APPENDIX C: ONLINE QUESTIONNAIRE

Introduction

This questionnaire forms part of a Master of Science research project at the University of Essex Online, conducted by Andrius Busilas, exploring the integration of Design Thinking and large language models (LLMs) to mitigate data leakage risks in finance chatbots, ensuring secure and compliant user interactions. Your insights will inform the development of a user-centric, secure chatbot system for financial services.

The survey takes approximately 10–15 minutes to complete. Participation is voluntary, open to individuals aged 18+, and you may withdraw at any time without consequence. All responses are anonymised and handled in compliance with GDPR. Data will be accessed only by the researcher (Andrius Busilas; andrius.busilas@gmail.com) and used solely for statistical purposes in this study. You may opt into a follow-up interview by providing your email address, which will be stored separately to ensure anonymity.

For further information, please contact: andrius.busilas@gmail.com.

Consent Form

I agree to participate in a study conducted by Andrius Busilas, a student at the University of Essex Online, to investigate the integration of Design Thinking and LLMs for mitigating data leakage risks in finance chatbots.

I have read the information and consent to participate in this study (Required)

Instructions

- Answer all questions to the best of your knowledge.
- For Likert scale questions, select the option reflecting your view (1 = Not at all/Strongly Disagree, 5 = Extremely/Strongly Agree).
- For open-ended questions, provide concise responses (character limits noted).
- Role-specific follow-up questions will appear based on your role (Developer, Customer-Facing Staff, Compliance Officer).
- Submit responses via the online platform (e.g., Google Forms, SurveyMonkey).

Glossary

- **Sensitive Data**: Information such as account numbers, names, or transactions that must be protected.
- **Data Leakage**: Unintentional sharing or access of sensitive data (e.g., disclosing account details to the wrong user).
- **Chatbot**: An AI tool that responds to customer queries using natural language.
- **AI (LLM)**: A language model generating human-like responses.
- **Secure Data Retrieval (RAG)**: A system retrieving only authorised data, akin to a locked filing cabinet.

Section 1: About You

Purpose: Provide context for your responses.

1. **What is your role?** (Select one)
    - Developer
    - Customer-Facing Staff
    - Compliance Officer
    - Other (please specify, max 200 characters): _____

2. **How many years have you worked in the financial sector?** (Select one)
    - Less than 1 year
    - 1–2 years
    - 2–5 years
    - 5–10 years
    - Over 10 years

3. **What is your age range?** (Select one)
    - 18–25
    - 26–35

- 36–45
- 46–60
- Over 60

Section 2: Handling Sensitive Data

Purpose: Understand frequency and types of sensitive data handled, and associated risks.

4. **How often do you or your team handle sensitive customer data (e.g., account numbers, names, transaction details)?**
    - Never (1)
    - Rarely (2)
    - Occasionally (3)
    - Frequently (4)
    - Daily (5)

    If 3 or higher:

    4a. Which types of sensitive data do you handle most often? (Select all that apply)
    - Customer names
    - Account numbers
    - Transaction details
    - National insurance numbers
    - Addresses
    - Telephone numbers
    - Email addresses
    - Other (please specify, max 50 characters): _____

5. **How concerned are you about sensitive customer data being exposed through a finance chatbot?**
    - Not at all concerned (1)

- Slightly concerned (2)
- Moderately concerned (3)
- Very concerned (4)
- Extremely concerned (5)

  If 3 or higher:

  5a. What specific data exposure risks concern you most? (e.g., disclosing account details to wrong user, max 100 characters): _____

6. **Which customer queries pose the highest risk of sensitive data leakage if handled by a chatbot?** (Select up to 3)
   - Balance enquiries
   - Transaction history requests
   - Account updates
   - Loan applications
   - Fraud reports
   - Password resets
   - Other (please specify, max 50 characters): _____

   For each selection:

   6a. Why do these queries pose a high risk? (e.g., "Transaction history may reveal account numbers," max 100 characters): _____

Section 3: Data Leakage Risks

Purpose: Assess likelihood and impact of data leakage risks.

7. **How likely is it that a finance chatbot could unintentionally leak sensitive data (e.g., due to errors or hacking)?**
   - Very unlikely (1)
   - Unlikely (2)
   - Somewhat likely (3)

- Likely (4)
- Very likely (5)

If 3 or higher:

7a. What type of incident concerns you most? (Select one)

- Incorrect response exposing sensitive data
- Unauthorised data access
- Data retention after query
- Other (please specify, max 50 characters): _____

8. **What would be the most severe consequence of a chatbot data leakage incident?** (Rank 1–5, 1 = Most severe)
   - __ Loss of customer trust
   - __ Financial loss to customers
   - __ Regulatory fines
   - __ Reputational damage to organisation
   - __ Operational disruption

   Follow-up:

   8a. Describe a worst-case scenario for a data leak in your role. (max 100 characters): _____

9. **How important is it for a chatbot to have mechanisms to detect and prevent data leakage (e.g., masking account numbers)?**
   - Not important (1)
   - Slightly important (2)
   - Moderately important (3)
   - Very important (4)
   - Extremely important (5)

   Role-Specific:

- **Developers (9a)**: Which technical mechanisms are critical? (Select all that apply)
    - Data encryption
    - PII masking
    - Secure data retrieval
    - Audit logs
    - Prompt sanitisation
    - Other (please specify, max 50 characters): _____

- **Customer-Facing Staff (9b)**: Which features would reassure customers? (Select all that apply)
    - Clear security messages
    - Human escalation option
    - Authentication prompts
    - Other (please specify, max 50 characters): _____

