System Proposal for ScamSafe: Enhancing Data Security

Name: Tang Joyce

Class: CSC3150 System Design

Professor Andy

Date: May 21rd 2024



### **Table of Contents**

**Executive Summary**

**1.0 Introduction and Overview**

* Problem Statement
* Project Vision and Scope
* Requirements Summary
* Stakeholders and Interests
* Expected Costs and Benefits
* Constraints
* Recommendation
* Document Overview

**2.0 System Initiation**

* System Request

**3.0 Feasibility Assessment**

* Introduction
* Feasibility Analysis
  + Technical Feasibility
  + Resource Feasibility
  + Schedule Feasibility
  + Organizational Feasibility
  + Legal and Contractual Feasibility
* Additional Comments
* Conclusion

**4.0 Requirements Definition**

* Introduction
* Functional Requirements
  + Must Have Requirements
  + Should Have Requirements
  + Could Have Requirements
  + Won't Have Requirements
* Data Requirements
* Non-functional Requirements

**5.0 Requirements Model**

* Introduction
* Use-Case Diagram
* Use-Case Descriptions

**6.0 System Evolution**

* Future Features and Enhancements
* Planned Upgrades

**7.0 Conclusions and Recommendations**

* Conclusions
* Recommendations

**Appendices**

* GDPR Compliance Checklist
* CCPA Compliance Checklist

**Glossary**

**Bibliography**

### **Executive Summary**

**Project Title**: System Proposal for ScamSafe: Enhancing Data Security

**Prepared by**: Joyce Tang

**Class**: CSC3150 System Design

**Professor**: Andy Cameron

**Date**: May 21, 2024

**Overview**: ScamSafe is a secure platform designed to protect personal information more effectively than standard note applications. With specialized legal compliance and fraud detection features, ScamSafe acts as a digital safe, ensuring data is securely stored, monitored, and protected against potential scams.

**Problem Statement**: In today's digital age, the security of personal information is critical, yet many commonly used applications lack robust security measures. This gap exposes consumers and financial institutions to increased risks of fraud and data breaches. ScamSafe aims to address these vulnerabilities by offering enhanced security solutions tailored to modern cyber threats.

**Project Vision and Scope**: ScamSafe aspires to revolutionize personal data security with a user-friendly interface, advanced security checks, and compliance with legal standards. The project will encompass real-time scam detection, data encryption, and fraud prevention tools, providing users with a reliable and secure platform for managing their personal information.

**Key Stakeholders and Interests**:

* **End Users**: Benefit from enhanced security and a simplified user experience for managing personal and financial information.
* **Financial Institutions**: Gain robust security measures to protect client data and ensure regulatory compliance.
* **IT and Legal Departments**: Focus on technical deployment, system support, and legal compliance to uphold data protection laws.

**Expected Costs and Benefits**:

* **Benefits**:
  + Enhanced Security: Reduces risks of data breaches and identity theft.
  + Increased Efficiency: Streamlines user interactions, reducing time and operational costs.
* **Costs**:
  + Development and Maintenance: Includes software design, testing, and ongoing updates.
  + Marketing and Customer Support: Necessary for promoting ScamSafe and ensuring user satisfaction.

**Constraints**:

* **Technical Constraints**: Dependence on continuous internet connectivity and advanced security technologies.

**Conclusion**: The ScamSafe project is feasible and well-supported, addressing critical needs in personal data security and fraud prevention. With a comprehensive approach and solid backing, ScamSafe is positioned to provide a secure, user-friendly platform that enhances trust in digital transactions.

1.0 Introduction and Overview

ScamSafe is a platform designed to secure your personal information more safely than storing it in a standard note app on your phone. It has specialized features to ensure your details are stored securely, checked against legal standards, and protected from fraud. It's like having a personal digital safe that keeps your information locked away and checks for potential scams or legal issues.

## Problem Statement

ScamSafe is tackling the urgent need for better personal information security at a time when digital transactions are everywhere. Consumers and financial institutions face significant risks because the security in many commonly used apps isn't strong enough. These weak spots open them to more fraud and data breaches, which can mess up personal and financial information and shake people’s trust in online shopping and banking.

As the digital transaction market booms, so do the kinds of clever cyber threats that old-school security can’t handle anymore. Banks, online shops, and everyday users are getting hit by cybercriminals who know how to exploit these systems' weaknesses. These attacks don't just mean lost money; they also chip away at customers' trust in these brands, potentially causing lasting damage.

ScamSafe is here to build a more robust security setup with real-time scam detection, top-notch data encryption, and easy-to-use fraud prevention tools. We’re here to do more than safeguard data; we want to rebuild and strengthen trust in the digital and financial world. By tackling the severe security gaps in current technologies, ScamSafe is ready to deliver the essential protection that evolves with the threats and covers users everywhere they go online.

## Project Vision and Scope

ScamSafe aims to revolutionize personal data security by providing a highly secure platform where users can confidently store and manage their personal information. The app will feature user-friendly interfaces, advanced security checks, and compliance with legal standards, ensuring user data is protected against potential scams and legal issues.

## Requirements Summary

**Must Haves**

* **User-Friendly Client Portal:** A secure and intuitive interface for users to manage their information.
* **Automatic Safety Checks:** Real-time scanning of user data against legal standards and fraud detection.

**Could Haves (Nice to Haves)**

* **Multilingual Support:** Accessibility in various languages to cater to a diverse user base.
* **Analytics Dashboard:** This monitors user interactions and improves system functions.
* **Won’t Haves (Don't Do's aka Out of Scope)**
* **Physical Mailing of Documents:** The system will be fully digital to enhance efficiency and security.
* **Offline Processing:** Requires constant internet connectivity to ensure real-time data accuracy.

## Stakeholders and Their Interests

**End Users:** Direct beneficiaries of the ScamSafe app, end users include individual consumers and small business operators who rely heavily on digital transactions. They stand to benefit from significantly enhanced data security measures and a more streamlined user experience that simplifies how they manage and protect their personal and financial information. These improvements safeguard their data and enhance their confidence in using digital platforms for their financial transactions.

**Financial Institutions:** As critical partners, financial institutions such as banks, credit unions, and fintech companies require robust security measures to protect client data against the increasing cyber-attack threat. These stakeholders are interested in integrating ScamSafe to safeguard their reputational integrity and comply with stringent regulatory requirements for data protection. Their collaboration is crucial in tailoring ScamSafe to meet industry-specific security standards.

