

Personal response on agentic payments

Question 15: how existing payment services regulation needs to adapt to support agentic payments

Respondent	King Yew Choo, London, United Kingdom
Capacity	Personal capacity
Contact	k.choo@trueprimary.com
Affiliation	Founder, True Primary; interest declared at paragraph 2
Written record	https://kingyewchoo.co.uk
Date	1 October 2026
Confidentiality	None. I am content for this response to be published in full and attributed to me.
Structure	Numbered paragraphs 1 to 29, with a summary above and references below.

Summary of what I ask for

I ask for five changes. They take question 15's three examples, consent, authentication and liability, and add the evidence that joins them.

- 1. A bounded delegation, recognised as consent.** A consumer's grant of spending authority to an agent should count as consent to a series under regulation 67(1)(b), recorded with its limits. A payment outside the limits should be unauthorised, however it is funded, as should a second execution under the same request key (paragraphs 7 to 10 and 16).
- 2. Authentication at the grant.** The FCA's outcomes-based rules should let strong customer authentication attach to the delegation when it is created or changed, with fresh authentication above a threshold, and the provider free to ask for it when monitoring flags a payment. The liability rules keyed to strong customer authentication should move with it, without making the grant prove that a later payment was authorised (paragraphs 11 to 14).
- 3. A credential issued for the agent.** The credential should be issued for one agent, bound to the limits the consumer authenticated and revocable at once. A consumer then need never hand an agent the codes and passwords that regulation 72(3) requires them to take all reasonable steps to keep safe (paragraphs 15 and 16).

4. **A decision on the payment the consumer did not intend.** Where a fraudster deceives the agent, the Faster Payments and CHAPS reimbursement rules should treat the consumer as deceived. The reimbursing provider should recover from the agent's provider where that provider's breach of a defined duty caused the loss. Loss on a payment outside the delegation should be recoverable from the party that should have stopped it (paragraphs 17 to 21).
5. **An evidence record, and Know Your Agent that covers the agent's state.** The FCA's rules should set what a record must show for an agent's payment, whichever scheme holds it, and the agent's provider should keep the consumer's instructions. Know Your Agent work should cover what the agent was running as well as which agent it was (paragraphs 22 to 24).

Paragraphs 25 to 27 apply these to three proposals made elsewhere in the consultation: the stablecoin perimeter, the review of the payment initiation definition, and the right of access for variable recurring payments.

Central position. The Payment Services Regulations already hold most of what agentic payments need: consent to a series, withdrawal with prospective effect, a refund where the payer did not consent, and a burden of proof on the provider. They do not yet name a bounded delegation as the object of that consent, or provide the authentication, credential and record that make it work. Who bears a payment the consumer did not intend is answered only in part. The consent rule belongs in legislation, authentication and the record in the FCA's rules, and fraud against the agent in the reimbursement rules (paragraph 28).

Introduction

1. I respond in a personal capacity, to question 15. Where I touch proposals the consultation makes elsewhere, at paragraphs 13, 19 and 25 to 28, it is only as they bear on agentic payments. On 2 September 2026 I responded to the Bank of England's consultation on the design of the future retail payments infrastructure, on what that infrastructure should carry for payments an agent initiates.¹ This response addresses the rules those payments run under.
2. I founded True Primary, which builds infrastructure for the agent-initiated purchase of expert work and has a commercial interest in the safe adoption of agentic payments. My related published work is an individual Internet-Draft² and a working paper³ on gating paid agent tasks on payment or entitlement. Both apply a pattern that the Action Evidence Boundary draft sets out more generally.⁴ No part of this response is confidential.

3. The independent Financial Services AI Adoption Plan, which HM Treasury published alongside this consultation, asks in its Recommendation 10 for a trust framework on three pillars: legal and liability frameworks, Know Your Agent protocols, and authentication and governance.⁵ Question 15's three examples, authentication, consent and liability, fall within those pillars.

