

Annex B

Submissions from Respondents to Consultation Paper on Enhancements to the E-payments User Protection Guidelines Shared Responsibility Framework

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

S/N	Respondent	Responses from respondent
1	BigPay Singapore Pte. Ltd.	Question 4. MAS seeks comments on including the measures in Table 1 of the consultation paper into the EUPG, which will make them applicable to all responsible Financial Institutions. Firstly as MPIs we do not issues digital security tokens. In addition we have enhanced security measures in place. Which consists of and are not limited to, Device Binding, Device Integrity Validation (blocks attempts to login from a rooted/jail broken device) and using a side-loaded/fake app, Authentication via in-app authorisation by the customer to confirm changes related to "high risk" events and also period based transactional limits. Hence we do not deem that the "cooling off period" is necessary for our organisation. In view of the preventive methods that have been adopted as part of our business operations.
2	Biocatch	Question 4. MAS seeks comments on including the measures in Table 1 of the consultation paper into the EUPG, which will make them applicable to all responsible Financial Institutions. <u>Measures prior to performing high-risk activities</u> Behavioural biometrics technology can be implemented as an additional layer of risk assessment to detect high-risk activities across a number of scenarios including when a customer is being coached by an attacker to approve a payment on an active call, when a remote access tool has

S/N	Respondent	Responses from respondent
		allowed an attacker to take over a customer's device to approve an action, or when malware is present on the device allowing an attacker to forward SMS OTPs and other data without the victim's knowledge. Many banks are using behavioural biometrics to provide a risk score to determine the likelihood that a scam is in progress and use this information to present additional pop-up risk warnings to the customer. For example, National Australia Bank has seen their payments prompt initiative, driven in part with the use of behavioural biometrics technology, get customers to stop and think before sending a payment. The bank was receiving over 2,500 calls a day from customers reporting scams and fraud and now see nearly \$300,000 AUD in payments abandoned daily after customers receive the warning messages. (Source: National Australia Bank). Other regulatory bodies, such as the Reserve Bank of India (RBI), have also called on regulated entities to employ mechanisms to alert customers in the event of high-risk activities and must be generated based on various parameters, including behavioural biometrics. A top Indian bank deploying behavioural biometrics to address the RBI Digital Payment Security Controls guidelines, issued in February 2021, achieved up to 94% fraud detection rates, a majority of which were remote access account takeovers. Additionally, multiple UK banks that have implemented simple questions within digital banking sessions where a high-risk potential scam payment is identified (e.g. via behavioural biometric profiling). Questions such as 'how well do you know this person?', 'have you confirmed this payment with someone you trust' and 'what is the purpose of this payment' have been used to help interrupt and prevent scam payments with great effect. <u>Cooling off period</u> As referenced above, behavioural biometrics technology can be implemented as an additional layer of risk assessment to detect when a scam is in progress. If the risk score is high indicating a scam, the financial institution can apply a policy to hold the payment for the suggested cooling off period until the customer can be contacted. <u>Outgoing transaction notification alerts</u> Notifications should not only arrive by SMS but an alternate method such as a secondary mobile number or email address and "In banking App" alerts that can't be deleted. Malware can intercept and delete SMS messages on Android. On IOS, a phone can be switched to "Focus mode" where notifications are not visible to the user.

S/N	Respondent	Responses from respondent
		Utilising behavioural biometrics to detect high risk transactions can remove monetary limits and issue different alert methods based on risk rather than hard rule. <u>Self-service feature ("kill switch")</u> Adding this feature is highly encouraged and a good way to raise consumer awareness by actively involving them in protecting their financial assets. Aside from being available through a different channel, it should not be dependent on knowing a password in the event the fraudster has taken full control of the account or ability to disable it from a mobile device that has been compromised by malware. <u>24/7 reporting channel</u> The reporting channel should be enabled with access to real-time behavioural biometrics data which includes the specific risk factors that determined a customer may be the victim of a scam or an unauthorised transaction has occurred. For example, most scams start over the phone where the customer is being directed by an attacker, posing as the bank or a government official, to make a payment. Behavioural biometrics looks for signs of an active call during a banking session which is a strong indicator of a scam in progress. Data shows over 50% of scams have an active call during the banking session compared to less than 1% of genuine banking sessions. Providing visibility into these types of risk indicators can help call centre agents ask the right questions to customers when they call in to report an unauthorised transaction (e.g. Were you contacted by someone over the phone?).
		Question 5. MAS seeks comments on the proposed enhancements to responsible Financial Institutions' duties in Table 2 of the consultation paper. <u>Notification alerts when high-risk activities are performed</u> As referenced above, notifications should not only arrive by SMS but an alternate method such as a secondary mobile number, email address or "In banking App" alerts that can't be deleted. <u>Expectations of responsible FIs' dispute resolution</u> Behavioural biometrics can provide additional forensic evidence to aid in speeding up the dispute resolution process. This is especially relevant in cases of malware or remote access where a victim's device has been taken over and controlled by an attacker. Behavioural signals, such as screen interactions, device movements and navigation patterns,

S/N	Respondent	Responses from respondent
		indicate whether the banking session was initiated by a genuine customer or a third party who is controlling the device. Analysts may also have access to video reconstruction of a banking session which shows a detailed breakdown of behavioural activity during the session. This additional evidence enables financial institutions to quickly uncover liability if a fraud prevention control has failed and feel confident in their course of action.
		Question 6. MAS seeks feedback on the additional duties for consumers in Table 3 of the consultation paper. <u>Cyber hygiene practices</u> It is important for financial institutions to remind their customers on a regular basis to practice good cyber hygiene such as not storing card, password, or pin details in note apps. However, we are strong advocates for communicating with customers as close to the point of payment as possible (through pop-up risk warnings as mentioned in the section on “Measures prior to performing high-risk activities”). These practices will have the most impact in preventing a scam or fraud from occurring.
		Question 7. MAS seeks feedback on the proposed new guidelines for handling erroneous transactions, where the request for the return of funds is initiated by the "wrong recipient". One solution that would help to mitigate erroneous transactions is an enhancement to the duties of responsible FIs that require the sending and receiving FI to participate in a Confirmation of Payee (CoP) program. Confirmation of Payee alerts someone setting up a new payee or amending details of an existing one if the recipient's name doesn't match their bank details. An analysis by SurePay, and reported by UK Finance, showed that using Confirmation of Payee resulted in a 67% reduction in misdirected payments (Source: UK Finance). Confirmation of Payee could also help avert some financial scams. Other countries requiring (or proposing to require) Confirmation of Payee controls include: 1. UK: Confirmation of Payee will be mandated for over 400 FIs in 2024. 2. European Union: The European Commission has proposed requiring Confirmation of Payee for instant payments as part of its 3rd Payment Services Directive (PSD3). 3. Australia: The Australian Banker's Association recently announced that Australian banks have committed to use Confirmation of Payee in the future as part of the Scam-Safe Accord.