**IT and Legal Departments:** These internal stakeholders are primarily concerned with the development, maintenance, and legal compliance of the ScamSafe app. The IT department focuses on the system's technical deployment and ongoing support, ensuring it remains resilient against new threats. Meanwhile, the legal department navigates the complex landscape of data protection laws to ensure that ScamSafe complies with GDPR, CCPA, and other relevant regulations, addressing any legal implications that may arise from the app's use.

## Expected Costs and Benefits

**Benefits**

**Enhanced Security:** By incorporating cutting-edge encryption and real-time monitoring algorithms, ScamSafe drastically reduces the risk of data breaches and identity theft, safeguarding user data from unauthorized access.

**Increased Efficiency:** ScamSafe streamlines user interactions and transaction processes, reducing the operational burden on users and decreasing the time and costs associated with managing security protocols manually. This efficiency can lead to increased user satisfaction and lower customer support calls.

**Costs**

**Development and Maintenance:** The initial development of ScamSafe is a significant expenditure that includes software design, testing, and deployment. Maintenance costs involve regular updates, security patches, and integrating new technologies to keep the app current and secure.

**Marketing and Customer Support:** Significant marketing efforts are required to promote ScamSafe effectively. This includes campaigns to educate potential users on the app's benefits and ongoing customer support to ensure users are satisfied and can use the app effectively.

## Constraints

**Technical Constraints**:

* The effectiveness of ScamSafe heavily relies on continuous internet connectivity to perform real-time data analyses and updates. This dependency means that any disruptions in internet service can compromise the app's functionality.
* Advanced security technologies are central to ScamSafe’s operations, requiring regular updates and adaptations to mitigate emerging cyber threats. This demands high-level expertise and can be resource-intensive.

**Operational Constraints**:

* Regular updates are essential to maintain optimal security measures and compliance with evolving regulations. This requires a proactive approach to software management, potentially increasing operational costs and complexity.
* Compliance with new regulations often necessitates quick adaptations, which can strain resources and require frequent system overhauls to ensure ongoing compliance.

Document Overview

This proposal outlines the initial plan for the ScamSafe app, detailing the problem statement, project scope, stakeholder interests, and anticipated costs and benefits. The subsequent sections will provide a more detailed feasibility analysis and definition of requirements.

2.0 System Initiation

Project Initiation Request (PIR)

**General Project Information**

|  |  |
| --- | --- |
| **Project Name:** | ScamSafe |
| **Two Sentence Request Description:** | *ScamSafe is a platform designed to secure your personal information more safely than storing it in a standard note app on your phone. It has specialized features to ensure your details are stored securely, checked against legal standards, and protected from fraud. It's like having a personal digital safe that keeps your information locked away and checks for potential scams or legal issues.* |
| **Requested Launch Date(s):** | *October, 15th 2024* |
| **Department(s) Affected By Project:** | *IT for development and maintenance, Customer Service for handling user inquiries and feedback, Marketing for promoting the app, and Legal for compliance checks.* |
| **Project's Customers:** | *Individual consumers are looking for additional security in their online and mobile transactions. The project also affects financial institutions seeking to provide added security solutions to their clients.* |
| **Date Request Submitted:** | April, 15th 2024 |

* 1. **Project Sponsor and Manager**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Project Sponsor** | |  | **Business Project Manager & Requestor** | |
| **Name:** | Andy Cameron |  | **Name:** | Joyce Tang |
| **Title:** | Professor |  | **Title:** | *Student* |
| **Department:** | Computer Science - SPU |  | **Department:** | *Computer Science - SPU* |
| **eMail:** | acameron@spu.edu |  | **eMail:** | *Tangj3@spu.edu* |

* 1. **Business Problem or Opportunity: The motivation for this reque**

*Describe the problem or opportunity that you would like to solve. Include a simple, high-level description of this request's business problems or opportunities. Focus on the problem or opportunity, not the solution. Be sure to include any date or deadline-related dependencies or needs related to the project.*

| *Our company currently faces a significant challenge with the client onboarding process, which is manual, time-consuming, and prone to errors.*  *This inefficiency delays the activation of services for new clients and affects our operational costs and client satisfaction levels. Our growing client base and the increased complexity of our services exacerbate the problem.* |
| --- |

* 1. **Justification, Impact, and Importance**

*What is the financial impact and justification for this request? How will the investment of time, resources, and capital be returned to our company? (Please note any contractual or regulatory requirements associated with the request. If you have an NPV, IRR, or ROI calculation, please provide the link(s) in this section.)*

**Assumptions**

|  |
| --- |
| * *Include at least two. Add more rows to each table as needed.* |
| * Client Growth Rate: We assume a 10% annual growth in new client acquisitions, increasing the demand for efficient onboarding. * Current Operational Costs: Based on current data, the manual onboarding process costs approximately $500 per client because of labor and time-intensive tasks. |

**Competitive Landscape / Context**

|  |
| --- |
| * *Include at least two.* |
| * Industry Standard: Competitors have implemented automated digital solutions, reducing their onboarding times by 30-50% and improving client satisfaction. * Regulatory Compliance: As regulatory requirements increase, automated compliance checks during client onboarding become a competitive and legal necessity to avoid penalties. |

**Tangible Return, Opportunity, or Value One Time On-Going**

|  |  |  |
| --- | --- | --- |
| * *Include at least two. Estimate the best you can.* | $ 0 | $ 0 |
| * Increased Revenue from Faster Onboarding.   Increased Revenue from Faster Onboarding: Shortening the onboarding process by 15 days increases revenue speed, potentially adding $100,000 annually.   * Reduced Onboarding Costs.   Automating data entry and compliance checks saves approximately $200 per client, translating to significant annual savings. | $ 0  $ 0 | $100,000 annually  $50,000 annually |

**Intangible Benefits Impact or Value**

|  |  |
| --- | --- |
| * *Include at least two.* | $ 0 |
| * Improved Client Satisfaction.   Faster, error-free onboarding processes lead to higher client satisfaction and retention rates.   * Enhanced Brand Reputation.   Being known for efficient and user-friendly processes enhances brand reputation, attracting more clients. | High  High |