The case the regulations have to handle

4. In this response an agent is an AI agent acting for a consumer; regulation 2(1) uses the word for an agent of a payment institution, which is a different thing. By the agent's provider I mean the business that takes on the consumer's delegation and runs the agent that exercises it. What I say of consumers applies equally to micro-enterprises and charities (paragraph 21). A consumer lets one named agent buy services within limits: up to £20 a purchase and £100 a week, from UK online sellers, for 3 months. The agent then pays many times, to payees the consumer has not seen, while the consumer is absent. Each purchase is an electronic remote payment transaction. Where the payer initiates it, directly or through a payment initiation service provider, regulation 100(2) requires strong customer authentication that dynamically links it to a specific amount and a specific payee, subject to the exemptions in the technical standards.⁶ The FCA applies strong customer authentication in the same way to a card payment initiated through the payee.⁷
5. The consumer cannot authenticate each payment, and being absent is the point of delegating. Three routes are open to get round this, and each strains a different part of the regulations.
- The consumer gives the agent their card details and passes it the one-time codes that authentication then asks for, or gives it their online banking password. The FCA reads personalised security credentials to include a PIN or password and to exclude the card number itself, and regulation 72(3) requires the consumer to take all reasonable steps to keep them safe.⁷
 - The consumer's provider fits the agent's payments into exemptions written for other patterns (paragraph 12).
 - A provider issues the agent a credential of its own, limited in what it can spend.
6. The third route is the one to make safe and ordinary, and industry has built several arrangements close to it. They bound different things. A Stripe shared payment token is a grant the agent makes to one seller, with a maximum amount and an expiry, so it bounds what that seller can take.⁸ Mastercard's Agent Pay for Machines lets an organisation set spending limits that are programmatically

enforced.⁹ A UK variable recurring payment consent, which a payment initiation service provider registers with the account provider, carries a maximum individual amount and periodic limits that the account provider applies.¹⁰ The last two bound what can be spent under them, which is the shape of a consumer's delegation.

Consent: a bounded delegation

7. Regulation 67(1)(b) already provides the home. A payment counts as authorised only if the payer consented to it, or to "the execution of a series of payment transactions of which that payment transaction forms part". A consumer who grants an agent spending authority once, for payments to come, can give consent of the second kind, in the form agreed with the provider (regulation 67(2)(b)). Regulation 71(1) lets the payer and the provider agree spending limits on a payment instrument, and requires none. Neither the FCA's guidance nor the Open Banking Standard yet applies the series limb to a delegation that leaves the payee to the agent, and a narrower reading is open. That uncertainty is itself a reason to state the rule in legislation (paragraph 28).
8. For a series an agent initiates for a consumer, the consent should carry its limits, recorded with the consumer's provider or with a provider acting for it. The limits are a maximum per payment, a cumulative limit over a stated period, the payees, or categories of payee, permitted, an expiry, the agent authorised, and a threshold above which a payment returns to the consumer (paragraph 13). They follow the mandate I set out to the Bank of England, with withdrawal covered at paragraph 9 and rails added at paragraph 25.¹ The expiry should be compulsory. A variable recurring payment consent may run indefinitely if its end date is left blank, and a delegation the consumer forgets should lapse on its own.¹⁰
9. The regulations should then state what is now only a reading of them: a payment outside the limits is not part of the series, so it is unauthorised under regulation 67 and refundable under regulation 76(1). Where it draws on credit, the consumer credit rules apply instead (paragraph 16). The FCA already reads a merchant's mandate this way: a payment at a price outside its scope "would be unauthorised unless the customer agrees to amend the mandate or set up a new mandate".⁷ The rule should attach to the limits the payment order lets the enforcing provider test when it decides the payment, such as the amounts, the payee and the expiry. What the agent may buy, which no payment order shows, sits with the party that accepts the agent's request (paragraph 15). Withdrawal already works in law: regulation 67(4) lets the payer withdraw consent to a series at any time, subject to regulation 83(3) to (5), so that future payments are unauthorised. For an agent that pays many times a day, withdrawal takes effect in practice only where the party enforcing the limits can stop the next payment. The credential at paragraph 15 is what makes that possible.

10. A repeat is where a series consent is weakest. An agent that times out and retries can present the same purchase twice. Where the consent is defined by its limits alone, both executions fall within it, so neither is unauthorised under regulation 67(1)(b). The consent for an agent's series should cover each purchase once, identified by a request key that travels in the payment order. A second execution under the same key should fall outside the consent. The key has to reach the provider enforcing the delegation, so that provider can refuse the repeat.⁴ If a repeat executes, it is outside the consent, and the consumer's provider refunds it as it would a payment outside the limits (paragraph 9). It should be able to recover from the party that received the key twice and executed it, as regulation 76(5)(b) already provides against a payment initiation service provider. A repeat sent under a fresh key meets no key check, and nothing in the payment distinguishes it from a second purchase the consumer wanted.¹ I would leave its cost between the consumer and the agent's provider, whose agent made it (paragraph 20). The consumer's instruction, which the agent's provider keeps (paragraph 22), should show whether the agent repeated a purchase.

