

Finance_Memory_Pack_v1_Global
“CRAFT – Financial Services Recon Pack”

Purpose

Enable the agent to guide sellers in:

- Banking (retail + commercial + central banks)
- Insurance (health/auto/cyber/property & casualty)
- Capital markets + exchanges
- Credit unions + mutual institutions
- Fintechs operating under national regulation

Designed for **any country**, automatically adapting terminology, regulators, and document sources.

Geo-Adaptive Targeting Logic

After the user selects **Finance** + Country...

The agent asks:

1. Which subsector?
 - A. Banking
 - B. Insurance
 - C. Capital Markets / Exchanges
 - D. Credit Union / Mutual
 - E. Fintech (regulated or unregulated)
2. Regulatory authority/oversight:
 - Who enforces compliance? (e.g., OCC/FDIC/Fed in U.S., FCA in UK, ESMA in EU)
 - Any cross-border regulations? (Basel III/IV, PSD2, GDPR, MAS, etc.)
3. System importance (scale & political impact):
 - Tier 1 national bank? Systemically Important Financial Institution (SIFI)?
 - Regional institutions serving critical populations?

- State-owned bank with government risk exposure?

Mission Signals — what moves action

Finance institutions care above all about:

- Risk mitigation → regulatory, operational, reputational
- Trust and continuity → uninterrupted consumer services
- Fraud & financial crime resilience
- Customer experience → speed + digital modernization
- Talent & infrastructure modernization under compliance scrutiny

Agent's narrative must tie security outcomes to:

“Preserve trust. Ensure uptime. Prevent regulatory exposure.”

Subsector Mission Differentiators

Banking

- Core banking stability = national economic strength
- Fraud, AML, identity, payment rails
- Cloud modernization friction vs. legacy core systems

Insurance

- Claims processing uptime
- Risk modeling + sensitive data protection
- Cyber underwriting shifts driving urgency

Capital Markets

- Fast execution + HFT race conditions
- SEC/ESMA compliance for trade monitoring
- Breach → immediate economic market impact

Credit Unions / Mutual

- Community trust + limited budgets
- Often lag on security modernization
- Ideal lighthouse accounts

Fintech

- Growth vs. compliance conflict
- Rapid innovation with third-party dependency
- OCC/other regulators increasing pressure globally

Funding & Oversight Signals

Agent should request:

- Annual financial reports + risk disclosures
- Regulator enforcement actions
- Public audit/oversight reports
- Technology or cyber transformation roadmaps
- Payment modernization initiatives
- Public tender documents (if procurement is formalized)
- Press releases around fraud incidents or outages
- Cyber insurance & underwriting data shifts

Examples by region:

United States

- OCC / Fed / FDIC guidance
- SOX compliance for public companies
- FFIEC cybersecurity assessments
- Payment rails modernizations (FedNow, RTP)

UK

- FCA enforcement and consultation papers
- PRA capital guidance
- Open Banking mandates

EU

- ESMA + ECB expectations
- PSD2 / NIS2 compliance
- Cross-border financial crime frameworks

APAC & Middle East

- National digital payment programs

- Sovereign investment fund dependencies
- Central bank cybersecurity advisories

Influence Centers

Altitude (Revenue + Risk)

- Chief Risk Officer
- CFO
- CIO + CISO
- Chief Compliance Officer (heavily influential)
- Chief Fraud Officer / Head of AML

Operator-level (execution friction)

- SOC + fraud investigation teams
- Core banking operations
- Payments operations
- Claims IT + underwriting security
- 3rd-party vendor risk managers

Hidden influence networks

- Regulators (pressure = urgency)
- Board risk committees
- Cyber insurance carriers
- Outsourced processors (FIS, Fiserv, Jack Henry, etc.)
- Cloud partners driving roadmap (Azure, GCP, AWS financial services)

Urgency Triggers — what forces a decision

Agent should elevate any institution experiencing:

- Fraud spike → customer restitution costs
- Regulatory action: fines, consent orders
- Payment or online banking outages → public backlash
- Data breach = trust loss, churn risk
- New compliance deadlines approaching
- M&A events → operational instability
- Cloud migrations under deadline pressure

Urgency = Flow: Window + Leverage + Nerve

Hiring + Workforce Scarcity

Agent checks for:

- Cyber + fraud investigation vacancies
- Tight labor competition with big tech + fintech
- High internal turnover → operational weakness
- Aging processor-skilled talent nearing retirement
- Over-reliance on third parties → compliance exposure

Interpretation:

Workforce fragility increases urgency to automate and reduce ops burden.

Partner & Procurement Dynamics

Ask the user:

- Which **core processors** are involved?
 - Fiserv, FIS, Jack Henry, Temenos, Tata, Infosys, etc.
- Who influences modernization decisions? (consultancies, SI partners)
- Cloud partner of record (if early cloud adoption)
- Cyber insurance carrier requirements
- Compliance frameworks selecting preferred vendors?

Partner alignment = leverage or blockade.

Agent Required Questions — Finance

After sector/region/subsector selection:

1. What regulatory framework applies?
2. What's the most recent enforcement or compliance pressure?
3. Any operational outages affecting customers?

4. Where is fraud or financial crime pressure rising?
5. Any modernization or cloud adoption initiatives underway?
6. Hiring pressure signals?
 - SOC, payments security, AML
7. Who controls purse strings + compliance approvals?
8. Procurement path = RFP? Panel? Direct award?

Document Upload Prompts

“To complete your CRAFT financial profile, please upload or paste any documents you have:

- Regulatory advisories / consent orders
- Annual risk and performance reports
- Cyber or fraud modernization strategy documents
- Processor or SI contract context
- Hiring/job postings tied to operational pressure
- Public news about incidents or fines”

Agent extracts signals into MAPS → WINDOW → FLOW.

FLOW Indicators — Finance

Fit

- Identity security, fraud prevention, SOC resilience
- Reduced operational burden
- Auditable risk reduction

Leverage

- Board-level visibility
- Regulator pressure aligning stakeholders
- Processor/cloud partner leverage

Outcome

- Protect trust + brand value
- Prevent fines + compliance cost exposure
- Improve customer experience + uptime

Window

- Regulatory deadlines
- Breach recency
- Payment modernization schedules
- Leadership turnover
- M&A or fintech competition acceleration

Example 90-Second Opener (Template)

“We help financial institutions reduce operational cyber and fraud risk in a way that strengthens compliance and protects customer trust. Based on recent regulatory advisories and the modernization challenges you’re facing with [system/process], your team is carrying a risk burden that is both expensive and highly visible to the board.

We can reduce that exposure while taking pressure off your overstretched operations and compliance staff — and show measurable benefit before the next audit cycle.”