* **Product Requirements**

*The Project team will gather detailed requirements once the project is approved. Use this section to articulate the critical solution components to help scope the project's size and complexity. Do not describe how the solution will be implemented; instead, only list the functionality or results you expect to receive when the product is complete/delivered.*

* 1. **Must Haves**

|  |
| --- |
| * + - *Include at least two. Add more rows to each table as needed.* |
| * + - **User-Friendly Client Portal:** A simple and secure online space where users can effortlessly upload necessary documents, view the status of their onboarding in a clear timeline and receive timely notifications about their service activation. This is like having a personal account on a website where you can see everything related to your service in one place.     - **Automatic Safety Checks:** The app will automatically check that all user information adheres to the latest legal standards, similar to an automatic checker that ensures all details are correct and within legal limits without needing manual review. Just like a spellchecker catches typos as you type, our app catches any issues with your details to keep you protected without having to do the extra work.   Ex. 1. Analyze the ID you upload to ensure it's valid and hasn't expired.  2. Cross-reference the details you provided with public records to ensure consistency and legality.  3. Alert you if there’s a mismatch or additional documentation is needed to comply with identity verification laws.  4. By monitoring your account for unusual patterns—for example, multiple sign-in attempts from different locations—ScamSafe can send you alerts if something seems out of the ordinary. |

* 1. **Could Haves** (Nice to Haves)

|  |
| --- |
| * + - *Include at least two.* |
| * + - **Multilingual Support:** To ensure everyone can use the app quickly, it will offer options in several languages, making it as accessible as ordering food online in your native language.     - **Analytics Dashboard:** A behind-the-scenes feature for our team to see statistics about how users interact with the onboarding process. This will help us identify any steps where users have difficulty and make those parts easier, like seeing which parts of a game most players get stuck on and improving those areas. |

* 1. **Won't Haves** (Don't Do's, aka Out of Scope)

|  |
| --- |
| * + - *Include at least two.* |
| * + - **Physical Mailing of Documents:** The system will operate entirely online to keep things fast and green. Users won’t be able to send in paper forms or documents - it’s like moving from postal mail to email.     - **Offline Processing:** All app parts require an internet connection, ensuring that user data is always current and processes remain quick. Like streaming – it’s all done over the internet to keep tunes fresh and accessible. |

3.0 Feasibility Assessment

Technical Feasibility: Moderate

ScamSafe leverages advanced encryption and real-time data analysis technologies. Technical evaluations confirm that current technological resources can support ScamSafe's needs. Future technology advancements will further enhance capabilities. Key challenges include secure integration of data sources and system scalability, managed through modular architecture and cloud solutions. Rating: Moderate - While capable, the need for ongoing adaptations poses potential risks.

Resource Feasibility: High

The project is supported by a team of experienced software developers, cybersecurity experts, and project managers. Funding for the initial phases is secure, with contingencies for unexpected costs. Resource expansion for deployment and maintenance will involve collaborating with external IT service providers. Rating: High - Adequate resources are in place, with solid plans for addressing future needs.

Schedule Feasibility: Moderate

ScamSafe's development timeline is planned for 18 months, aligning with strategic goals. Milestones include prototype development by month 6, beta testing by month 12, and full deployment by month 18. The main risk is potential delays from third-party integrations, mitigated by early engagement and parallel processing. Rating: Moderate - The schedule is feasible but subject to external dependencies.

Organizational Feasibility: High

ScamSafe is strategically aligned with the organization's goal to lead in digital security innovations. The organizational framework is robust, supported by top management, and underpinned by a dedicated project team and governance structure. Rating: High - Strong organizational support and readiness.

Legal and Contractual Feasibility: Moderate

Compliance with GDPR, CCPA, and other relevant regulations is fundamental to ScamSafe. All contractual obligations with vendors and service providers are aligned with project objectives. However, ongoing changes in privacy laws require continuous monitoring by the legal team, presenting a compliance risk. Rating: Moderate - Legally feasible but requires vigilant legal oversight.

Additional Comments

Conclusion

The feasibility assessment for the ScamSafe project indicates a high potential for success, supported by solid technical capabilities and organizational commitment. The detailed use case analysis has clarified key functionalities such as user registration, document upload and verification, fraud monitoring, and customer support. These functionalities address the critical need for enhanced data security and fraud prevention in digital transactions. The project's comprehensive approach ensures robust protection for users' personal information while maintaining compliance with legal standards.

4.0 Requirements Definition

Introduction

This section outlines the specific requirements for the ScamSafe project. It's divided into functional and non-functional requirements, providing a clear picture of what the system will do and the standards it must uphold. Functional requirements detail the actions the system must be able to perform, while non-functional requirements describe how the system performs these actions, focusing on usability, security, and performance.

Functional Requirements

### **Must Have Requirements:**

1. **User Registration and Authentication**
   * **Description**: Users must be able to register and log in securely using multi-factor authentication to ensure data security.
   * **Use Cases**: Register User (UC-01), Log In (UC-02)
2. **Manage User Profile**
   * **Description**: Users must be able to update, manage, and retrieve their profile information securely within the application.
   * **Use Cases**: Manage User Profile (UC-03)
3. **Upload Documents**
   * **Description**: Users must be able to upload necessary documents for verification and safety checks.
   * **Use Cases**: Upload Documents (UC-04)
4. **Perform Automatic Safety Checks**
   * **Description**: The system will automatically check uploaded documents against legal standards and potential scams.
   * **Use Cases**: Perform Automatic Safety Checks (UC-05)
5. **Monitor Transactions for Fraud**
   * **Description**: The system will analyze user transactions in real-time to identify and alert users of potential fraudulent activities.
   * **Use Cases**: Monitor Transactions for Fraud (UC-06)
6. **Receive Fraud Alerts**
   * **Description**: Users will receive real-time alerts for any suspicious activities detected.
   * **Use Cases**: Receive Fraud Alerts (UC-07)
7. **Update Legal Standards**
   * **Description**: Ensure the system is updated with the latest legal requirements and standards.
   * **Use Cases**: Update Legal Standards (UC-08)
8. **Generate Reports**
   * **Description**: Generate detailed reports on system usage, fraud detection, and compliance with legal standards.
   * **Use Cases**: Generate Reports (UC-09)
9. **Provide Customer Support**
   * **Description**: Provide support and assistance to users through various channels (e.g., live chat, email).
   * **Use Cases**: Provide Customer Support (UC-12)

