in 5.1 to 5.7.

We note that it is important to emphasise users have equal responsibility to protect their own accounts from unauthorised usage. FIs cannot accord complete protection and therefore, it is not equitable that an FI has to bear the burden of liability in cases where users have not done the best to counter fraud etc. For example, in relation to the duty to protect access codes in 5.6, we would like to emphasise that the users should also be made to ensure that that the anti-virus software is always running on the device. There are instances where account users may ensure that anti-virus software is up-to-date, but would disable it from time-to-time such that actual scans do not take place over extended periods. In addition, users should also refrain from downloading and using apps from unknown sources, and should ensure they only download and use apps from established app stores like Google Play, iOS App Store, Samsung Apps, etc. in order to protect their accounts from unauthorised usage.

Question 9. Information and facilities provided by the responsible FI

Singtel agrees with the need for notifiable transactions on protected accounts as outlined by the MAS. However, the MAS requires the notifications to be in SMSes. We believe that FIs should be given the autonomy and discretion to send in-app, SMS and/or e-mail notifications to customers in a timely and appropriate manner, but not be compelled to offer customers options to choose notification frequency, channel and applicable transaction types.

		<p>With reference to 6.3(b), we wish to clarify on the necessity of issuing a day-end summary of all transactions made in the last 24 hours to the account holder, even if the FI already sends the account holder a notification via an in app notice SMS/email for every transaction performed on his account. We want to be mindful not to inundate account holders with excessive SMSs/emails, as these may end up in spam folders.</p> <p>Hence, rather than to make the form of the summary mandatory, we propose giving the customer a choice – eg we can send an email notification to the user for every transaction performed on his/her Dash account, but we do not send day-end emails that summarise all Dash transactions performed by the account holder for the day. Another option is for the user to choose whether they want to receive the email notifications for each transaction or retain those in its own inapp account.</p> <p>In terms of the information contained in the notification, Singtel suggests that the MAS permits for alternatives to the required information. Eg protected account number or recipient account number may not always be available due to the way that an FI designs its scheme. So a replacement should be allowed. This also applies for the merchant’s reference number and name etc.</p> <p>In terms of recipient credential information, Singtel agrees with the proposed requirements. Singtel’s Dash service already provides for these in the transactional flow where users are expected to confirm the recipient details before finally executing the transaction</p> <p>Singtel also agrees with the requirement for a reporting channel in the way described except that Singtel believes fee(s) are reasonable if the complaint over unauthorised transactions etc are proven to be frivolous in nature or attempts by the user to escape liability for transactions that were otherwise correct.</p> <p>Question 10. <u>Claims investigation and outcomes.</u></p> <p>While the MAS has proposed some measures that may appear as good practices, the reality is that there will be many cases which are disputable or debatable. These include factors like the nature of the transaction, amount of loss and customer’s transactional history, behaviour,</p>
--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>risk appetite, etc., that would determine if an FI should or should not reimburse the account holder, whether in full or in part, prior to a conclusive outcome.</p> <p>Therefore, we request that the MAS does not dictate conditions under which an FI must credit the protected account for the loss arising from an unauthorised transaction while claim investigation is still underway,</p> <p>Notwithstanding this, Singtel believes that 21 business days may not be sufficient if the investigations has to involve third parties. Eg the transactions involve merchants or other recipients. In which case the FI may not be able to dictate the pace at which the third party can respond. We believe that at least 30 working days is required for most cases</p> <p><u>Question 11. Specific duties in relation to erroneous transactions</u></p> <p>Singtel agrees with the responsibilities outlined in Part D.</p> <p>In relation to paragraph 7.2(a), when the case involves remittance transactions (overseas funds transfer), the steps in 7.2(a) may be difficult to uphold most of the time. It is industry practice for remittance licensees to receive and process remittance instructions from account holders via hub partners that already have commercial and settlement arrangements with overseas remittance end-points, which may be a bank, cash pick-up agent, cash delivery service or digital wallet provider. While it is often possible for a local remittance licensee to inform the overseas remittance end-point via a hub partner of an erroneous transaction within 2 business days, in most instances the local licensee does not have control over the overseas end-point's processes and policies. It is therefore not possible for the local licensee to ensure that it is able to ask the overseas end-point for the unintended recipient's decision within the proposed timeline of 7 business days.</p> <p>In relation to the specific issues, we note that the information identified in 7.3 should be identified as the minimum set of information to be given by the user to assist with claims and investigations. Where necessary or required, the user should be prepared to provide more information. Please also refer to our response in Q10.</p>
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>Question 12. <u>General questions regarding these Guidelines</u></p> <p>We believe that this is appropriate and relevant in the context of the MAS requirements. We note that similar schemes may apply to the banks on grounds that banks transact in high volumes – both in value and customer volumes. However, we are concerned that without regulatory encouragement, there would be little incentive for insurers to offer coverage to FIs who are engaging in e-payments (and are not banks).</p> <p>If there is no incentive from the MAS, there could be a lopsided effect where an FI will bear the bulk of the responsibility and is not sufficiently covered / insured in the market place. We caution that this may in fact cause the market to shrink.</p> <p>We ask that the MAS requires that insurers actually put in place schemes to help FIs cover / obtain the requisite insurance.</p>
10	The Association of Banks in Singapore	<p><u>General Comments:</u></p> <p>This response to MAS’ “Proposed E-payments User Protection Guidelines” (“guidelines”) is by the Association of Banks in Singapore (“ABS”) on behalf of its member banks. It summarises the broad high-level comments on the consumer protection framework proposed in the guidelines. In addition, member banks will also respond in their individual capacities, including feedback on their individual bank’s procedures and processes in view of the guidelines.</p> <p>Generally, ABS is supportive of having a Consumer Protection Framework. We also support actions that will encourage wider adoption of electronic payments (“e-payments”) in Singapore. However, there is concern that some of the recommendations in the proposed guidelines may not fully achieve these objectives and there may be alternative frameworks that may be more effective in achieving these objectives.</p> <p>Broadly, this response will emphasise the following concerns. Details will be provided in the specific response to the questions in the consultation paper:</p>