S/N	Respondent	Responses from respondent
		Question 8. MAS seeks any other comments on the draft amendments to the EUPG (in Annex A), which have been published together with this consultation paper. <u>Description of a proposed additional duty of responsible for financial institutions</u> The bottom line: without a mule account, a fraud attack cannot be successful. Money mule accounts are one of the primary reasons that financial scams work. One of the most effective controls to reduce financial scam losses must be tighter controls around mule account detection. Thus, we are recommending an additional duty of responsible financial institutions (FIs) in the proposed E-Payment User Protection Guidelines to create a Money Mule Account Management Program. The proposed Money Mule Account Management Program consists of four key components: 1. Management of the Money Mule Account Program 2. Fraud controls around online account opening 3. Fraud controls around existing accounts to detect money mule activity 4. Reporting <u>Section 1: Management of the Money Mule Account Program</u> The Management of the Money Mule Account Program requires the designation of a named individual to oversee the implementation and ongoing operation of this program. For larger banks, this should also include dedicated staff responsible for the day-to-day administration of the program. The Program Manager must report quarterly to senior management or to the Board of Director's Risk Committee. The reporting can include: • The number of new accounts blocked from being opened at 1) time of account opening and 2) immediately (1-2 days) after account opening • The number of money mule accounts detected and closed • The amount of fraudulent money that flowed into money mule accounts • The amount of fraudulent money that flowed into money mule accounts that was not blocked prior to its exfiltration outside the money mule account (either to another On-Us account, to another FI account inside Singapore, to another FI account internationally, to a cryptocurrency exchange, etc.) • The list of controls being deployed to detect and block money mule accounts • The current gaps in money mule account controls

S/N	Respondent	Responses from respondent
		In order for such a program to be successful and effective requires sponsorship and support from executive management. The elimination of money mule accounts goes a long way to stopping consumer financial scams. Aside from the financial risks, money mule also pose reputational risks to the FIs and the Singapore banking environment. <u>Section 2: Fraud controls around online account opening</u> The second component of a Money Mule Account Management Program involves implementing controls to detect and decline fraudulent new accounts created as part of the FIs online account opening solution. Fraudsters use a variety of different techniques to create illegitimate accounts for the sole purpose of laundering stolen funds. Some of these techniques are listed below: • The use of intelligent bots to open new accounts at scale, using thousands of IP addresses and bot network devices. Intelligent bots can perform multiple activities including automating data entry on a new account application. • The use of mobile emulators. Fraudsters fake a mobile phone transaction from a PC. • The faking of device fingerprint data. Fraudsters can now define the device fingerprint (for web and mobile) to be used for the transaction. • Use of human fraud farms at large scale to enter the online account application data and to defeat CAPTCHA • Use of synthetic IDs. The combination of real personal data and fabricated data to create a synthetic identity. Sometimes referred to as “Frankenstein IDs,” fraudsters often spend months, or even years, building up credit under these identities to make them appear legitimate for use at a later time. • Soliciting genuine consumers to sell their legitimate account or open a new account under fraudulent circumstances (e.g. fake job adverts) There are a number of controls that an FI can deploy to detect and block a fraudulent or mule account from being opened online. Protecting online account opening is a defense-in-depth process that requires multiple solutions with some necessary overlap. <i>Primary Controls</i> • Bot detection. This is an important control to be at the top of the control stack to identify and eliminate as many bad new online account applications created by intelligent bot activity as early in the process as possible. Preventing bot activity early will also save the FI from paying transaction fees on many of the additional required controls. In addition, bot detection controls are effective at detecting and blocking credential stuffing attacks used at the start of account takeover fraud.

S/N	Respondent	Responses from respondent
		• Behavioural biometrics. There are many behavioural signals that can separate genuine customers from a fraudster in the account opening process. For example, genuine customers will exhibit fluid typing patterns as they are familiar with their personal data versus a fraudster who will exhibit segmented typing patterns, excessive deleting, and copy/paste (indicating they are working off a list of stolen credentials). <i>Additional Controls</i> • Device fingerprint detection. This is always an important control, but it really needs to take into account a fraudster creating their own device fingerprint to be inserted into the transactions or using a mobile emulator. • VPN detection. This can tell if the request is coming direct from a device or being routed through a virtual private network (VPN). • Validate physical address. Is it a legitimate address? Is it from a questionable address (e.g., prison)? • Validate phone number. Phone number should be a mobile phone number, a fixed VoIP phone number and possibly still a land line, but not non-fixed VoIP or Google phone type numbers. Using telco services, match the phone number to the name and address on the application. Phone number should also correlate to the use with the physical address and the email address. Identifying temporary phone number usage is also helpful. • Validate the email address. Look for recently created email addresses or email addresses from suspicious domains. • Validate true location of mobile phone. There are several ways to validate the mobile phone location, especially if the FI requires a user to download their mobile app as part of the account opening process (which is a good security control to require usage of the mobile app as part of the account opening process, even if it adds friction). • Perform synthetic ID validations. This can be performed in the United States but unsure if the same or equivalent vendors offer such services in Singapore. This is a quite important control. • Perform velocity checks on the applicant data within the FI and with other FIs in Singapore. Often, a fraudster will use the same personal information to open multiple accounts across multiple FIs. This is where consortium data sharing can come into play (e.g., has this person opened multiple new accounts recently?). • Document verification with liveness testing. This is where a consumer takes a picture of a Singapore driver's license or passport, and the vendor can run a series of tests to validate it is a legitimate document. This must be done with liveness testing of the consumer. The use of GenAI for fraud creating multiple challenges here. • Use AI and machine learning to look for anomalies among all of the data collected. Two simple examples are detecting email