### **Should Have Requirements:**

1. **Conduct Regular Security Updates**
   * **Description**: Regularly update the system to protect against new cyber threats and vulnerabilities.
   * **Use Cases**: Conduct Regular Security Updates (UC-10)
2. **Integrate with Financial Systems**
   * **Description**: Integrate ScamSafe with financial institutions' systems for seamless operation and data exchange.
   * **Use Cases**: Integrate with Financial Systems (UC-11)
3. **Promote the App**
   * **Description**: Involve marketing activities to promote ScamSafe to potential users through various channels.
   * **Use Cases**: Promote the App (UC-13)

### **Could Have Requirements:**

1. **Advanced Analytics Dashboard**
   * **Description**: Develop an advanced analytics dashboard for users to gain insights into their data security and transaction patterns.
   * **Use Cases**: Future implementation (System Evolution)
2. **AI for Enhanced Fraud Detection**
   * **Description**: Integrate AI and machine learning algorithms to improve fraud detection accuracy and speed.
   * **Use Cases**: Future implementation (System Evolution)

### **Won't Have Requirements:**

1. **Physical Mailing of Documents**
   * **Description**: The system will operate entirely online to enhance efficiency and security.
   * **Use Cases**: Out of scope
2. **Offline Processing**
   * **Description**: All app parts require an internet connection to ensure real-time data accuracy.
   * **Use Cases**: Out of scope

### **Data Requirements**

1. **User Registration and Authentication**:
   * **Description**: Users must be able to register and log in securely using multi-factor authentication.
   * **Data Needs**: Usernames, passwords, email addresses, authentication tokens.
2. **Fraud Detection**:
   * **Description**: The system will analyze user transactions in real-time to identify and alert users of potential fraudulent activities.
   * **Data Needs**: Transaction details, user behavior patterns, fraud detection logs.
3. **Data Encryption**:
   * **Description**: The system's user data will be encrypted using the latest encryption standards.
   * **Data Needs**: Encrypted user data, encryption keys, and secure transmission logs.
4. **User Profile Management**:
   * **Description**: Users must be able to update, manage, and retrieve their profile information securely within the application.
   * **Data Needs**: Personal information, contact details, profile updates.

### **Non-functional Requirements**

1. **Security**:
   * **Description**: The system must comply with international cybersecurity standards, including GDPR and CCPA compliance for data protection.
2. **Performance**:
   * **Description**: The system should handle up to 10,000 concurrent users without performance degradation.
3. **Usability**:
   * **Description**: The system interface should be user-friendly, with accessibility features supporting disabled users.
4. **Scalability**:
   * **Description**: The system architecture must support scaling to seamlessly accommodate increased user loads and data volume.

5.0 Requirements Model

### **Overview of ScamSafe Use Case Diagram**

This use case diagram shows how users interact with the ScamSafe system to secure personal information and detect fraud. It helps illustrate the system’s functionality and the relationships between its components.

### **Key Components:**

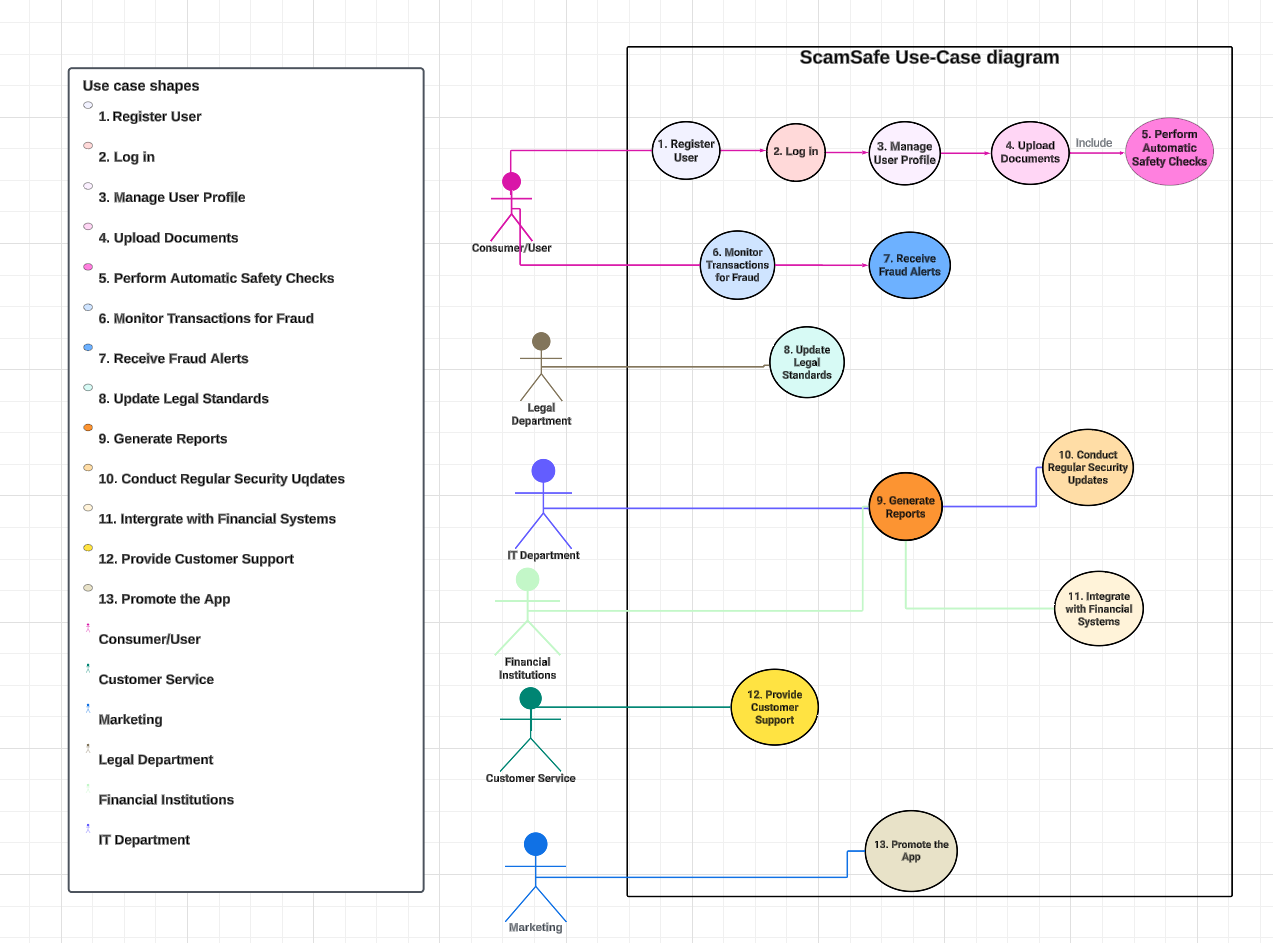
* **Actors**:
  + **Consumers/Users**: Use the app to secure information and monitor transactions.
  + **Legal Department**: Ensures compliance with legal standards.
  + **IT Department**: Manages security updates and system reports.
  + **Financial Institutions**: Integrate and generate reports.
  + **Customer Service**: Provides user support.
  + **Marketing**: Promotes the app.
* **Use Cases**:
  + **Register User**: Create an account.
  + **Log In**: Access accounts.
  + **Manage User Profile**: Update personal information.
  + **Upload Documents**: Upload documents for verification.
  + **Perform Automatic Safety Checks**: Verify documents against standards.
  + **Monitor Transactions for Fraud**: Detect fraudulent activities.
  + **Receive Fraud Alerts**: Get alerts for suspicious activities.
  + **Update Legal Standards**: Ensure regulatory compliance.
  + **Generate Reports**: Create usage and compliance reports.
  + **Conduct Regular Security Updates**: Maintain system security.
  + **Integrate with Financial Systems**: Ensure seamless operation.
  + **Provide Customer Support**: Assist users with issues.
  + **Promote the App**: Market to new users.