Authentication at the grant

11. Dynamic linking cannot attach to a delegation in which the agent chooses the payee. Article 5 of the technical standards makes the authentication code specific to the amount and the payee the payer agreed, or, for a batch, to its total and its specified payees.¹¹ A delegation fixes neither: the amount varies within a limit, and the agent chooses the payee. What the consumer can strongly authenticate is the delegation itself.

12. The exemptions that come closest each fit part of the case, and none fits all of it.

- Trusted beneficiaries (Article 13) needs the payee on a list the payer created in advance.
- Recurring transactions (Article 14) needs the same amount and the same payee.
- Low-value transactions (Article 16) caps each payment, and falls away once the payments since the last authentication pass a small cumulative value or a small count, whichever measure the provider applies.⁷
- Secure corporate payment processes (Article 17) covers dedicated processes, such as single-use virtual account numbers with restricted parameters in a corporate purchasing system, which is the shape of the credential at paragraph 15, but only for payers that are legal persons.⁷
- Transaction risk analysis (Article 18) can cover some agent payments, at each provider's discretion. It needs the provider's fraud rate within a reference rate, the amount within a threshold, and a real-time analysis of that payment that finds no warning sign, such as an abnormal spending pattern.

The consumer cannot know in advance whether the agent's next payment will stop for authentication. Outside the exemptions, the FCA's treatment of merchant-initiated transactions comes nearest: the mandate is authenticated when it is set up, and later payments the payee initiates are outside strong customer authentication, "provided that an action of the payer is not needed to trigger their initiation".⁷ An agent triggers each payment from the payer's side, often to a payee that holds no mandate, so that treatment does not reach it.

13. The consultation records the government's commitment to commencing the revocation of the authentication regulations relating to strong customer authentication in the regulations, so that the FCA can make more outcomes-based rules (paragraph 2.8).¹² Those rules should include an outcome for delegated payments:

- strong customer authentication when the delegation is created or changed, bound to its limits;
- no further authentication of the consumer for a payment inside the limits, provided the provider relying on it enforces them and keeps the transaction monitoring that Article 2 now requires;
- the provider's freedom to ask the consumer to authenticate any payment its monitoring flags, with the payment waiting until they do;
- fresh authentication for a payment above the delegation's threshold, dynamically linked to that payment in the ordinary way.

This extends the logic of Articles 13 and 14, which authenticate a list or a series once and exempt what follows, from a fixed payee or amount to a bounded set.

14. The liability rules keyed to strong customer authentication should move with it. Regulation 77(4)(c) relieves the payer of any loss, fraud aside, where regulation 100 requires strong customer authentication and the payer's provider did not require it. Regulation 77(6) makes a payee, or its provider, that does not accept strong customer authentication where regulation 100 requires it compensate the payer's provider for the refund. The FCA's new rules should state that authenticating the delegation satisfies the requirement for each payment made under it with the agent's credential. Without that, every payment under the delegation outside an exemption, including one made with a misappropriated credential, is one where regulation 100 required authentication and the provider did not apply it. No provider can lawfully carry agent traffic on that footing. That rule settles authentication only: a payment the agent did not make stays unauthorised, with the burden of proof on the provider and the consumer's liability limited by regulation 77 as for any authenticated payment (paragraphs 16 and 22). Regulation 77(6) should keep working on the payee side where the payee can see an agent at work. A payee, or its provider, that accepts a payment marked as agent-initiated without that credential should compensate the payer's provider. A payee shown no sign of an agent takes on nothing new.