S/N	Respondent	Responses from respondent
		addresses in a repetitive format (e.g., nnnnn456@gmail.com, nnnnn457@gmail.com) and assessing the structure of an email address. • Monitor for sudden changes to an email address, phone number, or physical address after an account has been successfully opened. <u>Section 3: Fraud controls around existing accounts to detect money mule activity</u> The third component of a Money Mule Account Management Program involves fraud controls around existing accounts to detect money mule activity. This component is often non-existent in most banks around the world. In developing this third component, it is important to understand and define the many money mule account personas. Examples include: • Mule accounts created by a fraudster using stolen PII data or synthetic IDs. • Consumers who are solicited by a fraudster to be a willing money mule by chasing an opportunity to make easy money • Consumer who agrees to allow their existing account to be used for a business purpose. • Naïve or vulnerable people who are not aware they are being used as a money mule. This could include a victim of a romance scam. In the last three cases, the fraudster or consumer may be the one accessing the money mule account. There are several controls that can be deployed to detect money mule accounts and money laundering activity using AI, machine learning, and behavioural biometrics for anomaly detection on the 'receiving' account. Here are some examples: • Identify changes in behavioural patterns that may indicate that a customer has been recruited as a money mule or sold access to their bank account to a malicious third party. This control is important as it is a pro-active control that can identify money mules prior to it receiving the proceeds of a fraud or scam event. • Analyze the historical data for inbound transactions coming into the account including how close these transactions are to the actual account opening date. Large dollars transactions would be especially suspect. • Analyze the sending bank account data to see if the transactions are odd for a consumer account. • Check the sending bank name on the inbound account to the actual name on the inbound account. Note: there could be some legal reasons to not perform this check. • For an existing customer account, consider the age of the customer to see if these transactions are normal. For example,

S/N	Respondent	Responses from respondent
		young adults who are receiving multiple large payments which is uncommon for this age group. Young adults are among the fastest growing segment of consumers associated with money mule activity. Data released by UK Finance and Cifas show that young adults up to 30 years old accounted for 64% of money mule cases in the first half of 2023. • Monitor for multiple high value deposits in a short period of time. • Monitor for long periods of latency followed by a sudden spike in activity (e.g. multiple logins prior to an incoming payment). Data released by BioCatch shows that 79% of confirmed mule accounts were highly active 90 days prior to an incoming payment. • Use the account opening data and account data as part of this analytics process. <i>Other Considerations</i> • If an anomaly is detected on the inbound current account, then, subject to regulations, the account should be frozen while an investigation takes place. • FIs should share information on confirmed money mule accounts. When an account is identified as a true money mule account, the account number and the account opening data could be shared, subject to regulation and privacy laws. • MAS should consider if Singapore banks should have limits moving money from consumer accounts to cryptocurrency exchanges. <u>Section 4: Reporting</u> The fourth component of a Money Mule Account Management Program involves reporting. As is often said, you cannot manage what you do not know. So, reporting is critical to ongoing management and improvement of the program. Reporting should be focused on two key areas: • Reporting on new account opening. Metrics may include total number of accounts opened, total number of accounts closed as part of the account opening process (system closure because of fraud rules, Day 2 closures) and total number of money mule accounts detected. • Reporting on potential money mule account activity. Metrics may include false:positive ratio of possible alerts to money mule activity vs actual money mule activity, total monetary value associated with money mule account activity, total monetary value of money mule account activity blocked from exfiltration, and number and value of actual exfiltration by source (On-Us, other Singapore banks, international banks, crypto exchange, etc.).

S/N	Respondent	Responses from respondent
3	Lymon Pte. Ltd. (part of IQ-EQ)	Question 4. MAS seeks comments on including the measures in Table 1 of the consultation paper into the EUPG, which will make them applicable to all responsible Financial Institutions. <i>Measures prior to performing high-risk activity</i> We respectfully propose that MAS provides further guidance on what would constitute as “high-risk activity” which warrants further authentication measures to take place. <i>Kill Switch</i> We respectfully propose that FIs are to include other channels for performing kill-switch features aside from the app or website itself, as the same login details will be utilized to access the app/website and it will be inaccessible if the login details have altered by the hacker/scammer. Question 5. MAS seeks comments on the proposed enhancements to responsible Financial Institutions' duties in Table 2 of the consultation paper. We agree with the proposal and have no further comments. Question 6. MAS seeks feedback on the additional duties for consumers in Table 3 of the consultation paper. In relation to the paragraph on “Preventive Measures: Cyber Hygiene Practices”, it advises against the downloading and installation of applications which are unverified to their intended functionalities. However, the only way to deduce which permissions the application requires would be to install the application, and then allowing or disallowing the requested permissions. As such, we respectfully seek clarification on the proposed process in which consumers without technical expertise would follow to determine if an application is unverified to their intended functionalities. We respectfully propose that it should be made a requirement for FIs to publish and highlight which permissions a legitimate app would require from the device. In relation to the paragraph on “Stronger Authentication Methods”, the primary concern would be on consumers who use older phone models. As the consumers would be unable to ensure the use of stronger authentication methods which will only be accessible through newer phone models.

S/N	Respondent	Responses from respondent
		In relation to the paragraph on “Reporting Unauthorised Activities”, consumers are to report any instance of unauthorised activity on his or her account no later than 30 calendar days after receipt of any notification alert for any unauthorised activity. As such, we respectfully seek clarification on the proposed consequences if the consumer misses this deadline, if any. We respectfully seek MAS’ clarification if a monetary threshold would be imposed for such unauthorised transactions, as the primary concern would be that certain consumers may not feel the need to report unauthorised transactions if they deem that the monetary value is too low. In relation to the paragraph on “Lodging police reports”, consumers should furnish the police report to the responsible FI within 3 calendar days after notifying the FI of the unauthorised transaction. We respectfully seek MAS’ clarification if there would be consequences if the consumer misses this deadline. Additionally, we respectfully propose the following: 1. The implementation of a separate mobile app for the uploading of police reports meant for the FIs to refer to; or 2. Imposing of a limit to in-person submissions and, exempting the consumers who are overseas from the 3-day deadline. Question 7. MAS seeks feedback on the proposed new guidelines for handling erroneous transactions, where the request for the return of funds is initiated by the "wrong recipient". In relation to Paragraph 6.4 of the revised Annex A, we noted that “Where confirmation is required from the FI of the account holder (who had made the erroneous transaction) before the recipient’s FI can return the sum sent in error, the FI of the account holder should also make reasonable efforts to facilitate the return of such sum.”. We respectfully seek MAS’ clarification on the circumstances where confirmation would be required from the FI of the account holders. Question 8. MAS seeks any other comments on the draft amendments to the EUPG (in Annex A), which have been published together with this consultation paper. We agree with the proposed draft amendments and have no further comments.
4	SingCash Pte Ltd	Question 4. MAS seeks comments on including the measures in Table 1 of the consultation paper into the EUPG, which will make them applicable to all responsible Financial Institutions.