### **Understanding the Diagram:**

* **Direct Connections**: Lines show direct interactions between users and system functions.
* **Includes Relationships**: Some use cases include others, like "Upload Documents" includes "Perform Automatic Safety Checks."

This diagram helps all stakeholders understand how ScamSafe works and each actor's roles within the system.

Use-Case Diagram

Link: <https://lucid.app/lucidchart/c719a409-5e9d-493e-b89a-e4f3596a6f2f/edit?viewport_loc=-6182%2C-1214%2C11058%2C4896%2C0_0&invitationId=inv_801b5b1e-3198-48e0-b133-3a291f16ac4f>

Use-Case Descriptions

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case Name**: Register User | | **ID**: UC\_001 | **Importance**: High |
| **Primary Actor**: Consumer/User | **Use Case Type**: Primary | | |
| **Supporting Actors:** None | | | |
| **Stakeholders and Interests**:   * Consumers/Users: Want a secure and easy account creation. * ScamSafe: Needs to ensure the registration process is secure and user-friendly. | | | |
| **Brief Description**:  Allows new users to create an account with ScamSafe by providing personal information and setting up login credentials. | | | |
| **Trigger**: User decides to create a new account on the ScamSafe app.  **Type** (mark one): \_X\_\_ External \_\_\_ Temporal | | | |
| **Relationships**:  **Association**: Consumer/User  **Include**: None  **Extend**: None  **Generalization**: None | | | |
| **The Normal Flow of Events**:  User opens the ScamSafe app and selects "Register."  User enters personal information (name, email, password).  User completes multi-factor authentication.  System validates the information and creates the account.  User receives a confirmation email. | | | |
| **Sub-flows**:  None | | | |
| **Alternate/Exceptional Flows**:  If the email is already registered, the system prompts the user to log in or reset the password. | | | |
| **Special Requirements:**  The system must securely store user credentials and personal information. | | | |
| **To do/Issues:**  **None** | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case Name**: Log In | | **ID**: UC\_002 | **Importance**: High |
| **Primary Actor**: Consumer/User | **Use Case Type**: Primary | | |
| **Supporting Actors:**None | | | |
| **Stakeholders and Interests**:  Consumers/Users: Want a secure and quick way to access their accounts.  ScamSafe: Needs to ensure the login process is secure and efficient. | | | |
| **Brief Description**:  Allows users to log into their ScamSafe account using their credentials. | | | |
| **Trigger**: User decides to access their account on the ScamSafe app.  **Type** (mark one): \_X\_\_ External \_\_\_ Temporal | | | |
| **Relationships**:  **Association**: Consumer/User  **Include**: None  **Extend**: None  **Generalization**: None | | | |
| **The Normal Flow of Events**:  User opens the ScamSafe app and selects "Log In."  User enters email and password.  User completes multi-factor authentication.  System verifies the credentials.  User is granted access to their account. | | | |
| **Sub-flows**:  None | | | |
| **Alternate/Exceptional Flows**:  If the credentials are incorrect, the system prompts the user to try again or reset the password. | | | |
| **Special Requirements:**  **The system must handle multiple failed login attempts securely.** | | | |
| **To do/Issues:**  **Ensure the authentication process is robust and user-friendly.** | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case Name**: Manager User Profile | | **ID**: UC\_003 | **Importance**: Medium |
| **Primary Actor**: Consumer/User | **Use Case Type**: Primary | | |
| **Supporting Actors:**  None | | | |
| **Stakeholders and Interests**:  Consumers/Users: Want to easily update and manage their personal information.  ScamSafe: Needs to ensure profile management is secure and accurate. | | | |
| **Brief Description**:  Allows users to update and manage their personal profile information within the ScamSafe app. | | | |
| **Trigger**: User decides to update their profile information.  **Type** (mark one): \_X\_\_ External \_\_\_ Temporal | | | |
| **Relationships**:  **Association**: Consumer/User  **Include**: Upload Document  **Extend**: None  **Generalization**:None | | | |
| **The Normal Flow of Events**:  User logs into the ScamSafe app.  User navigates to the "Profile" section.  User updates personal information (e.g., address, phone number).  User saves the changes.  System validates and updates the profile information. | | | |
| **Sub-flows**:  None | | | |
| **Alternate/Exceptional Flows**:  If the information is invalid, the system prompts the user to correct the errors. | | | |
| **Special Requirements:**  The system must validate and securely store updated information. | | | |
| **To do/Issues:**  Ensure real-time validation and user feedback during profile updates. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case Name**: Upload Document | | **ID**: UC\_004 | **Importance**: High |
| **Primary Actor**: Consumer/User | **Use Case Type**: Primary | | |
| **Supporting Actors:** None | | | |
| **Stakeholders and Interests**:  Consumers/Users: Want a secure and easy way to upload documents.  ScamSafe: Needs to ensure document uploads are secure and verified. | | | |
| **Brief Description**:  Allows users to upload necessary documents for verification and safety checks. | | | |
| **Trigger**: User decides to upload a document for verification.  **Type** (mark one): X\_\_\_ External \_\_\_ Temporal | | | |
| **Relationships**:  **Association**: Consumer/User  **Include**: Perform Automatic Safety Checks  **Extend**: None  **Generalization**: None | | | |
| **The Normal Flow of Events**:  User logs into the ScamSafe app.  User navigates to the "Documents" section.  User selects "Upload" and chooses the document type.  User captures or selects the document from their device.  User confirms the upload.  System performs automatic safety checks on the document. | | | |
| **Sub-flows**:  None | | | |
| **Alternate/Exceptional Flows**:  If the document is invalid, the system prompts the user to upload a valid document. | | | |
| **Special Requirements:**  The system must support various document types and formats. | | | |
| **To do/Issues:**  Ensure the document upload process is secure and user-friendly. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case Name**: Perform Automatic Safety Checks | | **ID**: UC\_005 | **Importance**: High |
| **Primary Actor**: Consumer/User | **Use Case Type**: Included | | |
| **Supporting Actors:**  None | | | |