- **Compliance Officers (9c)**: Which mechanisms ensure GDPR/EU AI Act compliance? (Select all that apply)
    - Data minimisation
    - Anonymised logs
    - Consent prompts
    - Other (please specify, max 50 characters): _____

10. **How concerned are you about a chatbot being manipulated to leak data through malicious inputs (e.g., tricking it with specific questions)?**
    - Not at all concerned (1)
    - Slightly concerned (2)
    - Moderately concerned (3)

- Very concerned (4)
- Extremely concerned (5)

If 3 or higher:

10a. What type of manipulation concerns you most? (Select one)

- Tricking the chatbot to reveal sensitive data
- Bypassing authentication
- Causing incorrect responses
- Other (please specify, max 50 characters): _____

Role-Specific:

- **Developers (10b)**: What technical safeguards would prevent this? (max 100 characters): _____
- **Customer-Facing Staff (10c)**: How would customers react to such an incident? (max 100 characters): _____
- **Compliance Officers (10b)**: What regulatory issues would arise? (max 100 characters): _____

Section 4: Trust, Usability, and Fairness

Purpose: Identify factors for trust, usability, and fairness in chatbot design.

12. **How much would you trust a finance chatbot to handle sensitive customer queries securely?**
    - Not at all (1)
    - Slightly (2)
    - Moderately (3)
    - Very much (4)
    - Completely (5)

    If 3 or lower:

11a. What would increase your trust? (e.g., certified security standards, max 100 characters): _____

13. **How important are these features for making a finance chatbot trustworthy and easy to use?**

    (Likert Scale for each, 1 = Not important, 5 = Extremely important)

    a) Fast response time (<1 second): [1] [2] [3] [4] [5]

    b) Clear and accurate responses: [1] [2] [3] [4] [5]

    c) Simple interface (e.g., text or voice): [1] [2] [3] [4] [5]

    d) Transparent security (e.g., "Your data is encrypted"): [1] [2] [3] [4] [5]

    e) Option to escalate to a human agent: [1] [2] [3] [4] [5]

    Follow-up:

    12a. Other features you'd prioritise for trust or usability? (max 100 characters): _____

14. **How should a chatbot respond to a sensitive or ambiguous query (e.g., "Show my account details" without authentication)?**

    - Refuse to respond
    - Request authentication
    - Redirect to human agent
    - Provide generic response
    - Other (please specify, max 50 characters): _____

    Role-Specific:

    - **Developers (13a)**: What technical approach would support this response? (max 100 characters): _____
    - **Customer-Facing Staff (13b)**: What response would maintain customer satisfaction? (max 100 characters): _____
    - **Compliance Officers (13c)**: What response ensures compliance? (max 100 characters): _____

15. **How important is it for a chatbot to handle diverse customer queries securely (e.g., multilingual, non-native speaker phrasing)?**
    - Not important (1)
    - Slightly important (2)
    - Moderately important (3)
    - Very important (4)
    - Extremely important (5)

    If 3 or higher:

    14a. What diverse query types should the chatbot prepare for? (Select all that apply)
    - Multilingual queries
    - Non-native speaker phrasing
    - Ambiguous slang
    - Culturally specific financial terms
    - Other (please specify, max 50 characters): _____

    Role-Specific:
    - **Developers (14b)**: What technical challenges would arise? (max 100 characters): _____
    - **Customer-Facing Staff (14c)**: What customer issues arise from diverse queries? (max 100 characters): _____
    - **Compliance Officers (14c)**: What compliance issues arise? (max 100 characters): _____

16. **How concerned are you about a chatbot providing biased or unfair responses (e.g., varying responses based on customer demographics)?**
    - Not at all concerned (1)
    - Somewhat concerned (2)

- Moderately concerned (3)
- Very concerned (4)
- Extremely concerned (5)

If 3 or higher:

15a. What type of bias concerns you most? (Select one)

- Language-based bias
- Gender-based bias
- Age-based bias
- Income-based bias
- Other (please specify, max 50 characters): _____

Role-Specific:

- **Developers (15b)**: What technical approaches could reduce bias? (max 100 characters): _____
- **Customer-Facing Staff (15c)**: Have you observed examples of bias in customer interactions? (max 100 characters): _____
- **Compliance Officers (15b)**: What regulatory risks arise from bias? (max 100 characters): _____

17. **How important is it for a chatbot to maintain performance (e.g., <1s response time) during high-demand periods (e.g., thousands of queries)?**
    - Not important (1)
    - Slightly important (2)
    - Moderately important (3)
    - Very important (4)
    - Extremely important (5)

    If 3 or higher:

16a. What performance issues concern you most during high demand? (Select one)

- Slow responses
- System crashes
- Increased leakage risk
- Inaccurate responses
- Other (please specify, max 50 characters): _____

Role-Specific:

- **Developers (16b)**: What technical solutions would ensure scalability? (max 100 characters): _____
- **Customer-Facing Staff (16c)**: How would performance issues affect customers? (max 100 characters): _____
- **Compliance Officers (16b)**: What compliance risks arise from performance failures? (max 100 characters): _____

Section 5: Final Thoughts

Purpose: Capture additional insights and preferences.

17. **Do you have additional concerns or suggestions about using a finance chatbot for customer queries?** (max 200 characters): _____
18. **Would you like a summary of anonymised findings from this research?**
    - Yes (provide email, stored separately): _____
    - No

Optional Follow-Up Interview

All responses are confidential and anonymised. If you are willing to participate in a short, follow-up interview, please provide your email address below (stored separately from survey data):

- Email: _____

Submission

Thank you for your valuable contribution! Your responses will help shape a secure and user-friendly finance chatbot. Please review your answers and click “Submit” to complete the survey.