S/N	Respondent	Responses from respondent
		In relation to paragraph 4.7 on cooling off, SingCash wishes to clarify that not all payment service providers, eg those issuing e-wallets, will make use of digital security tokens. Most will make use of other two-factor authentication (2FA) solutions, e.g. via email or SMS. Hence, cooling off under such circumstances will not be viable or efficient. SingCash notes that unlike banks, e-wallets or payment accounts have specific features imposed by the MAS: (a) Wallet caps (b) Annual flow caps Under the Payment Services Act and Payment Services Regulations, payment institutions who offer account services that issue e-money (i.e. e-wallets) can issue e-wallets of up to S\$5,000, and the total value of transactions per annum for that e-wallet cannot exceed S\$30,000. Such restrictions are not placed on bank accounts. These caps or limits become natural impediments for nefarious activities by scammers. As such, we believe that it is not necessary for payment service providers issuing e-wallets to include notification alerts on a real-time basis, for conduct of high-risk activities as set out in the proposed amendments to the EUPG. Alternatively, where the MAS considers it necessary for the payment institutions to build in such notifications for high risk transactions, we ask that the MAS reduces the burden for the payment institutions (on grounds that the wallet limits and other caps are already in place) and removes the requirement in paragraph 4.8 of the proposed EUPG [where 'a responsible FI should inform the account user of a protected account of the risks and implications of performing high-risk activities and obtain additional customer confirmations, at the point before the account user performs the high-risk activities']. Nonetheless, we note that the MAS has also included, in its proposed amendments, that notification alerts are now able to be delivered via SMS, emails or via their responsible FI's in-app notices. We say this because providing the notification on a real-time basis is only viable if it is sent out via the payment provider's own platform, e.g. via the app or on the portal. Once the notification has to be sent out via SMS or a third-party platform, there will be the possibility of a turnaround time being involved. Hence, we note that it is imperative that the MAS has considered it timely to amend the EUPG to allow payment institutions the right to deliver these real time notifications via the app.
		Question 5. MAS seeks comments on the proposed enhancements to responsible Financial Institutions' duties in Table 2 of the consultation paper.

S/N	Respondent	Responses from respondent
		In terms of the requirement to have a proper governance structure and investigation process and involving representatives who are independent from business units who are to carry out the above assessment, this may not be practical for smaller players who clearly will not be able to set up separate units. The same business units will manage the marketing and dispute resolutions. Separating the dispute resolution will end up replicating cost(s) and in fact lengthen the dispute resolution process. We ask that the MAS remove this or reconsider this for the smaller industry players. E-wallet providers clearly will not be able to waive or withhold charges relating to disputed charges as they would have had to settle any deducted charges with their partners. At most, they can credit these back to the users when the disputes are resolved. The EUPG should clarify these in advance so that users do not dispute these with the payment institutions who are e-wallet providers. Question 8. MAS seeks any other comments on the draft amendments to the EUPG (in Annex A), which have been published together with this consultation paper. Paragraph 4.28 of the draft EUPG requires that key obligations of the EUPG apply even during schedule system downtime. We ask that the MAS provides for some flexibility as system downtime is meant for maintenance of components and systems, including those parts of the operating systems that cater for those aspects of the networks that are meant to provide the aspects that provide the specific obligations. It is simply not possible to expect the obligations to be at full operation during system downtime. FIs could for example put out messages to warn their users of the possibility.
5	United Overseas Bank Limited	Question 4. MAS seeks comments on including the measures in Table 1 of the consultation paper into the EUPG, which will make them applicable to all responsible Financial Institutions. <u>1. Scope of EUPG</u> Currently, the EUPG applies to Sole Proprietors regardless of which business segment they reside in. However, the draft SRF guidelines only applies to individuals and sole proprietors under the retail segment. As such, we would like to confirm whether the EUPG will also apply only to individuals and sole proprietors under the retail segment. <u>2. Sending of Clickable links and phone numbers</u> Table 1 of the CP on EUPG states that “A responsible FI should not send clickable links or phone numbers to a retail consumer unless the

S/N	Respondent	Responses from respondent
		consumer is expecting it.” However, under the draft EUPG, Para 4.4 required clickable links to apply to a retail banking account, while Para 4.5 on sending of phone numbers via SMS applies to a protected account. We would like to clarify with MAS whether the requirement on Para 4.5 applies to sole proprietors under the wholesale segment. <u>3. Cooling off period</u> Table 1 of the CP 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; and (b) send a notification alert to the consumer’s registered contact with the responsible FI.” For our FI, the system is currently set up such that the 12-hour cooling period takes place upon registration of the security token, before the security token is activated. Customers would receive alert notifications upon successful registration of the security token and are not allowed to activate the digital token for use until after the 12-hour cooling period. This is, in fact, a more prudent approach and would meet MAS’ requirement where the digital security token cannot be used to authenticate high-risk activities until after the 12-hour cooling period. In any case, the user is only able to transact 12 hours post any change in token. We would like to clarify with MAS whether this approach is also acceptable for meeting MAS’ requirement. If yes, perhaps MAS could allow the requirement to be stated as “set up / activated” to allow for such circumstances as well. <u>4. Outgoing transaction notification</u> With reference to Para 4.10(c) of the draft EUPG, the transaction notification should be conveyed to the account holder by any of the following medium: i. SMS; ii. Email; or iii. In-app push notification. a. We would like to clarify with MAS that banks have the option of selecting which channel to avail to customers so long as the notifications are real-time. For example, the Bank is allowed to send SMS on a real time basis together with email notification in 30 minutes batches. Please confirm our understanding. b. We would also like to clarify whether sending email notifications in batches continue to be allowed on condition that all high-risk transactions notifications are sent on a real time basis (e.g., SMS).