A credential issued for the agent

15. The regulations should recognise a credential issued for an agent's use, by the consumer's provider or a provider acting for it, as the ordinary way to delegate. Regulation 71 already supplies two of its parts: the payer and the provider may agree spending limits on a payment instrument, and the provider may stop its use on reasonable grounds of security or suspected misuse. Its properties matter more than its form. It is issued for one agent, bound to limits the consumer authenticated, and revocable at once. The issuer enforces on every payment the limits it can test from the payment order, the amounts, payees and expiry, and reserves each amount against the cumulative limit before the payment proceeds.⁴ Without that reservation, concurrent payments can each pass against the same headroom. The reservation then has to be committed when the payment clears and released when it fails or lapses. Each rule's rules should say how a partial execution, a fee, a currency conversion, a return or a refund changes it, and whether a refund restores the allowance, since either answer costs the consumer something. What the agent may buy, which the payment order does not show, sits with the party that accepts the agent's request. I set out both points to the Bank of England.¹ The FCA must already have regard to technology and business-model neutrality when it makes technical standards (regulation 106A(2)(d)), and a definition by properties keeps to that principle.
16. Two consequences follow. A consumer whose provider issues the agent such a credential hands over none of their own codes or passwords. The regulations should say that this alone does not breach regulation 72(3), and square it with the issuer's duty under regulation 73(1)(a) to keep credentials from anyone but the user. The duty to report the credential's loss or misuse would remain (regulation 72(1)(b)). A payment made with it outside its limits is identifiable as unauthorised when it is attempted, by the party able to refuse it. Without such a credential, the provider's controls still apply, but nothing in a payment shows that the agent made it or what the agent may spend. An online purchase from a trader is normally a distance contract. Unless it is an excepted contract (regulation 77(5)), regulation 77(4)(d) then relieves a consumer of any loss on an unauthorised payment, except for fraud.¹³ The FCA reads it the same way.⁷ On a debit card or an account in credit, the loss from a misused card or code therefore falls first on the consumer's provider. Credit is different: where a payment draws on a credit line under a regulated agreement, such as a credit card or an overdraft, regulation 64 disapplies regulations 76(1) to (4) and 77(1) to (5), and the Consumer Credit Act 1974 applies instead. A payment that takes an account into its overdraft falls under both regimes, part by part.⁷ Section 83 of that Act relieves the debtor of loss from use "by another person not acting, or to be treated as acting, as the debtor's agent".¹⁴ Whether that protects a consumer whose agent exceeds its delegation is unclear, so the rule at paragraph 9 needs a counterpart there.

Liability for the payment the consumer did not intend

17. Regulations 76 and 77 allocate the loss on an unauthorised payment. Agent payments add a case they do not reach: a payment inside the delegation that the consumer did not intend, because the agent erred, was misled by content it read, or was changed by its provider after the consumer delegated. On the reading at paragraph 7, such a payment falls within the consent, so regulation 76 gives no refund unless the delegation itself fails. Whether it fails where the agent was manipulated is a question I raised with the Bank of England.¹ The other routes are partial. Regulation 79 may refund a card payment, which is initiated through the payee, where the authorisation named no exact amount and the amount exceeded what the payer could reasonably have expected. The request must come within 8 weeks, and an account payment that the agent initiates has no such route. Section 75 of the Consumer Credit Act 1974 reaches a credit card issuer, never a debit card issuer. It gives a claim only for the supplier's misrepresentation or breach of contract, and never for an item priced at £100 or less, as every purchase in the example at paragraph 4 is.¹⁴ Card scheme chargebacks sit in the schemes' own rules, outside the regulations.
18. Fraud against the agent is the case to settle first. As the Payment Systems Regulator describes it, the authorised push payment reimbursement requirement applies to Faster Payments and CHAPS payments where the consumer "has been deceived into granting that authorisation".¹⁵ The reimbursement rules define authorisation as the payer's explicit consent to the payment or to "the execution of a series of payment transactions of which that payment transaction forms part", so an honest delegation can be the authorisation. The difficulty is the deception. Where a fraudster deceived the agent after the consumer delegated, and the authorisation is the delegation, the consumer was not deceived into granting it, and the rules define a scam by fraud used to "manipulate, deceive or persuade a Consumer". The payment may fall outside the requirement, though the harm is the one it exists for. The statute is wider than that test. Section 72 of the Financial Services and Markets Act 2023 obliged the Regulator to require reimbursement for Faster Payments orders "executed subsequent to fraud or dishonesty", words wide enough to cover fraud against an agent.¹⁵
19. I would settle it by treating deception of the agent as deception of the consumer, on the rails the requirement covers. The change is for the reimbursement rules: on Faster Payments for the FCA, once it inherits the Regulator's General and Specific Direction power (paragraph 4.38),¹² and on CHAPS for the Bank of England, which sets the CHAPS reimbursement rules.¹⁵ A consumer who delegates should keep the protection they would have had by paying themselves, with the same claim excess and maximum. The consumer standard of caution should apply to the consumer's own conduct on its present terms: gross negligence, shown by the provider.¹⁵ Its exception for vulnerable consumers should look to the time of the agent's payments. Neither a permitted

delegation nor a warning given only to the agent should count against the consumer. The cost should not stop with the sending and receiving providers, which share it today. The reimbursing provider should recover from the agent's provider the part of its loss caused by that provider's breach of a defined duty. Letting its agent ignore a warning, or a change to the agent after delegation that caused the payment, would be examples; an update alone should establish nothing. Where a payment provider or a payee required evidence of the agent's state (paragraph 24) and the agent's provider cannot produce it, the breach should be presumed until that provider shows otherwise. Recovery should never delay the consumer's reimbursement, and no provider should recover more than it paid.