		<ol style="list-style-type: none">1. <u>Liabilities to be Proportioned Accordingly to Scope of Responsibilities</u> – Each stakeholder in the e-payments ecosystem has a role to play in safeguarding the financial stability of the e-payments ecosystem from unauthorised payment transactions. The liabilities of each stakeholder should commensurate with the level of responsibilities. The Guidelines should clarify the roles and responsibilities of each stakeholder in the e-payments ecosystem and assign liabilities accordingly. A misalignment of liabilities and responsibilities will lead to moral hazard situations where the entire e-payments ecosystem will be weakened. It is not clear if the proposed guidelines have correctly identified the responsibilities necessary and assigned the liabilities accordingly.2. <u>Erosion of Existing Prudential Controls to Safeguard Against Unauthorised E-payment Transactions</u> – There is concern that re-assigning the liabilities of end customers not in accordance with the principle in point one above would lower existing standards of established practices to safeguard against unauthorised transactions. Not only is this contrary to industry best practices (e.g. ABS Code of Practice for Banks - Credit Cards), it may encourage moral hazard from customers and weaken a key control measure against unauthorised transactions.3. <u>Systemic Risk to Financial Stability of Payment Ecosystem</u> – The proposal in the guidelines where Financial Institutions (“FIs”) are asked to absorb unauthorised transactions fully or for financial values above \$100 presents unprecedented financial risk to financial institutions. Accommodating customer’s negligence in protecting their banking credentials and delaying customer reporting duties from ‘reasonably possible’ to ‘one full business day’ are expected to spike financial losses arising from increased unauthorised transactions that are not prevented quickly. All these factors taken together will introduce systemic risk to the financial stability of FIs and the e-payment ecosystem.
--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Question 1. Scope of Application

These guidelines focus on the protection offered to individuals or micro-enterprises with a focus on limiting liability for such account users. We are fully supportive of encouraging the use of e-payments. However, limited liability for end consumers is not a panacea to increasing e-payments transactions. Account users should be liable for actual losses if they do not comply with their responsibilities to help safeguard their e-payment interests. Similarly, banks and FIs should also be held accountable against unauthorised transactions should they fail in their responsibilities. The onus is on the account users to prove that they are not liable, and if so a full refund should be given instead of limited liability.