S/N	Respondent	Responses from respondent
		Referring to FIs' duty to send transaction notifications on a real-time basis for all outgoing transactions, we would like to seek clarification on the definition and expectation of "real-time". 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. <u>5. Kill Switch</u> With reference to Para 4.14 of the draft EUPG, we understand that the kill switch is intended to allow customers to kill online and mobile access to their protected accounts, which includes online card transaction (e.g., credit/ debit card transactions for online purchases) and not for physical credit/ debit/ ATM card transaction. Please confirm our understanding. Question 5. MAS seeks comments on the proposed enhancements to responsible Financial Institutions' duties in Table 2 of the consultation paper. In relation to the implementation timeline, the Bank will need minimally 12 months to implement the requirements highlighted in Table 2 of the CP and can only confirm the specific time required after completing our gap analysis. <u>1. Dispute Resolution process</u> In relation to the implementation timeline to align current dispute resolution process to meet the expectations set out in Para 7 of the draft EUPG, the Bank will need minimally 12 months to implement the requirements and can only confirm the specific time required after completing our gap analysis. <u>2. Charges relating to disputed authorised transactions</u> a. In relation to the implementation timeline, the Bank will need minimally 12 months to implement the requirements and can only confirm the specific time required after completing our gap analysis. b. Para 8.2 of the draft EUPG guideline states that "...the responsible FI should withhold and/or waive the requirement for the account holder to settle the outstanding amount of that transaction and the charges directly relating to that transaction during the following periods:..." We are of the view that the Bank can reinstate the fees and charges applicable to customer from 31st calendar days onwards. <u>3. Withholding and/or waving of outstanding charges and reporting to licensed credit bureaus</u>

S/N	Respondent	Responses from respondent
		The current reporting to licensed credit bureaus e.g., CBS is fully automated. To ensure that consumer's credit records with licensed credit bureaus are not adversely affected by reason of the disputed transactions while pending investigation or pending processing by FIDReC requires enhanced flexibility in our system which is currently not available. In relation to the implementation timeline, the Bank will need minimally 12 months to implement the requirements and can only confirm the specific time required after completing our gap analysis. <u>4. Definition of "high-risk activities"</u> We note that the "high-risk activities" definition differs between the draft EUPG and the draft SRF guidelines. The definition referred to in the draft EUPG has a wider scope which states "include, but are not limited to", but not in the draft SRF guidelines. As the draft SRF guidelines refers to the draft EUPG, this may create confusion to the extent of high-risk activities covered. Moreover, the inclusion of "but are not limited to" means each FI has the discretion to include additional activities which they deem to be high-risk and such differing practice may cause confusion to customers who have accounts with different banks. Hence, we suggest MAS to adopt the high-risk definition in the draft SRF guidelines for the draft EUPG. <u>5. Para 4.2 of the draft EUPG states that "A responsible FI should inform every account holder of a protected account of the user protection duties".</u> In relation to the implementation timeline, the Bank can only confirm the specific time required after completing our gap analysis. Question 6. MAS seeks feedback on the additional duties for consumers in Table 3 of the consultation paper. We would like to propose for MAS' consideration to include scenarios for the loss of mobile devices where Customers are responsible to inform responsible FIs timely such that appropriate measures can be taken e.g., block further mobile and online access to the protected account through a different channel. In relation to Para 3.6(g) of the draft EUPG: Sideload apps can be downloaded as APKs through channels apart from websites e.g., sent directly by scammer through WhatsApp. Will MAS consider amending "third-party websites" to "third-party sources"? Apart from "Clickable Links" and "Phone Numbers", should consumer vigilance be extended to QR codes?

S/N	Respondent	Responses from respondent
		Question 7. MAS seeks feedback on the proposed new guidelines for handling erroneous transactions, where the request for the return of funds is initiated by the "wrong recipient". 1) Returning of erroneous transactions: If the sender account happens to be frozen/locked in the interim period e.g., due to FI or Police investigations, what should the beneficiary account FI do or where should such funds be held? 2) Noted that the draft EUPG covers on the request for the return of funds being initiated by the "wrong recipient". Given that there is plausibility where the "wrong recipient" would be receiving erroneous funds credited into his / her account, and where such funds are of wire-nature (i.e., telegraphic transfers) and are from FIs out of Singapore, it is possible where such overseas FIs may take a longer time to respond or to confirm on the erroneous transfers. In such a case, we are of the view local recipient is allowed to conform to the handling timeline of 21 business days / 45 business days (complex cases), as mentioned under Para 7.5 of the draft EUPG instead of the SLA stated in Table 4 in the CP. Please confirm our understanding. 3) Para 6.1 of the draft EUPG states that "where an account holder or his account user initiates a payment transaction from a protected account such that money has been placed with or transferred to a wrong recipient ("erroneous transaction")." Hence, we are of the view that cash deposits performed through Cash Deposit Machines (CDM) is not a form of payment transaction from a protected account and will not be in scope of Para 6 of the draft EUPG - specific duties in relation to erroneous transactions. Please confirm our understanding. 4) Major banks in the industry have adopted the practice to close the request on recall of funds for erroneous transactions if there is no response from the wrong recipient's FI after 30 business days. In this regard, we would like to seek MAS' consideration to include this practice as part of the guidance under Para 6.3 (a) of the draft EUPG.
		Question 8. MAS seeks any other comments on the draft amendments to the EUPG (in Annex A), which have been published together with this consultation paper. <u>1. Liability for losses arising from unauthorised transactions</u> With regards to Para 5.5 of the draft EUPG – "The account holder of a protected account is not liable for the first S\$1,000 of loss arising from

S/N	Respondent	Responses from respondent
		an unauthorised transaction, if the loss arises from any action or omission by any third party not referred to in paragraph 5.4 and does not arise from any failure by any account user to comply with any duty in Section 3.” a. With regards to Para 5.5 of the draft EUPG, in respect of unauthorised transactions which does not exceed S\$1,000, if the unauthorised transaction is due to the fault of a third party (and neither the Bank nor the customer is at fault), is the FI’s liability limited to the amount of the unauthorised transaction? b. Should the loss arising from an authorised transaction be more than S\$1,000, we are of the view that the current stance (i.e. FI should not be liable for the losses) should remain as we understand that the S\$1,000 threshold was set in recognition that most day-to-day payment transactions performed by individuals are under \$1,000, and that banks require their customers to perform transaction signing for payment transfers above \$1,000 to new payees. <u>2. Para 3.1 of the draft EUPG</u> “Where the protected account is a joint account, the account holders should jointly give instructions to the responsible FI on whether the responsible FI should send transaction notifications alerts under paragraphs 4.10 and 4.11 to any or all the account holders”. a. Please clarify if the obligations in Para 3.1 apply to Main Card (“MC”) and Supp Card (“SC”) holders in the same way that it seeks to be applicable to joint account holder. This becomes critical when read with Para 4.10 (which does apply to Cards). For instance: • If MC wants to receive transaction notification alert for SC, does FI need to allow? • If MC requests to receive transaction notification alert on some of his SC (some or all), must FI comply and allow MC to select? • If SC wants to receive transaction notification alert for MC, must this be disallowed? • For 2 different debit card customers linked to same CASA (i.e. joint account holders), please confirm that account holder 1 should not receive transaction notification alerts for account holder 2 and vice versa? b. MAS provided the following clarification on 25 Mar 2019 <u>Notification for Joint Accounts</u> <i>Handling notifications for joint accounts – we have earlier asked at the 3 Jan concall and MAS has clarified that the Bank is not expected to offer customer option(s) for notification to more than 1 account</i>

