

RESEARCH PAPER

AI Customer Service

Customers should be able to ask what Seatpack is without being shown an operator scoreboard. That sounds obvious. It took explicit refusals to make it true.

THECRINERS LLC · 2026

Problem

If you give a language model the company's internal files, it will be "helpful." Helpful includes quoting collected cash, process ids, and dashboard ports. Customer support that can do that is a leak with a chat bubble.

Projection, not dump

Each company writes a customer-safe facts file: name, offer, price label, public URL, FAQs, whether checkout is live. The parent stores a projection. Support answers from that plus a short public knowledge file. Internal headers, cash, sqlite, and secrets needles are stripped. Refund, contract, and identity-change intents are denied before tool selection.

Delegated actions

Support may identify the product, quote public facts, and open a case. It may not refund, spend, publish, or modify jobs. Regenerating an artifact can be HOLD. The chat widget on thecriners.com talks to a named tunnel that terminates on loopback. The support process is not the owner portal.

Tests

Prompts that mention passwords, cash, or ports must not echo them. "Refund my order" must not call an order-status tool just because the word "order" appeared. Empty or missing projections must fail closed to a generic apology, not to an internal README.

Limitations

This is not a human. The banner says so. It cannot sign contracts. Until checkout is live, it should say checkout is not live rather than improvise a payment story.

HTML is canonical. A PDF companion is offered where generated. Experimental laboratory results are labeled as such. This is not a product-market-fit claim and not a certification.

[← All papers](#) · [PDF](#)

TheCriners LLC · Coshocton, Ohio

Money Hunter, Packet Press, Pullsheet, Hearthlabel, Seatpack, and Company OS are projects of TheCriners LLC — not separate legal entities.