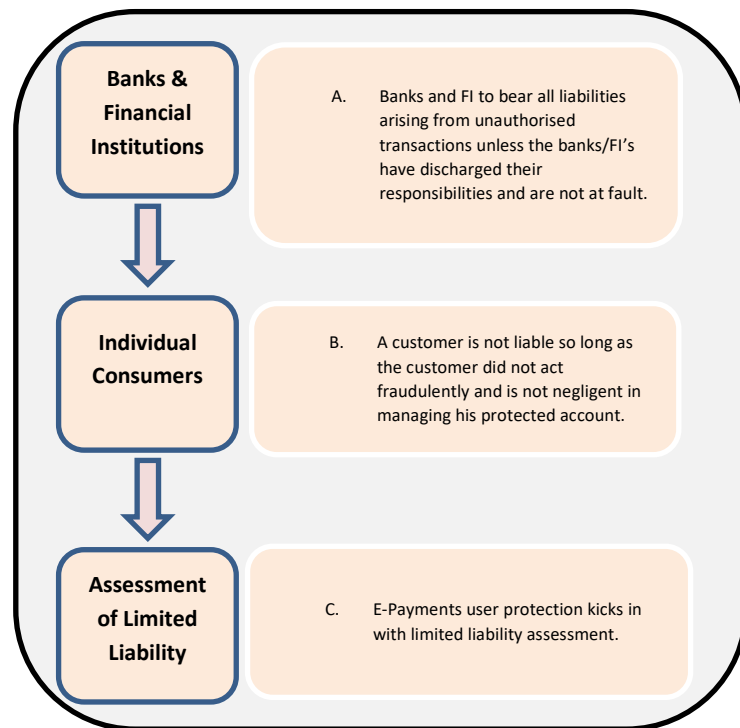
The account user is a major stakeholder in the ecosystem of e-payments. A more holistic approach would be to educate account users on why their actions (or inactions) contribute to unauthorised transactions and the appropriate measures they can take to protect themselves. Limited liability introduces moral hazard and reduces incentives for account user to adopt best practices and prudent behaviour to safeguard their interests. A framework that aligns the responsibilities with liabilities of all stakeholders in the e-payment ecosystem is the key to increasing consumer confidence in the use of e-payments and wider adoption. It is not clear that the proposed guidelines achieve this and hence the intended effect of wider adoption by the public of e-payments in Singapore.

To this end, the liability of stakeholders should not be represented in a binary manner as being placed on either the FIs or the account users to the exclusion of other stakeholders. ABS is of the view that in a holistic model, it is necessary to expressly acknowledge the alternative scenario where liability should lie with a third-party, in which event both the responsible FI and the account users are not at fault and the losses should be apportioned equitably. One such scenario would be where a hacker hijacks the email account of a third-party in a multiparty arrangement causing the account user to require the FI to transfer funds to the hacker's bank account. Both the FI and the account user are innocent victims in this scenario

		<p>and should not be liable. It is the third-party whose email account was hacked who should be potentially liable. The express acknowledgement of such third-party liability will help ensure all stakeholders continue to take adequate steps to safeguard their interests.</p> <p>ABS would like to propose an alternative framework where banks and FIs are only held accountable if they are at fault. Such a framework may be more effective in increasing consumer confidence and encouraging wider adoption of e-payments.</p> <p>Banks and FIs will bear all liabilities arising from unauthorised transactions if they have not discharged their responsibilities. Consumers will be liable for unauthorised transactions if they have not discharged their responsibilities.</p> <p>For the scenario where it is neither the fault of the customer nor the bank, we propose a clear need to identify possible situations that fall under this scenario and which should be subject to investigations, else it may be prone to abuse by customers and fraudsters. Fraudsters may engineer the situations where customers are deemed to be innocent. This can lead to a moral hazard and pose a systemic risk to the e-payments system. ABS will be happy to work with the Authority in determining how to resolved scenarios it is neither the fault of customer nor the banks.</p> <p>Such a framework may be more effective in increasing consumer confidence and encouraging wider adoption of e-payments.</p> <p>Given the difference in scope, scale and sophistication of transactions between individuals and micro-enterprises, ABS also proposes that the consumer protection framework focuses exclusively on individuals; and that micro-enterprises should be excluded from the scope. There is also concern whether the proposed guidelines are aligned with similar regulations from other jurisdictions (for example Australia and UK).</p> <p>There is already a well-established set of consumer protection and liability procedures for credit cards. However, it is noted that many of the proposals in these guidelines are not in line with established credit card industry practices. It is not clear if these proposed</p>
--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

guidelines that diverge from established industry practices are necessary to encourage wider adoption of electronic payments. Customer protection measures as prescribed by credit card practices have been sufficient for wide spread adoption of credit cards.

Alternative E-Payments User Protection Framework
Proposed By ABS



Question 2. Definitions

ABS will be deferring to member banks on their feedback of the proposed definitions used in the guidelines. In addition to seeking clarity of the proposed definitions, member banks may also request for additional definitions to avoid any ambiguity in the application of the guidelines.

The accounts that are not protected but are linked to protected accounts should be excluded from this feedback.