S/N	Respondent	Responses from respondent
		<i>holder and it is left to the Banks to agree with the account holders. Please confirm if this position still holds. [MAS: We leave this to the banks to work out the specific arrangement with their customers for joint accounts in respect of which account holder is to receive notifications]</i> The Bank would like to confirm if MAS' stance remains. 3. MAS provided the following clarification on 25 Mar 2019 <u>4.4(d) of Guidelines</u> <i>It was clarified at 3 Jan concall with MAS that the Bank need not strictly follow 4.4(d) of guidelines, as long as information reflected is sufficient for user to identify the transaction. Please confirm if this position still holds. [MAS: Banks should observe para 4.4(d), but we understand if some of the information may be carried within the form of notification e.g., time and date stamp. The purpose is to allow the customer to identify unauthorized transactions meaningfully]</i> The Bank would like to confirm if MAS' stance remains. 4. Para 4.4 of the draft EUPG - Should QR code be treated in a similar fashion as clickable links? 5. Para 4.11 of the draft EUPG - Outgoing payment transactions would include pre-authorised, first person or recurring transaction notifications. Please clarify what are the examples which fall under "pre-authorised", "first person" and "recurring transactions" mentioned under Footnote 15? - Do FIs have the discretion to mandate certain transaction notifications instead of allowing Customer to opt-in/opt-out of all notifications? 6. Para 4.13 of the draft EUPG – We note that incoming transaction notification are not mandatory. 7. Para 4.19 of the draft EUPG – Our understanding that whilst the reporting channel is "available at all times", there is no expectation for the industry to adhere to any prescribed service levels (e.g., call waiting time).
6	Walletery Pte Ltd	Question 8. MAS seeks any other comments on the draft amendments to the EUPG (in Annex A), which have been published together with this consultation paper.

S/N	Respondent	Responses from respondent
		<u>Suggestions & Recommendations:</u> 1. Support for educational centres for transaction and account opening for more vulnerable population – e.g. in Ireland, there was a project to have an educational branch for retired (and similar sample of population-clients), where the officers were trained to educate, explain in simplified way, demonstrate the product (in a more in-depth manner, unlike the standard explanations provided at a local bank branch) and helping people to open accounts and how to use them in person (i.e. not in a detached or removed manner) – thus they can keep regular contact with them to gain trust and be their contact person against scams (as people trust them – ask them for advice as their account managers) 2. Development of certain version of reputation-point system of financial institutions under the supervision of MAS (e.g. based on Matrix like number of complaints, real presence of officers who take care of the complaints (e.g. compared to being handled by permanently outsourced departments – higher risk of scam) 3. Development of system like CENTROlink in Lithuania – the main point is to avoid receipt of prepared reports by supervised subjects (as they might have minor incidental, but irrelevant errors) and keeping records also directly under MAS supervision (not proactively checking, but always available as the transaction must go via dedicated MAS account). 4. Full (or predominant) prohibition of certain ways of communication e.g. bank communicates strictly via its platform or on safe chat and never using SMS, whatsapp etc. anymore (including officers prohibited to use it for retail banking. It may however be used only for professional clients, who are expected to be significantly less vulnerable – e.g. using threshold in their income, qualifying them as VIP etc.) 5. Transactions to crypto assets OR crypto asset service providers must be always approved by a specific officer in the payment institution (to be able to warn the client before or send STR to warn about suspicious accounts) 6. Transaction to crypto assets OR crypto asset service providers will always work on T+1 basis at least and this is due to vulnerability in relation to scams (with necessary real person approval instead of system automatically doing it – e.g. risk manager for transaction monitoring) 7. Shared database of suspicious accounts between credit and non-credit financial institutions (e.g. suspicious crypto wallets, scam account in foreign countries, etc. – qualified for internal pre-checks before the execution of payments)
7	Respondent A	Question 4. MAS seeks comments on including the measures in Table 1 of the consultation paper into the EUPG, which will make them applicable to all responsible Financial Institutions.

S/N	Respondent	Responses from respondent
		1. We would appreciate MAS' clarification and guidance on whether there are minimum expectations or best practice examples on how additional confirmation / further authentication should be obtained from consumers prior to executing high-risk activities. We note that Table 1 suggests that FIs should inform consumers of the associated risks and implications of high-risk activities via pop-up risk-warning messages and would like to clarify if it is necessary for the confirmation to be a pop-up risk-warning message or if the warning can be presented in other ways e.g. disclosed and confirmed as part of the transaction confirmation rather than a separate pop-up. We would also appreciate clarification on whether the pop-up risk warning may only contain the associated risks and implications specific to the high-risk activity being executed by the consumer, or if it may be more generic to contain risks and implications of high-risk activities generally. 2. We note that the 12-hour cooling off period offers enhanced security, however, there may be consumers who wish to perform urgent legitimate transactions within the 12-hour period. In such cases, can FIs provide consumers with a way to bypass the minimum 12-hour cooling off period when a digital security token is activated (for example, through additional confirmation/verification from consumers)? 3. We note that Page 7 of the Consultation Paper on Proposed Enhancements to the EUPG states that a responsible FI should provide consumers with a kill switch which should be available through a different channel from the bank's mobile or internet banking channels. However, the draft revised EUPG at paragraph 4.14 states that the kill switch should be made available in a prominent manner via the mobile application of the responsible FI, the ATMs of the responsible FI, or the reporting channel provided by the responsible FI. We would therefore appreciate MAS' clarification on whether it would suffice for responsible FIs to provide a kill switch to consumers through the mobile application of the responsible FI. 4. We would appreciate MAS' clarification on how kill switches should be implemented operationally to satisfy the requirement. For example, would a helpline that customers can access to inform the payment service provider that their account has been compromised and request for the payment service provider to freeze their account to prevent any further unauthorised transactions suffice? The payment service provider would then verify the identity of the customer on the helpline, following which the payment service provider would then restrict the account to ensure that no further transactions of any sort may be executed through the account while pending further investigations by the payment service provider. 5. We note that Paragraph 4.4 of the draft revised EUPG makes reference to "protected retail banking account", however, Table 1 of the consultation paper seems to indicate that this preventive measure should apply to all responsible FIs. We would appreciate MAS'