20. A payment the agent made in error, without fraud, is a matter between the consumer and the agent's provider, under their contract and consumer law. The Competition and Markets Authority already tells a business using an AI agent in dealing with its customers that it is "responsible for what an AI agent does in the same way you are responsible for what an employee does".¹⁶ The part payment services regulation plays there is to make the facts of the payment provable (paragraph 22). Whether the agent was deceived or erred, the limits bound the spending the delegation admits in each period, on the reservation terms at paragraph 15. A defect in one agent reaches every consumer who delegated to it at once, so an issuer should be able to stop every credential it issued for that agent together.
21. Where a payment outside the delegation does execute, the consumer's provider refunds it, on the rule at paragraph 9. Where another provider issued and enforced the agent's credential, the regulations should let the consumer's provider recover from it, on the model of regulation 76(5)(b) (paragraph 10). Regulation 95 already makes another provider, or an intermediary, compensate a provider whose liability under regulation 76 is attributable to it. Whether an agent's provider or a credential issuer outside the perimeter is an intermediary there is unsettled. The regulations should say whether it is, and extend regulation 95 to it if not, whichever way the perimeter question at paragraph 26 is decided. As at paragraph 19, the refund should not wait on recovery. If recovery fails, the loss stays with the provider that refunded, as now, so HM Treasury should consider whether an agent's provider needs financial backing proportionate to what its agents can spend at once (paragraph 20). Payers other than consumers, micro-enterprises and charities may already agree with their provider that regulations 75 and 77 do not apply (regulation 63(5)), so the protections that need settling in law are those of consumers, micro-enterprises and charities.

Evidence, and Know Your Agent

22. Regulation 75 puts the burden on the provider to prove that a disputed payment was authenticated and recorded. Regulation 75(3) adds that the recorded use of a payment instrument is not in itself necessarily sufficient to prove that the payer authorised it. That holds for an agent's payment: a thief using the agent's credential inside its limits would leave the same record as the agent. For each payment, the record should show the delegation's terms in force, when they were authenticated and whether they had been withdrawn. It should also show the amount, payee and time, the credential used, a marker that the payment was agent-initiated, the request key, the agent that presented it, the reservation made against the limits and, by reference only, the service paid for. Existing records can supply the amount, payee, time and the delegation's terms by reference; the marker, the request key and the reservation are new fields. The record need hold none of the content of what was bought. A dispute over what the agent bought turns on the consumer's instruction to the agent. The agent's provider should keep that instruction for the dispute window and give the consumer, and whoever decides the dispute, timely access to it. The payment message need carry only references into the record: the mandate reference, the agent-initiated marker and the request key that I proposed to the Bank of England.¹ Industry is building records of this kind. Mastercard's Verifiable Intent records what a consumer authorised when an agent acts for them,¹⁷ and EMVCo's draft framework for card-based agentic payments, released on 1 September 2026, proposes intent services that register and retrieve consumer-authorised intent across participants.¹⁸ The FCA's rules should set what such a record must show to carry weight under regulation 75, whichever scheme holds it.
23. Know Your Agent, as described so far, centres on the agent's identity. Pillar 10.2 speaks of identity and verification frameworks for agents.⁵ EMVCo's framework centres on the consumer's authorised intent, and EMVCo said it may consider Know Your Agent capabilities in future publications, to help identify the agent involved and communicate relevant agent attributes.¹⁸ Visa's Trusted Agent Protocol and Mastercard's Agent Pay for Machines credential the agent in this sense.¹⁹ An identity alone does not show whether a registered agent still runs the model, tools and configuration it had when it was registered. The published descriptions of the programmes named here, Verifiable Intent included, mention no evidence of what the agent was running when it paid.
24. Evidence of that state exists in part. Remote attestation, in the architecture the IETF published as RFC 9334, reports on the state of the platform and software an agent runs on, and work on extending it to agents is under way.²⁰ I am preparing, as a use case for the ITU-T Focus Group on Trust and Identity for Humans and Agentic AI, the requirements a payee needs to check such evidence before committing a paid task.²¹ The trust framework's Know Your Agent work should

cover the agent's state as well as its identity. The FCA's evidence rules should leave room for a payment provider or a payee to require such evidence, without prescribing a technology. A dispute over a payment the consumer did not intend, and the recovery at paragraph 19, could then turn on what the agent was running when it paid.