Question 3. Where the account holder is not liable for any loss

Elaborating on the framework proposed in Question 1, we would like to illustrate the importance of the individuals as a prudential control in safeguarding against

		<p>unauthorised transactions. Failure to assign liability corresponding to responsibility erodes the effectiveness of such controls and threatens the viability and financial stability of the e-payments ecosystem.</p> <p>For example, paragraph 4.1(b) states that the account holder is not liable for any loss arising from goods or services purchased because of merchant fraud. This encourages moral hazard from account users and there may be less diligence to verify the authenticity of e-retailers. If account holders bear no liability, then corollary, FIs would have to bear full liability (and hence full responsibility) for merchant fraud. FIs merely provide payment facilitation services and are not responsible for the selection of merchant or goods purchased. Setting aside that such an arrangement is not equitable, the concern is that exempting the key decision maker of such transactions from any liability greatly reduces the prudential control in preventing unauthorised transactions. Responsibilities should be clearly demarcated, and situations where end customers bear “no liability” should only be restricted to situations where they bear no responsibilities for the unauthorised transaction. For example, if their payment accounts have been compromised due to inadequate security measures by the FIs, then customers should bear no liability. Corollary, account holders have certain responsibilities to help ensure secure and authorised transaction payments. Failure of these responsibilities should not be included in “no liability” situations.</p> <p>Question 4. <u>Where the account holder’s liability is capped</u></p> <p>The “ABS Code of Practice for Banks – Credit Cards” should be read in its entirety. Moral hazard is not limited because of a liability cap of \$100. The key element in containing moral hazard lies in the conditions expected of cardholders. For example, one of the conditions for the limited cap for credit cards is for cardholder to inform card issuers as soon as reasonably practicable after being aware that the card has been lost or stolen. The ABS Code is written on the principle of an equitable assignment of liabilities to responsibilities. Once responsibilities are appropriately discharged, a liability cap is then appropriately applied.</p> <p>There is concern that this industry best practice principle to address moral hazard is being removed in the proposed</p>
--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

guidelines. For example, the guidelines now propose that customer's limited liability situations extend to include account user's negligence as set out in paragraph 4.3. Paragraph 4.3 states that an account user's negligence from misplacement of the protected account or authentication device for that protected account would still qualify for a limited liability of \$100. This is not aligned with industry best practices. Account users' safeguarding of the protected account is a critical prudential control to prevent unauthorised or fraudulent transaction. The current guidelines appear to be downplaying the importance of such prudential controls by recognising that even such negligent behaviour deserves a limited liability of \$100.

Question 5. Where the account holder is liable for actual loss

Following the comments for the earlier questions, we are of the view that the section on where the account holder is liable for actual loss should also be reviewed. To address moral hazard concerns, there are many more situations that the guidelines should cater for under the "actual loss" category compared to what is currently listed. We reiterate that liabilities should commensurate with responsibilities.

Question 6. Liability for losses arising from unauthorised transactions

Please see our responses to earlier questions where the responsibilities and liabilities demarcation suggested by these guidelines are not in line with industry practices, risk control management and moral hazard considerations. We propose a review of paragraphs 4.1, 4.3 and 4.5. Many of the scenarios described in these paragraphs are likely to result in account user and FI disputes. We propose that these responsibilities outlines should be principle-based rather than rule-based.

When outlining the scope of responsibilities to customers, we should also provide guidance and education on how customers can meet these principle-based responsibilities and protect themselves appropriately. We propose referencing to other government agencies' work in this area, for example the Cyber Security Awareness Alliance

co-chaired by Cyber Security Agency of Singapore and Singapore Infocomm Technology Federation. Technologies development is fast paced, and we should equip customers with guidance on how to keep pace with new cyber security threats and typologies. Educating customers to cyber security guidelines and best practices is another way to boost consumer confidence and encourage e-payment transactions.

We agree with MAS' proposal that it would be more appropriate for the FI and account holder to go through a dispute resolution process for such situations as these contentious situations might not have clear demarcation of liability.

Question 7. Reporting duties of the account holder

The reporting duties proposed in these guidelines are inadequate, erode the effectiveness of reporting as a prudential control, encourages moral hazard and poses systemic risks to the entire payments ecosystem. In the following example, we will compare the reporting duties from industry best practices for credit cards to illustrate the concerns with the proposed reporting duties in the guidelines.

