

The Agentic Commerce Opportunity and its Regulatory Compliance

Andrea De Matteis
EU Payments Regulation | Partner




Put the user first — because regulators will!

The use cases

- **Cardholder Initiated transactions (Agentic CIT)**
 - The Agent helps with research, comparison, and checkout
 - The cardholder is **in-session** and always **initiates** and **authenticate** the transaction
- **Agent Initiated Transactions (Autonomous AIT)**
 - The cardholder gives the Agent an **initial mandate/authorization** to initiate the transaction on their behalf
 - The Agent **autonomously** initiates the transaction when cardholder is **off-session**

AUTHENTICATION – AGENTIC CIT

Agentic CIT – Compliance with PSD2/PSR by design

- **SCA by default.** The cardholder is in session and always initiates and authenticates each transaction with SCA
- **What's new:** the cardholder initiates the transaction through the Agent's interface, rather than directly on the merchant's website
- **Compliance with PSD2/PSR is straightforward and by design** 
-  Fully compliant with **SCA requirements** (Article 97 PSD2 and Article 85 PSR)
-  Fully compliant with **dynamic linking** requirement (Article 5 RTS on SCA), as the Agent uses the **merchant(s) name** and **transaction amount** in authentication

AUTHENTICATION – AUTONOMOUS AIT

Autonomous AIT – General settings




- **SCA by default for initial mandate/authorization.** The cardholder is in session and authenticates with SCA the **initial mandate/authorization** given to the Agent
- The Agent then **autonomously** initiates the transaction when the cardholder is offline
- When is a **second SCA required?**
 - If any **parameter changes** at the time of the transaction vs. those authenticated upfront
 - Cardholder may pre-select to be brought back into session (e.g., via push notification) **by default** whenever the Agent autonomously initiates a transaction

A. 2nd SCA not required: merchant and maximum amount known

Assumption: merchant(s) and maximum amount identified upfront (“**known**”) at authentication

Example: buy product X from merchant Y if price falls below maximum amount Z

Compliance with PSD2/PSR is straightforward 






-  Compliant with **dynamic linking** requirement as the Agent uses **merchant name(s)** and maximum **transaction amount** in authentication
-  Compliant with the **pre-authorization** model (without blocking of funds) as per [Q&A 2020_5133](#)
-  If multiple merchants (e.g., buy from merchant Y1, Y2, or Y3), then dynamic linking must be **specific to each individual merchant** (as in the travel industry today)

B1. 2nd SCA not required: merchant unknown but exemption applies

Assumption: merchant(s) and maximum amount **unknown** at authentication

Example: buy flight to Rome with any airline


Compliance with PSD2/PSR through an existing exemption 

-  **Transaction Risk Analysis (TRA):** for low-risk transactions below the applicable thresholds and where the PSP's fraud rates remain within the regulatory limits
-  **Trusted beneficiary / whitelisting:** where the merchant has previously been whitelisted with SCA (and issuer is in control of whitelisting)
-  **Low-value remote:** for transactions below EUR 30 (and cumulative limits)
-  **Recurring transactions:** for transactions of a fixed amount to the same payee
-  **Secure Corporate Payments:** where the transaction is made through a dedicated corporate payment process and the payer is not a consumer

B2. Merchant unknown and no exemption applies

Assumption: merchant(s) and maximum amount **unknown** and **no exemption** applies

a. **Compliance with PSD2/PSR through second SCA** 

 **Push notification** to bring the cardholder back into session and authenticate with SCA, or

b. **Prospective compliance with PSD2/PSR through:**

i. **Analogy with MITs**

- **MITs were not expressly addressed in PSD2**

If merchant unknown and no exemption applies (continued)

- **EC clarified with [Q&A 2018 4031](#)** (question submitted by Mastercard) that MITs are excluded from SCA – provided the initial mandate is always authenticated with SCA
- May AITs be **excluded similarly to MITs**?

ii. Compliance through new exemption

- **New exemption specific for AIT** may be developed in Level 2 regulation under PSR (RTS on SCA)

For prospective regulatory solutions, AITs must be demonstrably **very secure**, industry **alignment** needed and regulatory **confirmation** to be received from EBA/EC

AUTHENTICATION – KEY TAKEAWAYS

Key takeaways

- ✓ Agentic CIT are **SCA compliant by design** ✓
- ✓ Autonomous AIT are **SCA compliant** as follows:
 - A. If merchant(s) and maximum amount are **known** ✓ no second SCA required
 - B. If merchant(s) and maximum amount are **unknown**
 - 1. and **existing exemption** applies ✓ no second SCA required
 - 2. if no exemption applies
 - a. SCA is applied again ✓ or
 - b. prospective regulatory solutions:
 - i. MIT analogy → no second SCA required, or
 - ii. new specific exemption → no second SCA required

LIABILITY FOR FRAUD

Liability for fraud

- The cardholder is generally refunded by the issuer

Compliance with PSD2/PSR is straightforward

- Existing **PSD2** and future **PSR** rules apply:
 - ✓ Cardholder **refunded** except for gross negligence and friendly fraud
 - ✓ If SCA is not applied, cardholder is refunded **even if grossly negligent**
- **Agent** may be made contractually **liable** to the issuer for behavior that facilitated fraud (e.g., Agent did not send an authentication request)

LIABILITY FOR MISTAKES

Liability for mistakes

- If there is a mistake, this is still an **authorized** transaction under PSD2/PSR
 - Thus, **PSD2/PSR refund** protection for unauthorized transactions **does not apply**
- ✓ However, other existing **consumer protection principles** apply:
 - **Merchant** is liable for errors in the fulfillment of the order (e.g., wrong items, wrong size, wrong color)
 - **Issuers** will likely clarify in their T&Cs that they are not liable for those errors
 - **Agents.** Questions remain as how to operationalize cardholders' rights for Agent's hallucinations and mistakes

Liability for mistakes

Consumer Rights Directive (CRD) gives consumers a ‘no question asked’ **14-day right to withdraw from online contracts**

- ✓ Consumer is entitled to a **full refund from the merchant** without incurring any costs (other than the costs of returning the goods)
- ✓ This CRD refund right applies, in principle, to **Agentic Commerce transactions**
 - Limited **exceptions** apply (e.g., customized or perishable goods)

TRANSPARENCY

Transparency

Unfair Commercial Practices Directive (UCPD) prohibits unfair practices in consumer contracts

- Agent providers must **not mislead consumers** in their purchasing decisions
- Commercial models based on **referral fees or other commercial arrangements** between Agent providers and merchants **are in principle allowed**
- However, consumers must be able to:
 - Easily distinguish **paid placements** from other results
 - Understand when **merchant's sponsorship** influences the selection, placement or ranking of the results displayed by the Agent

OPEN QUESTIONS

Open questions

1. **Redress.** How to “operationalize” consumer rights against cases not covered (e.g., extension of the chargeback mechanism)?
2. **Market concentration.** Will Agents prefer to contract with a few selected large merchants?
3. **Role allocation.** Who will be “intelligent” here, the Agent or the merchant?
 - Will the Agent be a simple pass-through of the cardholder’s intent to the merchant?
 - Will the Agent really know cardholder’s preferences, or will it defer this to the merchant?
4. **Steering.** Will the Agent make its decisions based on cardholder’s preferences, or based on its referral fees from merchants?
5. **Access and incentives for SMEs.** Which legal and policy levers to encourage Agents to contract with small and medium-sized merchants?

Thank you for your attention!

Andrea De Matteis

EU Payments Regulation | Partner



BRUSSELS / ROME

andrea@dematteis.law