| **Stakeholders and Interests**:  Consumers/Users: Want assurance that their documents are safe and compliant.  ScamSafe: Needs to ensure the accuracy and security of uploaded documents. | | | |
| **Brief Description**:  The system automatically checks uploaded documents against legal standards and potential scams. | | | |
| **Trigger**: A document is uploaded by the user.  **Type** (mark one): \_X\_\_ External \_\_\_ Temporal | | | |
| **Relationships**:  **Association**: None  **Include**: None  **Extend**: Upload Documents  **Generalization**: None | | | |
| **The Normal Flow of Events**:  User uploads a document.  System automatically initiates safety checks.  System verifies the document against legal standards and potential scams.  System provides feedback to the user on the document's status. | | | |
| **Sub-flows**:  None | | | |
| **Alternate/Exceptional Flows**:  If the document fails the safety check, the system notifies the user and suggests corrective actions. | | | |
| **Special Requirements:**  The system must have up-to-date information on legal standards and scam detection algorithms. | | | |
| **To do/Issues:**  Ensure continuous updates and improvements to safety check algorithms. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case Name**: Monitor Transactions for Fraud | | **ID**: UC\_006 | **Importance**: High |
| **Primary Actor**: Concumer/User | **Use Case Type**: Primary | | |
| **Supporting Actors:**  None | | | |
| **Stakeholders and Interests**:  Consumers/Users: Want to ensure their transactions are secure and free from fraudulent activities.  ScamSafe: Needs to provide real-time monitoring to protect users from fraud. | | | |
| **Brief Description**:  Allows the system to continuously monitor user transactions for suspicious activities and potential fraud. | | | |
| **Trigger**: User initiates a transaction or system detects transaction activity.  **Type** (mark one): X\_\_\_ External \_\_\_ Temporal | | | |
| **Relationships**:  **Association**: Consumer/User  **Include**: Receive Fraud Alerts  **Extend**: None  **Generalization**: None | | | |
| **The Normal Flow of Events**:  User performs a transaction.  System monitors the transaction in real-time.  System analyzes transaction patterns for signs of fraud.  If suspicious activity is detected, the system generates an alert.  User receives a fraud alert and takes appropriate action. | | | |
| **Sub-flows**:  None | | | |
| **Alternate/Exceptional Flows**:  If no suspicious activity is detected, the transaction proceeds without any alerts. | | | |
| **Special Requirements:**  The system must use advanced algorithms for real-time fraud detection. | | | |
| **To do/Issues:**  Ensure continuous improvement of fraud detection algorithms. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case Name**: Receive Fraud Alerts | | **ID**: UC\_007 | **Importance**: High |
| **Primary Actor**: Consumer/User | **Use Case Type**: Primary | | |
| **Supporting Actors:** None | | | |
| **Stakeholders and Interests**:   * Consumers/Users: Want to be notified immediately of any suspicious activities. * ScamSafe: Needs to ensure timely and accurate fraud alerts. | | | |
| **Brief Description**:  Alerts users in real-time of any suspicious activities detected in their transactions. | | | |
| **Trigger**: Suspicious activity is detected during a transaction.  **Type** (mark one): X\_\_\_ External \_\_\_ Temporal | | | |
| **Relationships**:  **Association**: Consumer/User  **Include**: None  **Extend**: Monitor Transactions for Fraud  **Generalization**: None | | | |
| **The Normal Flow of Events**:   1. System detects suspicious activity in a transaction. 2. System generates a fraud alert. 3. User receives a fraud alert via their chosen method (e.g., push notification, email). 4. User reviews the alert and takes appropriate action (e.g., confirms or disputes the transaction). | | | |
| **Sub-flows**:  None | | | |
| **Alternate/Exceptional Flows**:  If the user does not respond to the alert, the system may take further protective actions (e.g., temporarily freeze the account). | | | |
| **Special Requirements:**  The system must support multiple alert methods and ensure immediate delivery. | | | |
| **To do/Issues:**  Ensure reliable and timely delivery of fraud alerts. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case Name**: Update Legal Standards | | **ID**: UC\_008 | **Importance**: Medium |
| **Primary Actor**: Legal Department | **Use Case Type**: Primary | | |
| **Supporting Actors:**  IT Department | | | |
| **Stakeholders and Interests**:   * Legal Department: Ensures the system complies with the latest regulations. * ScamSafe: Needs to maintain compliance with legal standards to protect users and avoid penalties. | | | |
| **Brief Description**:  Ensures the system is updated with the latest legal requirements and standards. | | | |
| **Trigger**: New legal regulations or standards are introduced.  **Type** (mark one): X\_ External \_\_\_ Temporal | | | |
| **Relationships**:  **Association**: Legal Department  **Include**: None  **Extend**: None  **Generalization**: None | | | |
| **The Normal Flow of Events**:   1. Legal department identifies new legal requirements. 2. Legal department updates the system with the new standards. 3. IT department implements the updates. 4. System ensures compliance with the new standards. | | | |
| **Sub-flows**:  None | | | |
| **Alternate/Exceptional Flows**:  If the updates fail, the IT department troubleshoots and resolves issues. | | | |
| **Special Requirements:**  The system must allow for quick and easy updates to legal standards. | | | |
| **To do/Issues:**  Ensure timely updates to comply with changing legal requirements. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case Name**: Generate Reports | | **ID**: UC\_009 | **Importance**: Medium |
| **Primary Actor**: Financial Instittutions, IT Department | **Use Case Type**: Primary | | |
| **Supporting Actors:**  None | | | |
| **Stakeholders and Interests**:   * Financial Institutions: Need detailed reports on system usage and fraud detection. * IT Department: Uses reports to monitor system performance and compliance. | | | |
| **Brief Description**:  Generates detailed reports on system usage, fraud detection, and compliance with legal standards. | | | |
| **Trigger**: Scheduled reporting period or ad-hoc request from stakeholders.  **Type** (mark one): \_X\_\_ External \_\_\_ Temporal | | | |
| **Relationships**:  **Association**: Financial Institutions, IT Deparment  **Include**: None  **Extend**: None  **Generalization**: None | | | |