It is grossly inadequate for an account holder to report any unauthorised transactions to the responsible FI by the next business day. Under the ABS Code of Practice for Banks – Credit Cards, cardholders are expected to report as soon as reasonably practicable. Early reporting allows the halting of any subsequent unauthorised transactions. Compared to credit card transactions, unauthorised e-payment transactions are at even greater risks of being expeditiously executed once compromised. By reporting as soon as possible, and not later than the next calendar day (this is to set a timeline for customer to report promptly) account holders are helping themselves reduce further exposure and possibly losses. It is unclear why the guidelines would recommend exposing account holders to a longer than necessary period of compromise by suggesting a reporting duty of next business or calendar day. Furthermore, responsible FIs have made investments to provide real time notification to boost consumer confidence in using e-payments. They also provide easily accessible reporting channels that are available all the time. It seems counterintuitive to delay reporting of

unauthorised transaction without further elaboration. From a payment ecosystem perspective, accumulation of such imprudent reporting duties from different account holders will also result in accumulation of mounting unauthorised financial transactions. These coupled with limited liability exemptions for customers would have a systemic impact that could threaten the financial stability of the entire e-payment ecosystem. Not only does prompt reporting help protect the account holder from future unauthorised transactions, by providing the details of the nature of the unauthorised transaction, the responsible FI may be able to prevent other account holders from similar unauthorised transactions.

We also note that the proposed guidelines are not aligned with industry best practices. For instance, paragraph 7 of the Notice on Technology Risk Management issued pursuant to the Securities and Futures Act on 21 June 2013 states that notwithstanding certain exceptions, an FI is required to notify the Authority “as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident”.

Therefore, the MAS proposal for an account holder to report any unauthorised transactions to the responsible FI by the next business day runs counter to the reporting standards expected of the FI. Early reporting allows the early prevention of any subsequent unauthorised transactions and helps protect account holders from further exposure to possible losses. This approach is similarly adopted by the UK Payment Services Regulation 2017 (Regulation 72(1)(b): customer is to notify the FI “without undue delay” on becoming aware of the theft, misappropriation or unauthorised use of the payment instrument) and the Australia ePayments Code (Paragraph 11.5: A user who *unreasonably delays* reporting the misuse, loss or theft of a device or breach of the security of all pass codes will be regarded as liable for the actual loss).

Question 8. Duty to protect access codes and protected accounts

Account holders and users are an integral and vital part of the control process to help deter and detect unauthorised transactions. It is not prudent for the guidelines to reduce such prudential controls to a list of basic “dos” and “don’ts”. To ensure the financial stability of the payment

		<p>ecosystem, some of these control responsibilities are currently enshrined in specific products/services terms and conditions for usage. The guidelines should elaborate on the effectiveness of such duties as controls and educate how account holders can help play a stronger role in ensuring financial stability of the payment ecosystem. The guidelines should help emphasise the importance of such responsibilities in preventing unauthorised transactions and provide assurance that so long as such responsibilities have been demonstrated, end consumers should not be required to bear full liability.</p> <p>ABS would also highlight that any proposed prudential controls be set out in a technology neutral manner. This will ensure that the guidelines are based on principles and intended outcomes rather than detailed rules as the latter provides for the promulgation of a rigid prescriptive set of standards. We would submit that a principle-based, technology agnostic set of guidelines will remain relevant in the current rigorous regulatory environment for e-payment services. This approach will further ensure that the guidelines continue to stay relevant as technology standards and platforms continue to relentlessly and rapidly evolve.</p> <p>Given the above, we propose that MAS review existing FI's list of current account user responsibilities to protect access codes and protected accounts. We support the view that a streamlining of these responsibilities will help ensure consistency and provide greater clarity to account holders and account users of the duties and responsibilities expected of them.</p> <p>Customers are advised to always refer to and abide by the respective bank's terms and conditions with respect to the services they subscribe to.</p> <p>Question 9. <u>Information and facilities provided by the responsible FI</u></p> <p>We agree with the proposal to provide the account users with sufficient payment information such that the account users may promptly report unauthorised or mistaken payment instructions to the responsible FIs. However, we recommend that the guidelines be principle-based as opposed to being overly prescriptive and rule-based. Given the pace of technological advances, specific</p>
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

reporting channels and its characteristics may evolve over time and the guidelines should ensure that broad principles continue to apply. The following are some examples:

1. The payment information should not be prescribed as it differs according to payment types. For example, FIs may not be able to provide the merchant's phone/identification/account number or registered/trading name.
2. There is also no necessity to provide such information onscreen when the account users are physically present to make payments at merchants' premises. It is also not practical for contactless payments as it creates friction and holds up the queue and may discourage use of electronic payment.
3. Furthermore, transaction alerts containing such detailed and sensitive information sent via non-secure modes of communication such as e-mail and SMS may pose an information security risk for our clients.
4. It is not practical to be prescriptive in the manner of transaction notification, for example, to prescribe the requirement that transaction notification should be sent at least once every 24 hours and to consolidate every notifiable transaction made in the past 24 hours.

