The agentic customer

What happens when your customer sends you an agent?

> *"Your customer already delegates to AI agents, and an agent always asks. Blocking loses business, tolerating costs concessions nobody measures: the posture is set by journey, with data."*

WHAT IT IS

A customer with an agent of their own

A personal AI agent researches, buys, claims or contracts for the customer. It arrives by four paths: it researches you with an assistant, buys with an agent, asks for service and its agent talks to the company's. Its traffic looks like an attack, but it acts legitimately.

Implication: Does your company know how many of its customer contacts are already made by an agent?

Risk: Without a decision, each team blocks or tolerates on its own and nobody adds up the cost.

WHAT IT PROPOSES

A posture by journey

In sales, service, concessions and cancellations, the board sets whether to block, tolerate or serve the agent through an identified channel: identity of the agent and of whoever answers for it, revocable permissions, limits, a log and concession rules outside the model. It is required with direct exposure to customers.

Implication: Who is the business owner of the agent posture in each journey?

Risk: Without an identified channel, nobody can prove what the customer authorised their agent to do.

HOW IT IS CHECKED

Measured exposure and a tested channel

Economic exposure is calculated as a separate scenario, with the company's own data, and never adds to net value. Agent traffic is detected and tagged, and the concessions it resolves are measured. The channel is tested before, and always, with synthetic customers, user simulation and red teaming.

Implication: Has your company tested its service channel against agents trying to abuse it?

Risk: A channel that has not been tested is, in fact, tested on customers.

FOUR QUESTIONS FOR THE BOARD

1. **Which journeys already serve customer agents?**
   Agent traffic detected and tagged by journey, with its volume, cost and the concessions it resolves, kept apart from human traffic.
2. **What posture have we set in each journey?**
   A written posture by journey (block, tolerate or serve), with its business owner and a yearly review.
3. **What would it cost if everyone asked for what they are due?**
   An exposure scenario with the company's own data, reported apart from net value, with its date and assumptions; with no data of its own, it says "no data".
4. **What did we test before opening the channel?**
   Scenarios with synthetic customers by journey, findings with owner and date, and a sample of real contacts to check against.

WHAT FAILS IF IT IS NOT GOVERNED

WHAT FAILS	LEVEL	WHAT TO DO
Concessions paid that nobody measures	HIGH	Measure the concessions each agent resolves
Actions by a customer's agent that nobody can attribute	HIGH	Log every action with its permission
Net value inflated by not deducting extra concessions	HIGH	Report exposure as a separate scenario
Concession rules decided by the model	MEDIUM	Apply the rules outside the model
Agents blocked without knowing what business is lost	MEDIUM	Set the posture with data by journey
A channel opened without testing for abuse	MEDIUM	Test with synthetic customers before, and always

FURTHER READING

AI and agent security
Document 35 · third-party agents acting for the customer

Value measurement rules
Document 40 · economic exposure

AI thesis, ambition and appetite
Document 13 · posture towards customer agents

When Your Customer Sends an Agent
Bain & Company · 10-11-2026

Fernando García Varela · CC BY 4.0 · Version 0.x, under review

Generic help offered free of charge, with no legal review for any specific case: each organisation adapts it, identifies the regulation that applies to it and is responsible for its own compliance. It is neither advice nor certification. To the maximum extent permitted by law, the author accepts no liability for the effects of its application.