Your Next Customer is a Bot

A series on agentic commerce, customer contact and service changes needed when AI acts for customers.

The front door is now open! Now what?

An external agent can reach the same service through a website, an API, a company agent or an adviser. Organisations need to decide what it may do, what evidence each action requires and how those decisions are enforced on every route.

Author Martin Hill-Wilson

Publication October 2026 | Pre-reading for the LinkedIn Live

BRAINfood

neos wave

Follow for more content at: dualcx.com

An external agent may reach the same service through a website, an API, a company agent or an adviser. Organisations need to decide what it may do, what evidence is required for each action and how those decisions will be enforced.

A customer asks her personal agent to change the delivery address for an order. She is staying with her daughter while repairs are carried out at home. Consider how the retailer might handle the same request through three routes.

THE REQUEST **"Send my order to my daughter's address while the repairs are done."**

API

The agent can retrieve the order but cannot change the address.

- **Restricts the operation**

WEBSITE

Account sign-in is sufficient to submit the change.

- **Relies on account access**

TELEPHONE

An adviser can make the change but has no clear instruction about accepting a request from a personal agent.

- **Leaves the adviser to interpret**

This is a fictional example. It illustrates how one request can encounter three different sets of controls. The API restricts an operation, the website relies on account access, and the adviser must interpret a situation the procedure does not describe.

The retailer needs to decide whether the change is permitted, what evidence is required and which routes can complete it. Those decisions should remain connected when the request moves between channels.

The contact centre as an interface to company systems

Brainfood's previous article, The protocols entering customer service, examined the different roles of commerce, payment, agent access and service protocols. It also argued that organisations need a common internal policy governing what an external agent may discover, read, propose and complete.

That policy needs to describe individual service actions.

A contact centre already connects customer requests to company systems. An adviser retrieves records, changes bookings, arranges refunds and applies policies. A company agent (the AI system acting for the business) may perform some of the same work. Websites and APIs provide other routes to those records and actions.

An external customer agent can therefore seek a change without having direct access to the system that makes it. It may ask an adviser or company agent to act.

Service leaders should treat each accepted route as an interface through which an external agent can request information or initiate a change. Restricting the API achieves little if the same request can proceed through a website or adviser without equivalent checks.

What the protocols and platforms already do

The protocols explored in a previous article provide mechanisms for parts of this work. Sierra's description of the Personal Agent Protocol says companies set the parameters within which personal agents can operate, including the available interfaces and access arrangements. UCP allows businesses to declare commerce capabilities that agents can discover and use.

Some specifications remain in draft. Sierra published the draft Personal Agent Protocol, known as Poppy, on 9 October 2026. Organisations should check the version and capabilities their chosen supplier actually supports.

Platforms can also apply rules during an interaction. Decagon says its Personal Agent Gateway places permissions within Agent Operating Procedures. Businesses define permission scopes, which specify the operations an agent may access, and attach them to relevant sections of those procedures. The platform restricts access where the required permissions are missing. Its PACT description also explains how additional permission can be requested during a conversation.

> **These are vendor descriptions of intended capabilities.** They do not establish that every deployment enforces every relevant rule correctly.

A platform can discover available operations, check granted permissions and apply configured rules. The business still needs to decide which operations to offer and what conditions govern them. Both Sierra and Decagon explicitly assign those choices to participating companies.

THE ORGANISATION SHOULD ESTABLISH WHICH DECISIONS ITS PLATFORM

- Already implements.
- Requires configuration to implement.
- Leaves outside its control, for the business, its other systems or its advisers to handle.

Start with the service action

"Will we accept customer agents?" is too broad to settle most operational decisions.

An organisation might accept an agent's request for opening times without identifying the customer. Retrieving an order requires more evidence. Redirecting a delivery creates different consequences. Accepting compensation as full and final settlement raises another question again.

THE POLICY SHOULD DISTINGUISH BETWEEN REQUESTS TO

- Discover public information. — LOWEST CONSEQUENCE
- Retrieve information about a customer or account.
- Prepare or propose a change.
- Complete an action within the customer's delegated authority.
- Seek a decision that requires customer confirmation or employee judgement. — HIGHEST CONSEQUENCE

Even an apparently simple request needs a precise description. “Change delivery details” could mean three different things, and they need not carry the same conditions.

> Updating instructions for the driver.

> Selecting another delivery date.

> Redirecting goods to a different address.

A useful policy names the operation, the information it affects and the conditions under which it may proceed.