Individual member banks will be providing more examples in their individual responses to MAS.

Question 10. Claims investigation and outcomes.

Responsible FI to Complete Claims Investigation - As aligned with current practice, the FIs have always endeavoured to complete its investigations quickly and, where appropriate, effect the refund. Drawing lessons from credit cards, the deadlines proposed are not aligned with the scheme timelines. For non-3D secured internet transactions, the investigation process can be from 60 calendar days and up to 180 calendar days or more, depending on the chargeback progress as the merchant's acquiring bank might reject the chargeback and the case will be escalated to the respective card associations. In

addition, the amount of time taken for investigations is dependent on how forthcoming the account holder is with the information.

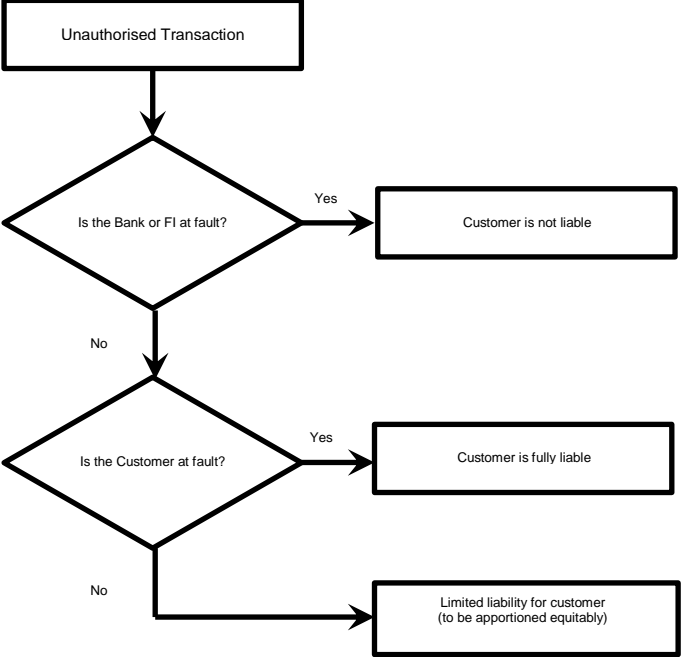
Responsible FI to Credit Protected Account - When investigation of the claim is still underway, the responsible FI would not know if there are good reasons to believe that the account holder is responsible for the loss arising from the unauthorised transactions. Crediting the protected account while the claims investigation is ongoing would create moral hazard. The account holder might try to game the system and use this method to obtain unsecured funding. If it was subsequently discovered that an account holder is responsible for the loss, more time and resources would need to be incurred to clawback the money from the account holder.

Question 11. Specific duties in relation to erroneous transactions

We recommend that the guidelines be principle-based instead of rule-based when outlining FIs' obligations in relation to erroneous transactions.

The proposed guidelines on handling erroneous transactions does not appear to be aligned with the government's *PayNow* initiative as described under ABS' *PayNow: FactSheet*. The factsheet states that *PayNow* account holders are reminded to check the recipient's details to ensure that it is correct before confirming the transfer. If there are erroneous transactions, the account holders are encouraged to reach out to the unintended recipient to request a return of the funds. Account holders can engage the bank if there is no response from the unintended recipient.

Account holders are the trigger point for transactions, so it would be most expeditious if account holders reach out to resolve the matter with the recipient first. This would also ensure that account holders take care to obtain and enter the right information to ensure that funds are properly transferred. Successful resolutions could then be filtered out in the process rather than have FIs investigate all account holder's errors. This would free up FI's resources to handle other erroneous transactions that could not be settled with the recipient. MAS should also

		<p>note that foreign FIs are not bounded by these guidelines and do not have to agree or cooperate with the reversal of erroneous transactions. The proposed guidelines are one-sided and would unilaterally bind only Singapore banks to erroneous transaction resolution.</p> <p>Question 12. <u>General questions regarding these Guidelines</u></p> <p>We understand that purpose of illustration 1 is to simplify the process for end customers so that the extent of their liabilities is clearly illustrated. However, given that mapping of liabilities to responsibilities is a major tenet of ABS' alternative framework, we propose the following decision tree instead to guide account users, account holders and responsible FIs on their expectations.</p>  <pre> graph TD A[Unauthorised Transaction] --> B{Is the Bank or FI at fault?} B -- Yes --> C[Customer is not liable] B -- No --> D{Is the Customer at fault?} D -- Yes --> E[Customer is fully liable] D -- No --> F[Limited liability for customer (to be apportioned equitably)] </pre>
11	Visa Worldwide Pte Ltd	Requested for their comments to be kept confidential
12	Respondent 1	<p>Question 1. <u>Scope of Application</u></p> <p><u>No. (1):</u></p> <p>Please clarify whether the Guidelines are intended to only apply to “protected accounts”, as currently defined in the Guidelines.</p>