| **The Normal Flow of Events**:   1. User requests a report or a scheduled report is due. 2. System gathers relevant data. 3. System generates the report. 4. System delivers the report to the requesting party. | | | |
| **Sub-flows**:  None | | | |
| **Alternate/Exceptional Flows**:  If the report generation fails, the system logs the error and notifies the IT department. | | | |
| **Special Requirements:**  Reports must be accurate, timely, and comply with relevant standards. | | | |
| **To do/Issues:**  Ensure data integrity and reliability in reporting. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case Name**: Conduct Regular Security Updates | | **ID**: UC\_010 | **Importance**: High |
| **Primary Actor**: IT Department | **Use Case Type**: Primary | | |
| **Supporting Actors:**  None | | | |
| **Stakeholders and Interests**:   * IT Department: Ensures the system remains secure against emerging threats. * Consumers/Users: Expect their data to be protected by up-to-date security measures. | | | |
| **Brief Description**:  Regularly updates the system to protect against new cyber threats and vulnerabilities. | | | |
| **Trigger**: Scheduled maintenance or discovery of a new threat.  **Type** (mark one): X\_\_ External \_\_\_ Temporal | | | |
| **Relationships**:  **Association**: IT Deparment  **Include**: None  **Extend**: None  **Generalization**: None | | | |
| **The Normal Flow of Events**:   1. IT department schedules a security update. 2. IT department develops and tests the update. 3. IT department deploys the update to the system. 4. System confirms the update is successful. | | | |
| **Sub-flows**:  None | | | |
| **Alternate/Exceptional Flows**:  If the update fails, the system rolls back to the previous version and IT investigates. | | | |
| **Special Requirements:**  Updates must be seamless and not disrupt user experience. | | | |
| **To do/Issues:**  Ensure timely and effective deployment of security updates. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case Name**: Integrate with Financial Systems | | **ID**: UC\_011 | **Importance**: High |
| **Primary Actor**: Financial Institutions, IT Department | **Use Case Type**: Primary | | |
| **Supporting Actors:**  None | | | |
| **Stakeholders and Interests**:   * Financial Institutions: Need seamless integration for smooth operation. * IT Department: Responsible for ensuring secure and efficient integration. | | | |
| **Brief Description**:  Integrates ScamSafe with financial institutions' systems for seamless operation and data exchange. | | | |
| **Trigger**: New integration request or system update.  **Type** (mark one): \_X\_\_ External \_\_\_ Temporal | | | |
| **Relationships**:  **Association**: Financial Institutions, IT Department  **Include**: None  **Extend**: None  **Generalization**: None | | | |
| **The Normal Flow of Events**:   1. IT department and financial institution plan the integration. 2. IT department develops integration interfaces. 3. IT department tests the integration. 4. IT department deploys the integration. 5. System confirms successful integration. | | | |
| **Sub-flows**:  None | | | |
| **Alternate/Exceptional Flows**:  If integration issues occur, IT department troubleshoots and resolves them. | | | |
| **Special Requirements:**  Integration must be secure and comply with relevant standards. | | | |
| **To do/Issues:**  Ensure ongoing support and updates for integration. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case Name**: Provide Customer Support | | **ID**: UC\_012 | **Importance**: Medium |
| **Primary Actor**: Customer Service | **Use Case Type**: Primary | | |
| **Supporting Actors:**  None | | | |
| **Stakeholders and Interests**:  Consumers/Users: Need reliable support for issues and inquiries.  Customer Service: Ensures user satisfaction and resolves problems promptly. | | | |
| **Brief Description**:  Provides support and assistance to users through various channels (e.g., live chat, email). | | | |
| **Trigger**: User initiates a support request.  **Type** (mark one): X \_ External \_\_\_ Temporal | | | |
| **Relationships**:  **Association**: Customer Service  **Include**: None  **Extend**: None  **Generalization**: None | | | |
| **The Normal Flow of Events**:   1. User logs into the ScamSafe app and navigates to the "Support" section. 2. User selects the preferred support channel (e.g., live chat, email). 3. User submits a support request detailing the issue or inquiry. 4. Customer service representative receives and reviews the request. 5. Customer service representative assists and resolves the issue. 6. System logs the support interaction for future reference. | | | |
| **Sub-flows**:  None | | | |
| **Alternate/Exceptional Flows**:  If the issue cannot be resolved immediately, the customer service representative escalates the request to the appropriate department. | | | |
| **Special Requirements:**  The system must ensure secure communication between users and customer service representatives. | | | |
| **To do/Issues:**  None | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Use Case Name**: Promote the App | | **ID**: UC\_013 | **Importance**: Medium |
| **Primary Actor**: Marketing | **Use Case Type**: Primary | | |
| **Supporting Actors:** None | | | |
| **Stakeholders and Interests**:   * **Marketing**: Aims to attract new users and increase app adoption. * **ScamSafe**: Seeks to expand its user base and market presence. | | | |
| **Brief Description**:  Involves marketing activities to promote ScamSafe to potential users through various channels. | | | |
| **Trigger**: Marketing campaign initiation or promotional event.  **Type** (mark one): X\_\_\_ External \_\_\_ Temporal | | | |
| **Relationships**:  **Association**: Marketing  **Include**: None  **Extend**: None  **Generalization**: None | | | |
| **The Normal Flow of Events**:  Marketing team plans a promotional campaign.  Marketing team creates promotional materials (e.g., ads, social media posts).  Marketing team launches the campaign through selected channels (e.g., online ads, social media).  Marketing team monitors the campaign’s performance.  Marketing team analyzes user engagement and feedback.  System logs new user registrations resulting from the campaign. | | | |
| **Sub-flows**:  None | | | |
| **Alternate/Exceptional Flows**:  If the campaign is not performing as expected, the marketing team adjusts the strategy and materials. | | | |
| **Special Requirements:**  The system must track the effectiveness of marketing campaigns and new user registrations. | | | |
| **To do/Issues:**  None | | | |

