Response to MAS Consultation P017-2026

Consultation on Expanding FIDReC Membership to Payment Service Providers
King Yew Choo · Submitted 6 November 2026

RESPONDENT DETAILS

Name / Organisation	King Yew Choo
Email address	k.choo@trueprimary.com
Identity published with the submission	Yes
Any part kept confidential	No

QUESTION 1

Question 1. MAS seeks comments on i) the requirement for all MPI and SPI licensees, and MAS-regulated stablecoin issuer licensees after the stablecoin regulatory framework comes into force, to subscribe to FIDReC; ii) the exclusion of money-changing licensees from this requirement; and iii) the corresponding amendments to Part 1 of the Second Schedule of the DRS Regulations.

Summary

I support the requirement in limb i), for MPI and SPI licensees and for MAS-regulated stablecoin issuer licensees on the timing MAS proposes. In the onboarding the paper envisages (paragraph 4.1), I suggest FIDReC ask each newly covered firm that accepts payment instructions from a customer's AI agent what it could show if the customer disputed a payment: the mandate in force, what happened to each attempt, and the amount still charged (paragraph 6). I ask MAS to set out in guidance what any institution accepting such instructions should keep. Four further suggestions for MAS follow from the worked example. They concern classifying a payment outside a mandate term the institution agreed to enforce, under the E-Payments User Protection Guidelines and for cards, tokens and stablecoins (paragraphs 3 and 9); guidance on which payment service, if any, a firm running an agent supplies (paragraph 5); period limits counted at approval (paragraph 7); and retention by a licensed provider that uses the customer's instruction in its licensed service (paragraph 8). I have no comment on limb ii) and two drafting points on limb iii).

i) The requirement for all MPI and SPI licensees, and MAS-regulated stablecoin issuer licensees after the stablecoin regulatory framework comes into force, to subscribe to FIDReC

1. I support the requirement. Paragraph 3.2 of the paper names the disputes customers of payment institutions can have, including "apportionment of liability (including scam losses)". Payments by AI agents add a form of that dispute: MAS's media release of 3 July 2026 on the Safeguards for Agentic Finance at Runtime (SAFR) white paper describes an industry use case in which agents "can execute routine transactions within predefined mandates". The requirement also brings in licensees beyond the e-wallet providers that already subscribe, such as digital payment token service providers. Their customers could then bring an eligible dispute about the firm's own service, for example a transfer made after the customer withdrew the mandate, where the case turns on when the withdrawal took effect and when the firm accepted the agent's instruction.

2. Take an individual who holds an e-wallet issued by a major payment institution whose licence covers account issuance. The account stores specified e-money, can hold more than S$1,000 and can be used for electronic payments, so it is a protected account under the Guidelines. The customer and the institution agree that an AI agent run by another firm (the agent's provider) may pay from it, without a card, up to S$50 a payment and S$200 a week, to online merchants, for three months, with one payment per purchase. I use an e-wallet, whose issuer already subscribes, because it is the payment institution account the Guidelines protect; the record in paragraph 6 matters as much at the newly covered firms. The agent pays many times while the customer is absent. A payment that goes wrong may fall into one or more of three cases.

(a) Outside the mandate. The payment exceeds a limit, goes to a payee outside the permitted categories, is made after the mandate expired or was withdrawn, or is a second payment for a purchase already paid. The customer can complain to the institution about terms it agreed to enforce, and to the agent's provider about any term the provider undertook to enforce. Who bears the loss then depends on what each firm agreed, what caused the loss, and the Guidelines (paragraph 3 below).

(b) Mistaken, inside the mandate. Within the limits and without fraud, the agent buys the wrong item, or buys the same item again as a new purchase. The customer can take that up with the agent's provider, under their agreement. If the institution executed a payment the mandate allowed, the shopping error alone shows no failure by the institution.

(c) Credential misuse. Someone other than the agent uses its credential. The customer reports it to the institution, which assesses the claim under the Guidelines' liability rules. A thief using the credential inside its limits can match the agent's credential reference, payee and amount, so a matching record does not by itself show that the agent made the payment; the institution can ask the account holder for information on the device used and on whether, and when, an access code or authentication device was lost, stolen or misused (Guidelines, paragraph 3.18), and compare its own authentication record with any record the agent's provider holds of sending the instruction.