		<p>Various sections in the Guidelines refer to “account holders”, “protected accounts”, “account users” and “responsible FI” simultaneously. This is problematic, because “account holders” and “account users” refer to holders of any payment account, whereas “responsible FI” are defined in relation to protected accounts only.</p> <p>For example:</p> <ul style="list-style-type: none">- Para 4.1 of the Guidelines states that “account holder” is not liable for any loss arising from any unauthorised transaction if the loss arises from certain prescribed situations. An “unauthorised transaction” is defined to refer to certain transactions in relation to any protected account. “responsible FI” is also defined to refer to FIs in relation to any protected account. However, “account holder” is defined to mean “any person in whose name a payment account has been opened...” and will include a holder of any payment account, not just a protected account. If the intention is for the Guidelines to only apply to “protected accounts”, we propose to replace references to “account holder” with “holder of a protected account” or such equivalent language.- Para 7.1 of the Guidelines refers to situations “where <u>an account holder</u> has informed his <u>responsible FI</u> in accordance with this Part that he or an <u>account user</u> has initiated a payment transaction from <u>a protected account</u> such that money has been placed with or transferred to the wrong recipient...”. While “account holder” refers to a holder of any payment account, “responsible FI” and subsequent reference to “a protected account” suggest that the intention may be for this part of the Guidelines to apply only to protected accounts. Please clarify if this is the intention. If so, the reference to “account holder” and the definition of “account user”, which includes an “account holder”, will need to be amended to reflect the intention accordingly.- Para 7.2(b) refers to “...responsible FI is the FI of the wrong recipient...” Please clarify whether the payment account of the wrong recipient must also be a “protected account”, given that the
--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>definition of “responsible FI” is in relation to a protected account only.</p> <p>No. (2):</p> <p>Please clarify whether parties may, by mutual agreement, agree to arrangements which are different from those prescribed in the Guidelines.</p> <p>Question 2. <u>Definitions</u></p> <p>Please see the comments in response to Question 1 above.</p> <p>Question 7. <u>Reporting duties of the account holder</u></p> <p>Para 5.2 of the Guidelines requires that an account holder should at a minimum, provide either his Singapore mobile phone number or his email address to the responsible FI, which must be complete and accurate.</p> <p>We propose that Para 5.2 be amended, to include a sub-paragraph (c), to broaden the type of contact information an account holder can choose to provide to the responsible FI, so that an account holder can be contacted via different means from SMS or email, for example, via Whatsapp, in-app notifications etc.</p> <p>Question 9. <u>Information and facilities provided by the responsible FI</u></p> <p>Para 6.3 of the Guidelines requires responsible FI to provide transaction notifications “in respect of all transactions made to or from the account holder’s protected account”. Para 6.3(c) further states that transaction notifications may be sent to an account holder via SMS, email, and where in-app notifications are sent, to be accompanied by an SMS or email.</p> <p>We would like to propose to remove the requirement for an SMS or email to be sent to an account holder where transaction notifications are made via in-app notifications, because in-app notifications function similarly like emails and are received instantaneously and account holders may configure the app settings to receive alerts of such in-app notifications.</p> <p>Question 10. <u>Claims investigation and outcomes.</u></p>
--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>Para 6.10 of the Guidelines states that “responsible FI should credit the account holder’s protected account with the total loss arising from any unauthorised transaction, regardless of whether the investigation of any claim is still underway, except where the responsible FI has good reasons to believe that the account holder is primarily responsible for the loss arising from the unauthorised transaction, and has communicated its reasons to the account holder.”</p> <p>We would like to request for MAS to re-consider the position as extracted above. If a responsible FI credits the account holder’s protected account with the total loss arising from an unauthorised transaction before investigations are completed, the responsible FI will have bear the responsibility and costs of recovering such amount from the account holder, if investigations shows that the account holder is liable for the loss. Where the loss in question is less than S\$20,000 and account holder refuses to return to the responsible FI the money credited upon completion of investigations, the responsible FI will have to commence action for recovery against the account holder in the Small Claims Tribunal. We propose that crediting of account holder’s protected account with the total loss should only be done upon completion of investigations by responsible FI and where investigations shows that account holder is not liable, or liable only up to a prescribed limit.</p> <p>In addition, the Guidelines also do not provide additional elaboration on the situations where an account holder is “primarily responsible for the loss arising from the unauthorised transaction”. This is likely to lead to disputes between the account holder and the responsible FI, and we request that the Guidelines describe in greater detail the relevant situations or parameters of situations where an account holder is primarily responsible for the loss.</p> <p><u>Question 11. Specific duties in relation to erroneous transactions</u></p> <p>Para 7.2 of the Guidelines stipulates the timelines within which certain steps have to be taken by responsible FI in</p>
--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>its reasonable efforts to recover the sums sent by account holder / account user in error.</p> <p>Given that the Guidelines will apply to Payment Services Licensees after the Payment Services Bill is passed, we propose that a different set of extended timelines be applied to non-bank responsible FIs, to take into account the time required for such non-bank responsible FIs to liaise with their banks.</p>
13	Respondent 2	Requested for their comments to be kept confidential
14	Respondent 3	Requested for their comments to be kept confidential
15	Respondent 4	Requested for their comments to be kept confidential
16	Respondent 5	Requested for their comments to be kept confidential
17	Respondent 6	Requested for their comments to be kept confidential
18	Respondent 7	<p>Question 4. <u>Where the account holder's liability is capped</u></p> <p>We would like to seek a clarification on the definition of "recklessness".</p> <p>We would like to ask about the rationale on why losses as a result of "misplacement of the protected account or authentication device or access code for that protected account" are for the FI to bear. Also, what if the unauthorised transaction amount is a huge amount for eg. SGD 50,000?</p> <p>Question 5. <u>Where the account holder is liable for actual loss</u></p> <p>(Same as above) We would like to seek a clarification on the definition of "recklessness".</p> <p><i>"The account user is expected to provide the responsible FI with information the responsible FI reasonably requires to determine whether any account user was reckless."</i></p> <p>We feel that it is counter-intuitive for users to volunteer information that would result in them bearing the full amount of the loss.</p> <p>Question 7. <u>Reporting duties of the account holder</u></p>