Rails and the perimeter

25. The same delegation can meet different protections depending on the rail. Mastercard describes Agent Pay for Machines as settling across cards, accounts and stablecoins,⁹ and the x402 payment protocol, in the "exact" scheme its specification currently supports, settles by blockchain token transfer.²² The consultation proposes that overseas-issued stablecoins stay outside the payments perimeter unless HM Treasury recognises the regulatory framework of the issuer's jurisdiction (paragraph 3.12).¹² An agent that chooses its own rail could therefore take a consumer's payment outside Part 7 of the regulations without the consumer choosing that. The delegation's limits should include the rails the agent may use. The consent and liability rules above should apply to payments in UK-issued qualifying stablecoins on the same terms as to other funds.
26. The perimeter also turns on the rail. An agent's provider that initiates payment orders from the consumer's account at another provider, at the consumer's request, provides a payment initiation service. That needs authorisation: it cannot form part of a small payment institution's registered business (regulation 14(4)), and regulation 138(1) confines payment services to the providers it lists.⁶ The exclusion for technical service providers expressly does not cover payment initiation (Schedule 1, Part 2, paragraph 2(j)). An agent's provider whose agent pays by card with a credential issued for the agent's use may sit outside payment initiation. In the FCA's view, "the provider of a service that transmits a payer's card details, along with a payment order, to the payer's payment service provider, but does not come into possession of personalised security credentials, is not carrying out a payment initiation service".²³ Whether a credential issued for an agent is such a credential, and whether the provider then meets the technical-services exclusion's own conditions, are open. On any rail it may also fall within the exclusion for a commercial agent authorised to negotiate or conclude purchases for the payer alone (Schedule 1, Part 2, paragraph 2(b)). The same spending authority can then be regulated on one rail and unregulated on another, or on neither. The review of the payment initiation definition (paragraph 4.18) should decide whether exercising a consumer's delegated spending authority brings a provider inside the perimeter, whatever the rail.¹²

27. On the account-to-account rail the consultation already has the vehicle. The proposed right of access for variable recurring payments could take the form of letting a payment initiation service provider lodge a payment mandate for a series of payments (paragraph 4.12).¹² If that mandate can carry the delegation's limits, the agent authorised and an agent-initiated marker, agent payments by account transfer have the structure above from the start. The interface standards proposed at paragraphs 4.22 and 4.31 are where to require it, with each amount reserved against the limit before the payment proceeds. Today a variable recurring payment consent whose payee varies runs only under delegated authentication,¹⁰ where the account provider lets the initiating provider authenticate under a contract that, the FCA expects, addresses the allocation of liability between them.⁷ The outcome at paragraph 13 would give that arrangement a rule to stand on, beside the contract.

What should sit in legislation

28. The government may retain in legislation provisions that "establish key rights, obligations or protections for consumers and firms" (paragraph 2.9).¹² On that test, legislation beside regulations 67, 71, 76, 77 and 95 should carry the consent rule at paragraph 7 and the recognition of a credential issued for the agent (paragraph 15). It should also carry the rule that a payment outside the delegation, or a repeat under the same request key, is unauthorised, with the refund and the recovery that follow and a counterpart for regulated credit (paragraph 16). The form of authentication at the grant, the contents of the evidence record and any technical profile belong in the FCA's rules, where they can change with the technology. The reimbursement change at paragraph 19 belongs in the reimbursement rules.

29. With these changes, a consumer could delegate spending to an agent and keep the protections they have when they pay themselves, provided the limits are enforced as paragraph 15 sets out. A payment the agent makes in error inside those limits would remain, like a consumer's own mistake, a matter of contract and consumer law (paragraph 20). I would be glad to contribute to the trust framework work that Recommendation 10 proposes, and to provide further detail on any point.

References

1. King Yew Choo, "Personal response on programmable and agentic payments", response to the Bank of England's Retail Payments Infrastructure Board consultation on the Design of the Future Retail Payments Infrastructure, 2 September 2026, paragraphs 9, 18, 19, 22, 24, 25, 38, 44 and 51. <https://kingyewchoo.co.uk/responses/bank-of-england-retail-payments/> Accessed 30 September 2026.
2. King Yew Choo, "A Server-Side Model for Gating Agent-Initiated Human-Sourced Asynchronous HTTP Tasks on Payment or Entitlement", Internet-Draft draft-king-yew-choo-agentic-payments-00, 23 July 2026. An individual submission, not adopted by any IETF

working group; work in progress. <https://datatracker.ietf.org/doc/draft-king-yew-choo-agentic-payments/00/> Accessed 1 October 2026.