S/N	Respondent	Responses from respondent
		confirmation if the duties in that paragraph should also be applicable to non-bank payment service providers who have issued their users with a retail payment account.
		Question 5. MAS seeks comments on the proposed enhancements to responsible Financial Institutions' duties in Table 2 of the consultation paper. 1. The proposed e-payments user protection guidelines ("EUPG") state that the financial institutions ("FI") should when notified of the unauthorised transaction, withhold or waive the requirement for the account holder to settle the outstanding amount of the disputed transaction and direct charges until completion of investigation, or where there are disputes on the results of the investigation for the additional period described. We will suggest that the guidelines correspondingly also provide for the payment due to the recipients (e.g. merchants) to be withheld if the FI had yet to transfer the payment to the recipients and there should be no legal ramifications if so. The EUPG takes reference from measures discussed with the Association of Banks in Singapore and accordingly considers the financial resources of the banks. Unlike banks, a Major Payment Institution ("MPI") offering account issuance services containing e-money may not be as financially resourced and should not be expected to make payments to recipients but withhold settlement from the account holder. 2. The proposed EUPG also describes the steps that the FI should take to ensure that the non-payment of disputed transactions does not affect the credit records with the credit bureau. Given that the guidelines will also apply to MPI offering only account issuance services containing e-money, these measures that are often applicable to the banks issuing the credit cards should not be applicable to the MPI as they will not have relationship with the credit bureau. We will suggest that this be scoped out for MPIs.
		Question 7. MAS seeks feedback on the proposed new guidelines for handling erroneous transactions, where the request for the return of funds is initiated by the "wrong recipient". We agree that this is a good initiative, however, there may be operational concerns regarding costs which could be significant for cross-border transactions. We would appreciate MAS' clarification on which party should bear the costs relating to the return of the funds. Given that the erroneous sender is at fault, we believe that the erroneous sender should bear the costs and any costs should be settled

S/N	Respondent	Responses from respondent
		between the erroneous sender's FI and the sender. Where it is not possible for the costs to be borne by the erroneous sender's FI upfront, the wrong recipient's FI should be allowed to deduct costs from the amount to be returned.
8	Respondent B	Question 4. MAS seeks comments on including the measures in Table 1 of the consultation paper into the EUPG, which will make them applicable to all responsible Financial Institutions. The proposed EUPG and proposed Shared Responsibility Framework Guidelines ("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 8. MAS seeks any other comments on the draft amendments to the EUPG (in Annex A), which have been published together with this consultation paper. We recommend the "protected account" definition 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 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.
9	Respondent C	Question 4. MAS seeks comments on including the measures in Table 1 of the consultation paper into the EUPG, which will make them applicable to all responsible Financial Institutions. a) For Measures prior to performing high-risk activities: (i) Since additional confirmation has already been put in place, will it be necessary to include pop-up risk-warning messages? (ii) Will there be prescribe guidance on the associated risks and implications to be included to ensure that it standardize across all FIs?

S/N	Respondent	Responses from respondent
		b) For outgoing transaction notification alerts: (i) For Paynow transactions, the default FI's practice is sending in batches (e.g. every 5 minutes). Does this fulfil the real time requirement as per set out? (ii) Can the FI's set the default notification alert to be received via email? However, account holder will have the option to switch to SMS as the preferred mode, if any. (iii) Due rising cost of sending real time outgoing notification alerts via SMS, can the FI levy charge to the account holder to share the cost incurred?
		Question 5. MAS seeks comments on the proposed enhancements to responsible Financial Institutions' duties in Table 2 of the consultation paper. <u>Information to enable consumers to validate their intended recipient:</u> We would like to seek clarification on the definition of "Sufficient information". For example, would "Sufficient information" be referring to Section 4.16 and/or 4.18 of the Revised EUPG (Annex A of the consultation paper)? We would like for the definition to be clear so that we can provide consumers with the right information.
10	Respondent D	Question 4. MAS seeks comments on including the measures in Table 1 of the consultation paper into the EUPG, which will make them applicable to all responsible Financial Institutions. <u>Sending of clickable links and phone numbers</u> We seek clarification in regards to what kind of clickable links are allowed and under what circumstances. In particular we would like to seek clarification on whether: 1. How can we determine whether a consumer is "expecting to receive" an SMS or Email? For example: a. Would having this information as part of the customer agreement which the consumer acknowledges be considered sufficient? b. Would the customer need to select this as a preference in his or her account and would this be sufficient? Or c. Would it require another kind of acknowledgement? If this is the case, we seek MAS' kind assistance to elaborate. d. In a scenario where a customer's transaction requires additional information, we currently send out clickable links for the customer to rectify this, by providing more information on the transaction, however the customer may not be "expecting to

S/N	Respondent	Responses from respondent
		receive” these links as they may not be aware of any issues with their transaction. Can we please confirm whether this would fall under MAS’ definition of not “expecting to receive”? If we changed this to a push notification via the app instead would it then be allowed? 2. What is the definition of “a website where the account user provides his access codes or performs any payment transaction”? a. In particular, can we confirm that this does not refer to the Customer Login page, e.g. where the customer can input his username and password? b. We would also like to request a clearer definition of “a website where the account user performs any payment transaction”. E.g. We assume that this means a website where the user is already logged into his / her account and can already send or authorise a transaction, i.e. it does not refer to any public web pages / websites. c. In regards to “a platform where the account user is able to download and install applications”, can we please confirm that this means we cannot provide links for the customer to download our app from the Google Play Store or the Apple App Store? <u>Cooling off period</u> We agree that a 12-hour cooling is an effective security measure to reduce phishing scams and that it should be implemented. We would however, like to propose allowing consumers the option of alternate biometric verification controls when activating the token on new devices that would hopefully achieve a similar level of effectiveness when activating a digital token. One such alternate control would be “Face Detect” which is a type of liveness check, where we would have previously taken a 3D map of the consumer’s face and then use this data to compare against the consumer’s face taken with the camera on the new / separate device. In this case, the 12-hour cooling off control would remain as a default but we would provide an option to do alternate controls to activate the token immediately if the consumer can pass the “Face Detect” test. <u>Outgoing transaction notification alerts</u> In regards to “Transaction Notification Threshold”, the Revised EUPG (Annex A of the consultation paper) mentions: “(b) if the account holder did not set any threshold for transaction notification alerts, the default industry-baseline transaction notification threshold.”

