

# APPENDIX G: SEMI-STRUCTURED IN-DEPTH INTERVIEWS WITH BANK EMPLOYEES

## Introduction (5 minutes)

- **Purpose:** This interview is part of a Master of Science research project at the University of Essex Online, conducted by Andrius Busilas, to design a secure finance chatbot using AI (large language models and secure data retrieval) to handle customer queries while preventing data leakage. Your insights will shape a user-centric, compliant system.
- **Context Briefing:** Large language models (LLMs) are AI systems that understand and generate human-like responses, like a smart librarian answering questions. Retrieval-Augmented Generation (RAG) ensures only authorised data is accessed, like a secure vault.
- **Ethics:** Participation is voluntary, and you may withdraw at any time. Responses are anonymised, audio-recorded with consent, and stored securely (AES-256 encryption) per GDPR and CCPA. Data is used solely for research. Contact: andrius.busilas@gmail.com.
- **Consent:** Verbal or written consent is required before proceeding.
- **Format:** This 45-minute semi-structured interview encourages open discussion. I'll ask follow-up questions to clarify your thoughts.

## Question Guide

The following 10 questions are organized into three sections, with role-specific probing to elicit insights from developers, customer-facing staff, and compliance officers. Probing ensures depth and addresses limited technical literacy.

## Section 1: Understanding User Needs and Financial Contexts (15 minutes)

**Goal:** Identify customer query types, financial contexts, and usability expectations.

1. **What types of customer queries and financial contexts do you encounter most often in your role, and which are most sensitive?**

- *Examples:* Balance enquiries, transaction disputes, loan applications; contexts like budgeting or fraud reporting.
  - *Probing:* How complex or sensitive are these queries? Which would you hesitate to trust a chatbot with? Why?
  - *Role-Specific:*
    - *Developers:* Which queries require secure data access (e.g., real-time account details)?
    - *Customer-Facing Staff:* Which queries frustrate customers most, and in what contexts (e.g., urgent fraud reports)?
    - *Compliance Officers:* Which queries involve regulated data (e.g., PII under GDPR)?
- 2. What features would make a finance chatbot most useful for you or your customers?**
- *Examples:* Fast responses (<1s), multilingual support, fraud alerts.
  - *Probing:* How do you balance speed vs. accuracy? Would customers value text, voice, or both?
  - *Role-Specific:*
    - *Developers:* What technical features (e.g., API integration, PII masking) are critical?
    - *Customer-Facing Staff:* What features would improve customer satisfaction (e.g., human escalation)?
    - *Compliance Officers:* What features ensure compliance with GDPR or EU AI Act (e.g., consent prompts)?

## **Section 2: Identifying Data Leakage Concerns (20 minutes)**

**Goal:** Elicit specific concerns about PII leakage and security risks in chatbot interactions.

- 3. What sensitive data do you handle that a chatbot might need to access, and how should it be protected?**
- *Examples:* National insurance numbers, transaction details, customer names.
  - *Probing:* How is this data currently protected? What risks (e.g., customer trust, legal issues) arise if exposed?
  - *Role-Specific:*

- *Developers*: What data types are most vulnerable in AI systems (e.g., unencrypted PII)?
  - *Customer-Facing Staff*: What data do customers expect to stay private?
  - *Compliance Officers*: What data falls under GDPR or EU AI Act regulations?
4. **What specific risks concern you most about a chatbot handling sensitive financial data?**
- *Examples*: Data leaks, prompt injection, incorrect responses exposing PII.
  - *Probing*: Can you share an example of a data security issue you've encountered? How would you detect a chatbot leak?
  - *Role-Specific*:
    - *Developers*: What technical vulnerabilities (e.g., prompt injection) concern you?
    - *Customer-Facing Staff*: What risks would erode customer trust?
    - *Compliance Officers*: What risks could lead to non-compliance (e.g., PII retention)?
5. **How would you define a 'data leakage' incident in a chatbot, and what would be its worst-case scenario?**
- *Examples*: Sharing account details with the wrong user, storing unencrypted PII.
  - *Probing*: How detectable should leakage be (e.g., via audit logs)? What impact would a leak have in your role?
  - *Role-Specific*:
    - *Developers*: What technical indicators (e.g., log anomalies) signal leakage?
    - *Customer-Facing Staff*: What leakage signs would customers notice?
    - *Compliance Officers*: What leakage scenarios violate GDPR or EU AI Act?

## **Section 3: Exploring Trust, Usability, Diversity, and Performance (15 minutes)**

**Goal:** Understand trust factors, usability expectations, diverse query handling, and performance under high demand for a user-centric chatbot.

**6. What would make you trust a chatbot to handle sensitive financial queries securely?**

- *Examples:* Security certifications, transparent responses (e.g., “Your data is encrypted”), human oversight.
- *Probing:* Would explaining data protection increase trust? What would undermine trust (e.g., vague responses)?
- *Role-Specific:*
  - *Developers:* What technical assurances (e.g., AES-256 encryption) build trust?
  - *Customer-Facing Staff:* What would reassure customers about security?
  - *Compliance Officers:* What compliance measures (e.g., anonymised logs) enhance trust?

