

Your analysts are already using ChatGPT. Customer account data doesn't survive the paste.

Sovara Browser checks every draft message and file name against your firm's policy — **locally, before it's sent** — across ChatGPT, Claude, Gemini, Copilot and Perplexity. Customer text never leaves the machine to be checked, and connected deployments record each decision as metadata-only evidence.

75%¹

of UK financial services firms already use AI, with a further 10% planning to within three years — up from 58% in 2022.

22%²

of employee pastes into generative AI tools contain PII or payment-card data — and 82% of pastes come from unmanaged personal accounts.

\$5.6m³

average cost of a financial-sector data breach — second only to healthcare, and well above the \$4.4m global average.

+\$670k⁴

added to the average breach cost where "shadow AI" — staff using unapproved AI tools — is prevalent.

THE REGULATORY POSITION

The FCA has set no bespoke AI rulebook — it expects firms to manage AI within the **existing framework**: SM&CR accountability, the Consumer Duty, and operational-resilience and outsourcing rules. Customer financial data is personal data under UK GDPR, and cardholder data pasted into a public AI tool leaves your PCI DSS control environment. "We didn't know staff were using it" is not a defence — senior managers remain accountable.⁵

Three verdicts, shown at the moment of send

● **Block**

A hard stop. The message is held in the composer and never sent.

● **Warn**

A nudge to reconsider. The analyst can justify and proceed — both are recorded.

● **Redact**

Sensitive content is masked with labelled placeholders before it can be sent.

The Finance preset, ready on day one

- **Card numbers blocked outright** — Luhn-checked PANs never reach the prompt, keeping PCI DSS scope out of public AI.
- **Banking identifiers** — sort-code + account-number pairs and IBANs blocked; SWIFT/BIC and US routing numbers warned.
- **Identity numbers** — NI numbers and SSNs blocked; email and phone warned.
- **Business-hours access** — 07:00–19:00 UK, weekdays, with sensible daily and monthly quotas.
- **The full secrets suite** — JWTs, AWS/GitHub/Slack tokens and private keys blocked on every preset.

PRIVACY-FIRST

Evaluated locally

The policy runs inside the browser. Customer text is never transmitted for a check — only audit metadata syncs.

UNIFIED AUDIT

Defensible record

Every decision becomes a metadata-only audit event. Signed evidence exports support compliance reviews and incident investigations when signing is configured.

FILES TOO

File metadata flagged

File names and sizes are checked before upload. File contents are not inspected.

DEPLOYMENT

Managed rollout

Deploy via Intune, Group Policy, or Google Admin. Staff can't override firm configuration.

Covers the sites your people actually use

ChatGPT

Claude

Gemini

Copilot

Perplexity

All five verified blocking in a real browser. Site redesigns are fixed centrally by publishing new selectors, reducing recovery time without waiting for a new store release.

Plans

FREE

£0

/ single seat

TEAM

£7

/ user / mo,
annual

ENTERPRISE

£15+

/ user / mo

Sovara — people at Send, agents at the tool.

Start a team pilot.

Built by Weldon Web Ltd, UK ·
sovarahq.com/products/sovara-browser · Hosted in Azure UK
South

1. Bank of England & FCA, Artificial Intelligence in UK Financial Services 2024 (third survey, c. 120 firms) · 2. LayerX Enterprise AI & SaaS Data Security Report 2025 · 3 & 4. IBM Cost of a Data Breach Report 2025 · 5. FCA AI Update (Apr 2024); SM&CR; Consumer Duty; UK GDPR / DPA 2018; PCI DSS v4.0.