3. The Guidelines define an unauthorised transaction as one initiated "without the actual or imputed knowledge and implied or express consent of an account user", and an account user includes a person authorised "by the responsible FI and any account holder" under the account agreement to initiate payments. If the agreement authorises the agent's provider in that way, the provider is an account user, and paragraph 5.3 treats a transaction that "any account user knew of and consented to" as authorised, "notwithstanding that the account holder may not have consented to the transaction"; read literally, a payment its agent initiates outside the mandate could then be authorised, depending on whether the provider knew of and consented to that payment and whether its authority had already ended. Footnote 4(b), which covers a transaction "performed by a person as a result of the account holder sharing access and usage of their devices with the person", does not address a credential issued for an agent under limits agreed with the institution. Paragraph 5.3 makes the account holder "liable for all authorised transactions up to any applicable transaction limit or daily payment limit that the account holder and responsible FI have agreed to". The example's S$50 is such a transaction limit, so it caps the customer's liability for one authorised S$60 payment at S$50; two S$30 payments for one purchase each fall within it, though together they break the one-payment term. Paragraph 5.3 does not expressly reach the mandate's other terms: the S$200 weekly limit, the permitted payees or the one-payment term; a payment after expiry or a withdrawal turns first on whether the provider was still an account user when it was made. A second payment goes to the intended merchant, so Section 6's recovery duties for money sent to a wrong recipient do not reach it either.

Today, an institution that assesses a customer's claim over such a payment as outside Section 5 should still resolve it "in a fair and reasonable manner" (paragraph 4.23), and paragraph 4.27 lets the customer and the institution then turn to other dispute resolution, including mediation at FIDReC where the institution is a member. I suggest MAS state, in the Guidelines or in guidance on them, that a payment outside a term of the mandate that the institution agreed with the customer to enforce is unauthorised unless the customer separately approved it before it was made. Paragraph 5.4 would then leave the customer not liable where the loss arises from the institution's action or omission and not from an account user's failure to comply with a duty in Section 3. The rule would settle only how such a payment is classified; who bears the loss would still turn on its cause and the rest of Section 5.

4. FIDReC's Terms of Reference decide whether it can hear such a complaint. The customer first raises it with the institution (Rule 4(2)), and the activity or dispute must arise "out of matters relevant to the Eligible Complainant being or having been a customer of the FI" (Rule 4(1)(iii)). The customer can apply to FIDReC once the institution's internal dispute resolution has failed to resolve it, or four weeks after it was referred to the institution, whichever is earlier, and no later than six months after the institution's final reply (Rule 13), subject to the exclusions in Rule 5. The institution must be within FIDReC's jurisdiction as a subscriber or by consent (Rule 4(1)(ii)), and so must the activity complained of (Rule 4(1)(iv)); the institution must also have been a subscriber at the time of the act or omission complained of, or have agreed to let FIDReC consider the complaint, and must not have withdrawn by the time it is referred (Rule 4(1)(vi)). For a payment outside the mandate, that act or omission may be the payment itself or an earlier failure to act on a withdrawal. The consent route in Rule 4(1)(ii) is for an FI, which the Terms define as "a financial services provider that provides Financial Services to individuals and / or businesses" admitted as a subscriber; Annex 1 makes an Agreed Fee payable by an FI that submits to FIDReC's jurisdiction without being a subscriber, and by a subscriber that chooses to submit to FIDReC's jurisdiction over a dispute that is not an Eligible Dispute (Clauses 6.7 and 6.8). An agent's provider that is not a financial services provider cannot open either route; a complaint against the provider about the agent's choice of purchase can reach FIDReC only where the provider is an FI within FIDReC's jurisdiction and either the complaint meets the conditions above or the provider, as a subscriber, chooses to submit to FIDReC's jurisdiction over it.