S/N	Respondent	Responses from respondent
		MAS must be specific as to what it considers the “default industry-baseline transaction notification threshold” for Payment Service Providers. E.g. Is there a specific body / organisation / study / guidelines that we can refer to. We believe it is unlikely that this is just what the Payment Service Provider considers as the baseline based on the activities of their consumers. As such, we just want to understand how we can reasonably determine what this baseline might be. <u>Self-service feature (“kill switch”)</u> We seek some clarification on the account recovery process in the event that a consumer activates the kill switch. Can we reactivate the account via email / 2FA or does MAS have preferred reactivation options for a customer in such a scenario? We would like to ask, MAS mentions that Kill switch should be "available through a different channel from bank's mobile or internet banking channels". Could you provide some examples of different channels? If it is a log out of all devices function, that will cease the log in session for everyone, including the current user, and the customer must change the password by email to access the account again, will this be sufficient as a Kill switch Can the Kill switch simply block off the account for just making transactions (including not using the card) be sufficient? Question 8. MAS seeks any other comments on the draft amendments to the EUPG (in Annex A), which have been published together with this consultation paper. Section 5.5 of the EUPG states that “The account holder of a protected account is not liable for the first S\$1,000 of loss arising from an unauthorised transaction, if the loss arises from any action or omission by any third party not referred to in paragraph 5.5 and does not arise from any failure by any account user to comply with any duty in Section 3.” Can we please clarify who should be liable for this loss in this case. Is the intention for the FI to be liable and to pursue claims against the third party? Could MAS please provide some examples of such situations so we can understand the context of this better. Is the intention here to set up a mandatory imbursement facility?
11	Respondent E	Question 4. MAS seeks comments on including the measures in Table 1 of the consultation paper into the EUPG, which will make them applicable to all responsible Financial Institutions.

S/N	Respondent	Responses from respondent
		Our comments on specific proposed measures are set out below. As a separate comment, the development of such enhancements proposed by MAS may require contributions from multiple specializations (such as legal, risk & compliance, product engineers, customer service, etc.). Therefore, if MAS decides to mandate such measures, we seek MAS' understanding to grant FIs sufficient time for the development, testing, and implementation of these measures as part of the enhancements by responsible FIs. We request that MAS provide PSPs (Payment Service Providers) with a transitional period of at least 6 to 12 months to implement these changes. Removal of Hyperlinks: Embedded hyperlinks are particularly helpful to certain customer segments that may have challenges navigating to certain e-payment features that they need. Such customer segments include non-digital natives, senior citizens, etc. If the removal of hyperlinks is eventually deemed as not necessary, we propose the alternative that payment service providers provide regular education to users to identify legitimate websites and phone numbers and that sender of messages are legitimate. In fact, allowing payment service providers to provide hyperlinks and phone numbers increases the chances of users navigating to legitimate websites and businesses. Measures prior to performing high-risk activities: We submit that FIs be permitted to adopt a risk- based approach when implementing authentication measures and pop-up risk warning messages prior to performing a high-risk activity. Blanket triggering of authentication measures and warning messages can desensitize a user and make user less likely to detect unauthorized transactions. Instead, if FIs take a risk-based approach and perform these measures considering other information about the user e.g. profile, user behavior to date, transaction patterns, geolocations, these measures can be targeted and more effective. Duty to impose cooling off period: We request that MAS clarifies what it means by "activating a digital security token", i.e. does it mean turning on the digital security token for the first time? In addition, a 12-hour cooling off period arguably causes disproportionate friction to legitimate users. Legitimate users could have a genuine need to make a certain payment within a short timeframe after activating a digital security token. We recommend MAS consider alternative approaches that protect users whilst enabling legitimate transactions, such as requiring additional login steps for high-risk activities taken within 12 hours from the time the token was activated. Kill Switch: We respectfully submit that a self-service kill switch that freezes many account functions in one step would not be as effective as multiple layers of protections and checks that payment service providers currently have in place. For instance, we have developed technical capabilities to detect factors suggesting that an unauthorized

S/N	Respondent	Responses from respondent
		transaction is taking place and has built identity and authentication controls to safeguard the customers. Examples include device fingerprinting, browser fingerprinting and telemetry that allows detection of new devices being used to access an account, changes in the user's usage pattern etc. Also, there are email and in-app notifications for all critical activities like password changes, transaction, profile change. We send notification alerts and make users go through authentication measures proportionate to the risk when we detect suspicious activities like log-in from new device, geolocation change or when we suspect unauthorized actions. This tailored approach calibrates defenses based on risk and balances protection against unauthorized transactions and enabling legitimate use of accounts. A kill switch is a blunt tool that disproportionately impacts user's payment experiences. In the event MAS mandates a kill switch, we would like to seek MAS' expectations on the extent of such a kill switch and whether it should result in the complete shutdown of the account or suspension of certain services or functionalities only (e.g. critical access to high-risk activities). Question 5. MAS seeks comments on the proposed enhancements to responsible Financial Institutions' duties in Table 2 of the consultation paper. Information to enable consumers to validate their intended recipient: We submit that in practice, including all the recommended information in an SMS message is counterproductive. First, SMS messages have a character limit and overly long messages may not always be displayed clearly to the user, preventing successful authentication. Messages spread over several SMS-es will also increase costs disproportionately, which leads to additional data costs to the customer. Second, having full details of the transaction may increase chances of such information being exposed to scammers. Instead, customers should be educated to report on OTPs that they are not expecting from the FIs.
12	Respondent F	Question 7. MAS seeks feedback on the proposed new guidelines for handling erroneous transactions, where the request for the return of funds is initiated by the "wrong recipient". We would like to clarify whether the scope of payment transactions include those made within the FI's ecosystem (i.e. sender and recipient FI are the same). If so, will the proposed timeline in Table 4 continue to apply, or will it be sufficient to just adhere with the last duty under T+9 days?