3. King Yew Choo, "A Payment and Entitlement Gate for Self-Serve Agentic Expert-Access: Architecture and a Formal Admission Model", working paper, version 2.9, 29 September 2026, posted on SSRN on 30 September 2026. <https://doi.org/10.2139/ssrn.7543686> Accessed 30 September 2026.
4. I. Schrock, "The Action Evidence Boundary for Consequential Agent Effects", Internet-Draft draft-schrock-action-evidence-boundary-07, 25 September 2026, work in progress. It requires, among other things, exact-action binding, durable atomic consumption or reservation of authority, and a durable same-action fence that refuses a new attempt while an earlier attempt at the same action is in flight or uncertain. <https://datatracker.ietf.org/doc/draft-schrock-action-evidence-boundary/> Accessed 30 September 2026.
5. HM Treasury, Financial Services AI Adoption Plan, independent report, 14 July 2026, Recommendation 10 ("Agentic payments readiness"), pillars 10.1 to 10.3. <https://www.gov.uk/government/publications/ai-adoption-plan-financial-services/financial-services-ai-adoption-plan> Accessed 30 September 2026.
6. The Payment Services Regulations 2017, S.I. 2017/752, as amended: regulations 2(1), 14(4), 63(5), 64, 67, 71, 72, 73(1)(a), 75, 76, 77, 79, 80, 83, 95, 100, 106A and 138(1), and Schedule 1. <https://www.legislation.gov.uk/ukSI/2017/752/contents> Accessed 30 September and 1 October 2026.
7. Financial Conduct Authority, "Payment Services and Electronic Money: Our Approach", version 8, May 2026, paragraphs 8.144, 8.179, 8.200, 8.201, 8.218, 8.223, 20.9, 20.25, 20.62 and 20.65. <https://www.fca.org.uk/publication/finalised-guidance/payment-services-electronic-money-approach.pdf> Accessed 30 September 2026.
8. Stripe, "Shared payment tokens", documentation, public preview: a shared payment token is "a scoped grant to use the customer's payment method", which the agent grants to a seller "with usage and expiration limits". <https://docs.stripe.com/agentic-commerce/concepts/shared-payment-tokens> Accessed 30 September 2026.
9. Mastercard, "Mastercard launches Agent Pay for Machines to unlock super-fast, always-on payments", press release, 10 June 2026: organisations "can set authorization rules and spending limits that are programmatically enforced", and the service supports settlement "across cards, accounts and stablecoins". <https://www.mastercard.com/us/en/news-and-trends/press/2026/june/mastercard-launches-agent-pay-for-machines.html> Accessed 30 September 2026.
10. Open Banking Limited, Read/Write API Specification version 4.0, Domestic VRP Consents, control parameters MaximumIndividualAmount and PeriodicLimits, <https://openbankinguk.github.io/read-write-api-site3/v4.0/resources-and-data-models/vrp/domestic-vrp-consents.html>; and Open Banking Limited knowledge base, Variable Recurring Payments: "ValidToDateTime can be left blank which means the validity of the consent is indefinite", and, where authentication is delegated to the initiating provider, the payee's details "are not part of the VRP consent", <https://openbankinguk.github.io/knowledge-base-pub/standards/general/vrp.html> Both accessed 30 September 2026.
11. Financial Conduct Authority, Technical Standards on Strong Customer Authentication and Common and Secure Methods of Communication Instrument 2020 (the SCA-RTS), made under regulation 106A of the Payment Services Regulations 2017 and in force from 31 December 2020, replacing Commission Delegated Regulation (EU) 2018/389: Articles 2, 5, 13, 14, 16, 17 and 18. Current text: Chapter 1, <https://handbook.fca.org.uk/technical-standards/s140c1224>; Chapter 2, <https://handbook.fca.org.uk/technical-standards/s140c1225>; Chapter 3, <https://handbook.fca.org.uk/technical-standards/s140c1226> Accessed 1 October 2026.
12. HM Treasury, Modernising Payment Services Regulation: Consultation, 14 July 2026, PDF edition, paragraphs 2.8, 2.9, 3.12, 4.12, 4.18, 4.22, 4.31 and 4.38, and question 15. https://assets.publishing.service.gov.uk/media/6a54b3302467584757371dc4/Modernising_payment_services_consultation.pdf Accessed 30 September 2026.
13. The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013, S.I. 2013/3134, regulation 5, definition of "distance contract", and regulation 6(1) and (2), on which regulation 77(5) of the Payment Services Regulations 2017 defines an

"excepted contract". <https://www.legislation.gov.uk/ukxi/2013/3134/regulation/5> and <https://www.legislation.gov.uk/ukxi/2013/3134/regulation/6> Accessed 30 September and 1 October 2026.