5. The Payment Services Act 2019 decides which providers of agents this proposal brings in. Section 5(1) requires a licence, or an exemption, for each type of payment service a firm carries on a business of providing within its territorial scope, and an agent's provider may supply one, several or none. Where the agent pays in money, the First Schedule excludes executing a payment transaction "if performed by a commercial agent authorised to negotiate or conclude the sale or purchase of goods or services on behalf of the payer or the payee" (Part 2, paragraph 2(a)). That excludes only the execution, so a provider that also issues the customer a payment account or e-money, as section 2 defines them, may supply another payment service. Paragraph 2(h) excludes services of a technical service provider "that supports the provision of any payment service, but does not at any time enter into possession of any money under that payment service". A provider that transmits the customer's digital payment tokens, or arranges their transmission, may supply a digital payment token service, which the Act defines separately. I suggest MAS set out in guidance which service each of three providers supplies, if any, and so whether it needs a licence: one in the business of concluding the customer's purchases as its authorised agent, which pays for them in money; a technical provider that only passes the agent's instructions to the customer's institution, never entering into possession of money or arranging a cross-border transfer; and one that arranges transfers of the customer's tokens for the agent. Once licensed as an MPI or SPI, a provider would have to subscribe under this proposal; one holding no licence the proposal names would not.

6. When FIDReC's Case Manager writes to the institution advising it of the complainant's dispute resolution form and requesting relevant information (Rule 15(3)), the institution must respond "within 21 Days of the date of the Request" (business days) with its full investigation report, the grounds of its decision and the relevant documents. I suggest MAS set out in guidance what an institution that accepts payment instructions from a customer's agent should keep, and that FIDReC, when it onboards each newly covered firm, ask it to say, for each such payment, which of the following it holds or can obtain, which it cannot, and which do not arise in its service:

- the mandate's terms in force when the payment was made: the limits per purchase or payment and per period, the payees or categories permitted, the expiry, the one-payment term or any agreed instalments, the agent authorised, and any amount above which the customer must approve;
- when the customer authenticated those terms, and when any withdrawal reached the institution and took effect;
- the amount, payee and time of each attempt, a non-secret reference to the credential presented, and any separate approval the customer gave;
- the outcome of each attempt, and a reference linking it to any hold, its release or expiry, posted debit, reversal or refund, with the amount and time of each and the net amount still charged;
- who supplied any indicator that the agent initiated the payment, and the identifier of the purchase it paid for, which the agent should repeat on every retry;
- for the period limit, the amount each approval counted against it before the payment proceeded, in the order approved, and the running total.

7. Two items in that list, the purchase identifier and the running total against the period limit, bear on the hardest complaints, and neither settles them alone. A repeated purchase identifier links attempts at one purchase, but an agent whose reply was lost may retry under a fresh identifier, and agreed instalments can share one; the investigation compares the customer's instruction with the provider's order, the attempts, and the payments that remained after reversals and refunds. For the weekly limit, suppose S$170 is used and two S$20 payments are approved together. If each is checked against the S$170 already used, both pass, approvals for the week reach S$210, and neither record shows which payment crossed the limit. An institution that counts each amount against the limit as it approves it admits the first and declines the second; I suggest MAS expect that of any institution enforcing a period limit for an agent. An institution may already hold each payment's amount, payee and time; the onboarding question tests whether it can link them to the mandate in force and to each attempt's outcome, and shows the gap where the payment message carries neither the identifier nor the indicator to the institution.

8. The institution's record need hold nothing of what was bought. A complaint over what the agent bought turns on the customer's instruction to the agent, which may sit with the agent's provider or on the customer's device. A provider could give the customer a dated copy of the instruction, with its order reference, on accepting the order, for the customer to put before FIDReC, which can request relevant material from the complainant as well as the institution (Rule 15(3)). Where a licensed provider uses the instruction in its licensed service, I suggest MAS expect it to keep the relevant part for a stated period after the purchase is completed or cancelled, long enough for the customer to complain; to preserve it, once it knows of a complaint, until six months after the final reply defined in Rule 13 or, if the complaint is referred to FIDReC in time, until the case closes; and to give the customer timely access. SAFR asks each Audit Log entry to capture "the mandate against which the action was checked", "subject to appropriate data minimisation, access controls, and retention requirements"; its Mastercard case study describes a record of the consumer's authorisation that "supports dispute resolution and audit across the ecosystem".