		<p>We feel that if an account holder only needs to report unauthorised transactions by the next business day, this might be too long of a delay especially where a lot of FIs are moving towards instant settlement.</p> <p>We are currently able to support receipt of reports every calendar day.</p> <p>Question 8. <u>Duty to protect access codes and protected accounts</u></p> <p>We agree that the MAS is correct in its push for digital security. These are basic password security measures that should be upheld.</p> <p>Question 10. <u>Claims investigation and outcomes.</u></p> <p>The responsible FI should credit the account holder’s protected account with the total loss arising from any unauthorised transaction, regardless of whether the investigation of any claim is still underway, except where the responsible FI has good reasons to believe that the account holder (or in the case of a joint account, any account holder) is primarily responsible for the loss arising from the unauthorised transaction, and has communicated its reasons to the account holder.</p> <p>We feel that this is very onerous on smaller companies. This is an even bigger imposition for companies looking to offer B2B epayment services where the volume of each transaction is much bigger.</p>
19	Respondent 8	<p>Question 1. <u>Scope of Application</u></p> <p>We are of the view that the scope of protected accounts should apply only to individuals and not micro-enterprises. The definition that is being proposed for micro-enterprises (i.e. business employing fewer than 10 persons or with annual turnover of no more than S\$1m) seems to imply that there is an onus on FIs to determine whether an entity falls within the definition of a micro-enterprise. Having to determine this for each entity on an ongoing basis will be onerous for FIs. We urge MAS to consider limiting the scope to only individuals.</p> <p>Question 4. <u>Where the account holder’s liability is capped</u></p>

		<p>While we support the idea of a “limited liability”, we are of the view that the liability amount should be commensurate with the responsibility of the account holder. In cases where the account holder has not acted in a responsible manner, the liability of the account holder should be higher, so as to avoid any moral hazards.</p> <p>Question 7. <u>Reporting duties of the account holder</u></p> <p>In general, the financial industry should inculcate and reinforce to consumers, a discipline of reporting unauthorised transactions as soon as detected or possible. Prescribing a time frame to report might inadvertently dilute that rigour, potentially injecting more risk into the financial system.</p>
20	Respondent 9	Requested for their comments to be kept confidential
23	Respondent 10	Requested for their comments to be kept confidential