6.0 System Evolution

**Future Features and Enhancements:**

1. **Advanced Analytics Dashboard**:
   * **Description**: Develop an advanced analytics dashboard for users to gain insights into their data security and transaction patterns.
   * **Benefit**: Provides users with detailed reports and visualizations to better understand their data security status.
2. **Artificial Intelligence (AI) for Enhanced Fraud Detection**:
   * **Description**: Integrate AI and machine learning algorithms to improve fraud detection accuracy and speed.
   * **Benefit**: Enhances the system's ability to detect sophisticated fraud patterns and reduce false positives.
3. **Multi-Language Support**:
   * **Description**: Expand the app’s language options to include more languages beyond the initial offering.
   * **Benefit**: Makes the app accessible to a broader, more diverse user base.

**Planned Upgrades:**

1. **Continuous Security Updates**:
   * **Description**: Implement a continuous update cycle for security patches and system improvements.
   * **Benefit**: Keeps the system secure and up-to-date with the latest cybersecurity measures.
2. **User Experience (UX) Improvements**:
   * **Description**: Regularly update the user interface and experience based on user feedback and technological advancements.
   * **Benefit**: Enhances user satisfaction and engagement with the app

7.0 Conclusions and Recommendations.

**Conclusions:** The feasibility study and requirements analysis indicate that the ScamSafe project is well-positioned for success. The system will address critical needs in personal data security, fraud detection, and legal compliance. The development of ScamSafe will significantly enhance user confidence in digital transactions and provide robust protection against cyber threats.

**Recommendations:**

1. **Focus on User-Centric Design**:
   * Ensure that the app’s development prioritizes user experience and ease of use to maximize user adoption and satisfaction.
2. **Invest in Security and Compliance**:
   * Continually invest in the latest security technologies and compliance measures to stay ahead of emerging threats and regulatory requirements.
3. **Plan for Future Enhancements**:
   * Develop a roadmap for future features and system enhancements to keep ScamSafe competitive and responsive to user needs.
4. **Engage with Stakeholders**:
   * Maintain regular communication with all stakeholders, including users, financial institutions, and regulatory bodies, to gather feedback and ensure the app meets their needs.

By following these recommendations, ScamSafe can achieve its goal of providing a secure, user-friendly platform that protects personal information and fosters trust in digital transactions.

# **Appendices**

### **A.1 GDPR Compliance Checklist**

**Purpose of Data Collection**

* **Legal Basis for Collection:** Document the lawful basis for data processing (e.g., consent, contract necessity, legal obligation).
* **Data Minimization:** Ensure that only the minimal necessary data for the intended purpose is collected.

**Data Subject Rights**

* **Right to Access:** Procedures in place for users to request and receive a copy of their data.
* **Right to Erasure:** This process allows users to request the deletion of their data and ensure compliance with the request.

**Data Protection Measures**

* **Encryption:** All personal data is encrypted during transit and at rest.
* **Anonymization:** Techniques used to anonymize collected data where applicable.
* **Regular Audits:** Schedule and methodologies for regular data protection audits.

**Data Breach Notification**

* **Breach Detection Systems:** Description of systems in place to detect data breaches.
* **Notification Procedure:** Steps to notify authorities and affected individuals within 72 hours of a breach discovery.

### **A.2 CCPA Compliance Checklist**

**Consumer Rights**

* **Right to Know:** Consumers can know what personal data is collected, used, and shared.
* **Right to Opt-Out:** Mechanism for consumers to opt out of selling their personal data.
* **Right to Deletion:** Procedures for consumers to request deletion of their personal data.

**Data Handling and Privacy Policy**

* **Transparency:** Ensure that privacy policies include detailed information about data handling practices.
* **Training:** Mandatory training programs for employees handling personal information.

**Service Provider Agreements**

* **Vendor Compliance:** Ensure contracts with service providers include obligations that comply with CCPA regulations.

**Accountability and Governance**

* **Privacy Officer:** Appoint a Privacy Officer responsible for data protection strategies and compliance.
* **Impact Assessments:** Conduct regular privacy impact assessments to evaluate the risks associated with data processing activities.

# **Glossary**

* **API (Application Programming Interface):** A set of routines, protocols, and tools for building software applications. APIs specify how software components should interact and are used when programming graphical user interface (GUI) components.
* **Compliance Certifications:** Documents or credentials that verify the software meets all legal and regulatory requirements applicable to its function and use, ensuring adherence to standards such as GDPR or HIPAA.
* **Data Encryption:** Converting information or data into a code to prevent unauthorized access. This security measure protects sensitive data by making it unreadable without the proper decryption key.
* **GDPR (General Data Protection Regulation):** A regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.
* **Non-functional Requirements:** Requirements that describe how a system operates rather than the specific behaviors of that system. This includes aspects such as system performance, security, and user accessibility.
* **Prototype:** An early sample, model, or release of a product built to test a concept or process. In software development, a prototype is used to evaluate a new design to enhance precision by system analysts and users.
* **Scalability:** The capability of a system, network, or process to handle a growing amount of work or its potential to be enlarged to accommodate that growth. For software systems, this refers to the ability to handle increased loads on the system by making hardware or software adjustments.
* **Stakeholders:** Individuals, groups, or organizations interested in a project's success or failure. Stakeholders for ScamSafe include users, developers, investors, and regulatory bodies.

# **Bibliography**

System Proposal Part1+Part2 - One Page OUTLINE v9.pdf

CSC 3150 Lecture Feasibility and Risk, Nonfunction Requirements Triggers, Requirement, What we are seeking. Use Case Description Template - ANNOTATED.docx