Four decisions for each action

The External Agent Action Matrix provides a structure for recording four connected decisions.



It does not require a separate spreadsheet if the organisation already holds these decisions in a suitable system. Its purpose is to make the rules explicit, identify omissions and compare how they are applied across service routes.

Each action also needs an accountable owner, a record of where its rules are enforced and evidence of how those controls have been tested.

A Admission

Who may use this route?

Which agents may use which routes for this task?

The organisation needs criteria for accepting an agent, rather than relying only on a list of recognised providers. It should decide how to handle declared agents, unrecognised agents and requests whose origin remains uncertain.

Acceptance can vary by route. A company might support account enquiries through a structured interface while directing consequential changes to another process. These choices must remain consistent with its legal duties and relevant customer support requirements.

Admitting the interaction does not authorise every request made during it.

P Permission

What may the agent do?

What may the agent retrieve, propose or complete?

Reading an order, proposing a new delivery address and making that change are separate permissions. A policy that records only "account access" leaves these distinctions unresolved.

The decision should identify the evidence required for the particular action. That includes the customer's instruction and any limits on what the agent may do: the mandate.

The organisation must also check whether the action is available under the applicable service rules. Customer authority does not make an unavailable delivery slot, expired return option or prohibited account change permissible.

In Detecting a personal AI agent is only the first test, I distinguished five things. The matrix turns those distinctions into requirements attached to named operations.

Agent identity | **Customer identity** | **Account access** | **Delegated authority** | **Entitlement**

I Intervention

Who must confirm or decide?

What requires customer confirmation, employee judgement or both?

Some decisions require the customer's approval rather than the agent's. The organisation must define which decisions require that approval, explain exactly what the customer is approving, and specify how their response will be obtained and recorded.

Employee judgement addresses matters such as conflicting evidence, policy exceptions or an outcome that cannot be determined by the routine rules.

An employee's involvement does not supply missing customer authority. Equally, a customer's approval does not resolve whether the company may make an exception or whether the requested outcome is available.

The matrix should identify the decision required and who has authority to make it. "Refer to a human" is incomplete if the receiving adviser has neither the evidence nor the decision rights needed.

A Alternative

What happens if it stops?

What happens when the request cannot proceed?

A refusal should distinguish between different problems, and each condition needs an appropriate next step.

Why the request cannot proceed	A possible next step
The action is prohibited.	An explanation that the requested action is unavailable.
The evidence is insufficient.	Customer confirmation, or an adviser review.
The mandate has expired.	Fresh instruction and confirmation from the customer.
The chosen channel cannot complete the necessary checks.	A supported agent interface, or a route that can complete them.

One completed example

The action matrix brings together the rules for individual service actions. The table below expands one entry to illustrate a retailer's policy for changing a delivery address. It is an example, not a recommended rule for every business.

Field	Example decision
Action	Change the delivery address for an existing order before dispatch.
Agent permission P	The agent may retrieve the order and propose a new address once its connection to the customer and permission to access the order have been verified.
Execution condition P	The change may proceed only if the order remains eligible and the required customer confirmation is recorded.
Customer confirmation I	The customer approves the specified order and new address through the retailer's signed-in account.
Employee judgement I	Refer conflicting ownership evidence or fraud concerns to the designated team.
Alternative A	If the order cannot be redirected, explain the available options and retain the request in the case record.

The retailer would also record the rule's owner, where it is implemented and the results of testing it. A table containing only "allowed", "not allowed" and "human review" would leave too much for systems and staff to interpret.

Turn the decisions into controls

Each decision in the matrix needs to be connected to the control that enforces it.

Decision	Control that enforces it
The agent may check an order but not change it.	The system gives it access only to the information and functions needed to view that order, and prevents it from changing the address, cancelling the order or taking other actions outside that permission.
The customer must confirm.	A workflow holds the proposed change until approval is recorded.
The case is disputed.	Routing to an employee with defined authority.

Some controls may already exist in the chosen platform. Others may require configuration, integration or changes to adviser procedures.

An organisation can begin this work using its existing systems and staff procedures, without adopting a new agent protocol. Protocols such as PACT and UCP can support parts of the implementation where participants need an agreed way to discover available functions, exchange permissions or coordinate actions.

Whatever the implementation, record separately whether each rule has been agreed, put into operation and tested. This distinguishes a documented decision from a control that has been shown to work.