**7. How should a chatbot handle diverse or ambiguous queries to ensure security and usability?**

- *Examples:* Multilingual queries, non-native speaker phrasing, ambiguous slang; responses like refusing to answer or requesting authentication.
- *Probing:* How should it respond to “Show my account details” without authentication? How should it handle cultural financial terms?
- *Role-Specific:*
  - *Developers:* What technical safeguards (e.g., RAG, NER) handle diverse queries?
  - *Customer-Facing Staff:* What responses maintain customer satisfaction for diverse users?
  - *Compliance Officers:* What handling ensures compliance for diverse queries?

**8. What concerns do you have about a chatbot providing biased or unfair responses (e.g., based on language, demographics), and how should these be addressed?**

- *Examples:* Different responses for non-native speakers, income-based biases.
- *Probing:* Have you observed biased interactions in customer services? What features (e.g., bias detection algorithms) could mitigate this?
- *Role-Specific:*
  - *Developers:* What technical approaches (e.g., Fairlearn, data debiasing) could reduce bias?

- *Customer-Facing Staff*: What biased responses might customers notice, and how would they react?
- *Compliance Officers*: What regulatory risks (e.g., EU AI Act) arise from biased responses?

**9. How should a finance chatbot maintain performance (e.g., <1s response time) when handling high volumes of queries (e.g., thousands daily)?**

- *Examples*: Handling peak periods like tax season, ensuring no crashes or leakage risks.
- *Probing*: What performance issues (e.g., slow responses, inaccurate answers) concern you most? How should the chatbot prioritize speed vs. security?
- *Role-Specific*:
  - *Developers*: What technical solutions (e.g., load balancing, caching) ensure scalability?
  - *Customer-Facing Staff*: How would performance issues (e.g., delays) affect customer trust?
  - *Compliance Officers*: What compliance risks arise from performance failures under high demand?

**10. Based on your experience, what improvements could a finance chatbot offer to enhance security, usability, or fairness?**

- *Examples*: Stronger authentication, bias mitigation, multilingual support.
- *Probing*: How should it address biases (e.g., language-based)? Do survey findings (e.g., concerns about multilingual queries, PII masking) align with your views?
- *Role-Specific*:
  - *Developers*: What technical improvements (e.g., prompt sanitisation) are feasible?
  - *Customer-Facing Staff*: What improvements would customers value?
  - *Compliance Officers*: What improvements align with GDPR/EU AI Act?

**Closing (5 minutes)**

- **Summary**: Recap key insights and their role in designing a secure chatbot.

- **Open Feedback:** “Is there anything else about chatbots, data security, or customer needs you’d like to share?”
- **Next Steps:** Explain how insights will inform the Define and Ideate stages. Offer to share anonymised findings if requested (via email: [andrius.busilas@gmail.com](mailto:andrius.busilas@gmail.com)).
- **Thank You:** Acknowledge your time and contribution.

## Implementation Guidelines

### 1. Interview Format:

- **Duration:** 45 minutes per employee (5-minute intro, 15/20/15 for sections, 5-minute closing) to balance depth and avoid fatigue.
- **Setting:** Virtual via Zoom with end-to-end encryption, or in-person if feasible, ensuring GDPR compliance.
- **Recording:** Audio-record with consent, transcribe using automated tools (e.g., Otter.ai), and anonymise responses (hash participant IDs with SHA-256).
- **Facilitation:** Use a semi-structured script (questions above, with flexibility to reorder based on responses). Start with a 2-minute context briefing using role-tailored analogies:
  - *Developers:* “LLM as a neural network processing language; RAG as a secure database query system.”
  - *Customer-Facing Staff:* “Chatbot as a virtual assistant; RAG as a locked customer file.”
  - *Compliance Officers:* “LLM as a smart clerk; RAG as a secure vault for regulated data.”
- **Probing:** Use neutral follow-ups (e.g., “Can you give an example?” “Why is that a concern?”) to clarify vague or biased responses, ensuring depth for non-technical participants.

### 2. Addressing Stakeholder Bias:

- **Context Briefing:** Tailor explanations to mitigate technical knowledge gaps (e.g., compliance officers may focus on regulation over AI mechanics).
- **Neutral Phrasing:** Avoid leading questions (e.g., “What risks concern you?” instead of “Are you worried about hacking?”).
- **Response Validation:** Cross-check responses with survey findings (e.g., Q10 probing survey themes like multilingual queries, PII masking) to reduce subjective bias.

### 3. Data Collection and Analysis:

- **Tools:** Use NVivo for thematic analysis (Braun and Clarke, 2023), coding themes like PII risks, trust factors, diverse query challenges, scalability, and bias. Achieve 85% inter-coder reliability with a second coder.

- **Outputs:** Anonymised transcripts, sensitive data list (e.g., national insurance numbers), stakeholder risk perceptions, and feature ideas for the Define stage (5.2.2).
- **Anonymisation:** Store data with AES-256 encryption; delete after analysis (Liang et al., 2023).

#### 4. **Ethical Considerations:**

- Obtain informed consent via verbal confirmation or signed forms, detailing data use, anonymisation, and withdrawal rights.
- Submit interview protocol to the University of Essex ethics board in Month 1, per the Methodology timeline.
- Ensure no PII is collected during interviews; use hashed IDs for tracking.