9. Among MPI and SPI licensees, the Guidelines' liability rules protect accounts only at a major payment institution whose licence covers account issuance, and only accounts storing specified e-money. Section 5 does not apply to credit, charge or debit cards the institution issued (paragraph 5.1; footnote 2 defines debit cards), and the Guidelines' definition of money "does not include digital payment tokens", so an agent's payment in digital payment tokens falls outside their definition of an unauthorised transaction and their liability rules. The customer could still bring an eligible dispute to FIDReC about a newly covered firm's own token service (paragraph 1), though the Guidelines give no rule to classify the payment. For payments by those cards, in digital payment tokens, and in MAS-regulated stablecoins once their framework is in force, I suggest MAS consider an equivalent classification under the arrangements that govern each service, and expect the record in paragraph 6 wherever a licensee accepted the agent's instruction. The paper's reason for issuer membership is holders' envisaged right to redeem directly from the issuer (paragraph 3.3); a complaint about the agent's transfer concerns the licensee that accepted the instruction, which need not be the issuer.

ii) The exclusion of money-changing licensees

No comment.

iii) The corresponding amendments to Part 1 of the Second Schedule of the DRS Regulations

10. Proposed item 10 would cover MPI and SPI licensees, and paragraph 3.5 envisages a further amendment for MAS-regulated stablecoin issuer licensees after their framework comes into force. Two drafting points: the banner above Annex A refers to the Payment Services Regulations 2019, though the amendment is to the DRS Regulations; and paragraph 3.3 refers to footnote 6 for "eligible complainant", which footnote 7 describes.

Capacity and interest

11. I respond in a personal capacity. My response to MAS consultation P012-2026 on 30 July 2026 discussed tracing one instruction across retries. My working paper and an individual Internet-Draft (work in progress) set out the checks a server makes before it starts paid work for an agent, and the use case I submitted to the ITU-T Focus Group on Trust and Identity for Humans and Agentic AI (FG-TIDA) covers what a seller can check before it commits that work. This response asks what an institution can show its customer and FIDReC after a disputed payment. I founded True Primary, which builds infrastructure for the agent-initiated purchase of expert work, and declare its commercial interest in the safe adoption of agentic payments.

References

- MAS, Consultation Paper on Expanding FIDReC Membership to Payment Service Providers, P017-2026, October 2026.
- MAS, E-Payments User Protection Guidelines, with effect from 16 December 2024: https://www.mas.gov.sg/regulation/guidelines/e-payments-user-protection-guidelines
- FIDReC, Terms of Reference, version 2.2, 1 July 2025: https://www.fidrec.com.sg/knowledgebase/article/KA-01002
- Payment Services Act 2019, sections 2, 5, 13 and 100 and First Schedule: https://sso.agc.gov.sg/Act/PSA2019
- MAS, media release, "MAS Partners Industry to develop Safeguards for AI Agents in Finance", 3 July 2026: https://www.mas.gov.sg/news/media-releases/2026/mas-partners-industry-to-develop-safeguards-for-ai-agents-in-finance
- MAS, Safeguards for Agentic Finance at Runtime (SAFR), white paper, version 1.1, 9 October 2026 (the version quoted in paragraph 8): https://www.mas.gov.sg/-/media/mas-media-library/development/fintech/ai-safr/safr-v1-1.pdf
- King Yew Choo, Response to MAS Consultation P012-2026, submitted 30 July 2026.
- King Yew Choo, A Payment and Entitlement Gate for Self-Serve Agentic Expert-Access: Architecture and a Formal Admission Model, version 2.9, dated 29 September 2026, posted on SSRN 30 September 2026: https://doi.org/10.2139/ssrn.7543686
- King Yew Choo, A Server-Side Model for Gating Agent-Initiated Human-Sourced Asynchronous HTTP Tasks on Payment or Entitlement, draft-king-yew-choo-agentic-payments-01, individual Internet-Draft, work in progress, 8 October 2026: https://datatracker.ietf.org/doc/draft-king-yew-choo-agentic-payments/
- King Yew Choo, FG-TIDA use case, "A seller checks the paying agent's attested software and its user's spending authority before starting paid work", submitted 19 October 2026: https://github.com/FG-TIDA/use-cases/issues/35