Agreed	Implemented	Tested
THE DECISION	THE CONTROL	THE EVIDENCE
The rule is documented and has an owner.	Systems and procedures apply it.	It has been shown to work on each route.

Apply the decision across routes

For the delivery address policy above, testing should establish whether each service route enforces the required customer confirmation.

Route	What must hold before the address changes
API	The agent may view the order, but an address change is directed to the retailer's confirmation process.
Website	Confirmation is obtained before the change is made. Where an agent uses delegated access, the system also checks that its permissions cover the requested action.
Company agent	Access to the order is not enough. It establishes what permission and customer confirmation have been supplied, and what is still required.
Adviser	The same as the company agent, with a clear route to transfer the request if the call cannot obtain the evidence.

The organisation should define which checks are required for the action, then ensure every route authorised to complete it performs those checks. Routes may obtain the evidence in different ways. If a route cannot meet the requirements, it should transfer the request to one that can.

For example, if the API requires customer confirmation but an adviser can make the same change without it, establish whether there is an approved reason for the difference. If there is not, assign an owner to correct it.

Changing channels should not allow a request to bypass a required check.

Give the rules an owner

An action matrix requires decisions from several functions.

Operations
Defines the work and the exceptions advisers encounter.

Security and identity
Establishes how relevant claims can be verified.

Product and digital
Confirms what each interface can enforce.

Legal, compliance and data protection
Assess the duties relevant to the action.

A named service owner should be accountable for the rule and its consistent application across routes. They should also ensure advisers have a clear escalation route for cases the rule does not resolve.

The service owner may handle those cases or delegate them to an authorised manager or specialist. If an adviser cannot establish whether the customer's instruction permits the requested action, the designated decision maker

must determine what further evidence or customer confirmation is needed.

The service owner should also ensure that any change to the rule is reflected in every affected system and adviser procedure, including escalation guidance. Otherwise, the API might enforce the revised rule while the website or advisers continue to apply an older version.

Provide a clear next step

An earlier Muse article in the series argued that blocking an external agent without a controlled alternative can redirect demand into repeated attempts, other channels or complaints.

The action matrix should therefore specify what happens next for each reason a request cannot proceed.

If the agent has permission to investigate a bill but not accept a settlement, the company can continue the investigation while reserving the settlement decision for the customer. If a telephone interaction cannot provide sufficient evidence for an address change, the company can direct the request to a suitable confirmation route.

When the request moves to another route or decision maker, it should carry the evidence already accepted and a clear explanation of what remains unresolved. The customer should not have to reconstruct the case because the first route could not complete it.

Choose one action and test it

The action matrix brings together the decisions described in this brief: what an external agent may do, what evidence it must provide, when customer approval or employee judgement is required, and what happens when a request cannot proceed. Each decision then needs to be mapped to the controls that enforce it.

A FIRST EXERCISE

1. Start with one consequential action, such as redirecting an order, changing a booking or accepting a settlement.
2. Trace the same request through each relevant route: the API, website, company agent and adviser procedure.
3. Record whether each route allows the action, stops it, seeks customer approval or refers it to an authorised decision maker.
4. Check what the platform enforces, what another system or employee must do, and whether the requirements still hold when the request changes channel.
5. Keep agreed rules, implemented controls and tested outcomes distinct. Resolve any gaps before extending the exercise to other service actions.

For service leaders, this provides a way to bring policy decisions, platform capabilities and adviser procedures into agreement. Digital, security and governance teams can see where their controls need to connect, while advisers gain clearer instructions about when to act and when to escalate.

The customer should be able to use an authorised agent without losing control over decisions reserved for them, or having to rebuild the case when it moves between channels.

The purpose of the matrix is to make those conditions explicit and give the organisation a way to check that its service honours them.

GET READY FOR DUAL CX

Putting this into practice requires the people responsible for policy, systems and service delivery to agree the rules and examine evidence of how they operate. Brainfood and Neos Wave offer a facilitated review within a defined service area, bringing those owners together, challenging assumptions and tracing selected requests across the agreed routes.

An action matrix
For the selected service actions.

Findings
Where controls are missing or inconsistent.

An implementation brief
With named owners and checks for completion.

We also run LinkedIn Live discussions, podcasts and a resource centre to help educate, swap experiences and guide the redesign for how the new world of Dual CX works.

www.dualcx.com

Your Next Customer is a Bot
A series from Brainfood and Neos Wave. Follow for more content at dualcx.com
© 2026 Brainfood Consulting. All rights reserved.

BRAINfood neos wave