14. Consumer Credit Act 1974, sections 75(1) and (3)(b) and 83(1). <https://www.legislation.gov.uk/ukpga/1974/39/section/75> and <https://www.legislation.gov.uk/ukpga/1974/39/section/83> Accessed 30 September and 1 October 2026.
15. Payment Systems Regulator, APP scams reimbursement requirement: consolidated policy statement, PS25/5, May 2025, paragraphs 1.3, 1.4, 2.5, 2.9, 3.2, 3.21, 3.31 to 3.33 and 3.36 to 3.37; the consumer standard of caution exception is at paragraphs 3.40 to 3.46. The statement is guidance: the definitive requirements are the regulator's legal instruments and the Faster Payments and CHAPS reimbursement rules (paragraphs 1.3 and 1.4). <https://www.psr.org.uk/media/rhelv4op/ps25-5-app-scams-reimbursement-consolidated-policy-statement-may-2025.pdf>; Pay.UK, FPS Reimbursement Rules, Schedule 4, version 4.0, 1 May 2026, rule 3.6 and section 10, definitions of "APP scam" and "Authorisation", <https://www.wearepay.uk/wp-content/uploads/2024/12/FPS-Reimbursement-Rules-Schedule-4.pdf>; Bank of England, CHAPS reimbursement rules, Annex A to the CHAPS Reference Manual, section 2, <https://www.bankofengland.co.uk/-/media/boe/files/payments/chaps/chaps-reimbursement--rules-annex-1.pdf>; and the Financial Services and Markets Act 2023, section 72(2) and (5), <https://www.legislation.gov.uk/ukpga/2023/29/section/72> Accessed 30 September and 1 October 2026.
16. Competition and Markets Authority, "Complying with consumer law when using AI agents", guidance, 9 March 2026. <https://www.gov.uk/government/publications/complying-with-consumer-law-when-using-ai-agents/complying-with-consumer-law-when-using-ai-agents> Accessed 30 September 2026.
17. Mastercard, "When AI starts buying for you, trust becomes the product", 5 March 2026: Verifiable Intent "creates a tamper-resistant record of what a user authorized when an AI agent acts on their behalf". <https://www.mastercard.com/us/en/news-and-trends/stories/2026/verifiable-intent.html> Accessed 30 September 2026.
18. EMVCo, "EMVCo Requests Feedback on Framework for Secure, Interoperable and Scalable Card-Based Agentic Payments", 1 September 2026: "Intent Services provide a shared, interoperable layer that enables payment participants to register, reference, retrieve and manage consumer-authorized intent", and EMVCo "may consider capabilities related to Know Your Agent (KYA) and Agentic Transaction Indicators to be included in future publications". <https://www.emvco.com/news/emvco-requests-feedback-on-framework-for-secure-interoperable-and-scalable-card-based-agentic-payments/> Accessed 30 September 2026.
19. Visa, "Visa Introduces Trusted Agent Protocol: An Ecosystem-Led Framework for AI Commerce", press release, 14 October 2025, <https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.21716.html>; and Mastercard at reference 9: "Every agent is credentialed, and with Verifiable Intent, can be recognized and transact with trust across ecosystems". Both accessed 30 September 2026.
20. H. Birkholz, D. Thaler, M. Richardson, N. Smith and W. Pan, "Remote Attestation procedureS (RATS) Architecture", RFC 9334, January 2023, <https://www.rfc-editor.org/rfc/rfc9334>; and the theme proposal "Remote Attestation for Agentic AI (RA-AAI)" in the ITU-T Focus Group on Trust and Identity for Humans and Agentic AI, <https://github.com/FG-TIDA/themes/issues/22> Both accessed 30 September 2026.
21. ITU-T Focus Group on Trust and Identity for Humans and Agentic AI (FG-TIDA), use-cases repository, to which the use case is to be submitted. <https://github.com/FG-TIDA/use-cases> Accessed 30 September 2026.
22. x402 Protocol Specification, version 2, which currently supports the "exact" scheme (section 1); in its core payment flow (section 2) the server "verifies the payment authorization and initiates blockchain settlement". <https://github.com/x402-foundation/x402/blob/main/specs/x402-specification-v2.md> Accessed 30 September 2026.
23. Financial Conduct Authority, Perimeter Guidance manual, PERG 15.3, Q25B. <https://handbook.fca.org.uk/handbook/perg15/perg15s3> Accessed 1 October 2026.