

**Progressive Education Society's**

**MODERN COLLEGE OF ARTS, SCIENCE AND COMMERCE(Autonomous)**

**GANESHKHIND, PUNE-16**

**A PROJECT REPORT ON**

# **“Fraud Complaint and Guidance System”**

For ACADEMIC YEAR 2024-2025

TY BBA(CA) SEMESTER-VI

### SUBMITTED BY:

**Name: Sujal Jawalkar Roll No:243731028**

**Name: Khushdil Gupta Roll No: 243731022**

### Guided by:

### **Prof. Suwarna Mhasekar**

**CERTIFICATE**



This is to certify that **Sujal Gajanan Jawalkar** and **Khushdil Ramesh Gupta** of Class **TYBBA**(**CA**) Semester **VI** has satisfactorily completed Project Entitled “**Fraud Complaint and Guidance System**” as prescribed by Modern College of Arts, Science and Commerce (Autonomous)Ganeshkhind, Pune 16 affiliated to Savitribai Phule Pune University for the academic year **2024-2025.**

**Project Guide BBA-CA Coordinator**

**Internal Examiner External Examination**

**ACKNOWLEDGEMENT**

I want to express my sincere gratitude Dr. Sanjay Kharat principal and Dr. Shubhangi Joshi vice principal commerce faculty of Modern College of Art, Science & Commerce, Ganeshkhind, Pune-16 for providing me the opportunity to do my project on” Fraud Complaint and Guidance System”. I want to sincerely thank my project guide Prof. Suwarna Mhasekar for guiding and encouraging us throughout the project work. Special thanks to all the lab systems for seemingly small but valuable helps in terms of timely Internet and lab access.

|  |  |  |
| --- | --- | --- |
| **Sr.no.** | **Contents** | **Page No.** |
| **1** | **Abstract** |  |
| **2** | **Introduction:**   * Motivation * Problem Statement * Purpose/objective and goals * Literature survey * Project scope and limitations |  |
| **3** | **System Analysis:**   * Existing systems * Scope and limitations of existing systems * Project perspective, features * Stakeholders |  |
| **4** | **Requirement Analysis:**   * Function requirement * Performance requirement * Security Requirement |  |
| **5** | **Design System:**   * Design constraint’s * System Model * Data Model * User Interface |  |
| **6** | **Implementation details:**   * Software/ Hardware specifications |  |
| **7** | **Output and Report Testing**   * Test Plan * Manual Testing * Automation Testing * Function Validation |  |
| **8** | **Conclusion and Recommendations** |  |
| **9** | **Future Scope** |  |
| **10** | **Bibliography and References** |  |

**ABSTRACT**

The Fraud Complaint Guidelines System is an innovative digital platform designed to assist users in fraud prevention, reporting fraudulent activities, and seeking guidance on necessary actions after encountering fraud. This system enables users to report fraudulent websites, phone numbers, and other suspicious activities, ensuring that authorities are informed and can take appropriate action.

The primary goal of this application is to enhance public awareness regarding fraud prevention while providing a streamlined process for victims to file complaints online. Additionally, the system includes a dedicated portal for police officers, allowing them to review, approve, or reject complaints, ensuring a structured and efficient complaint-handling process. By offering a user-friendly interface and real-time notifications, the Fraud Complaint Guidelines System aims to bridge the gap between victims and law enforcement, ultimately contributing to a safer digital and financial ecosystem.

**INTRODUCTION**

* **Motivation:**

In today's digital age, fraud and cybercrime are increasing at an alarming rate, with many individuals falling victim due to a lack of awareness and proper guidance. Unfortunately, most victims do not know the appropriate steps to take after encountering fraud, making it difficult for them to seek justice or prevent further harm.

By providing a centralized “Fraud Complaint Guidelines System”, we aim to bridge this knowledge gap and offer a streamlined approach to fraud prevention and reporting. Many individuals hesitate to report fraud due to complex complaint procedures or lack of trust in the system. Our platform simplifies this process, ensuring that users can easily report fraudulent activities and access step-by-step guidance on how to respond.

Additionally, law enforcement agencies often face challenges in efficiently handling fraud-related complaints. Our system enables police officers to manage and verify complaints in an organized manner, allowing for quicker responses and better tracking of fraud cases. By making fraud prevention and reporting more accessible, we strive to empower individuals and contribute to a safer digital and financial environment.

* **Problem Statement:**

Fraud and cybercrime have become widespread issues, affecting individuals across various sectors, from financial scams to identity theft. A major challenge is that many victims are unaware of the necessary steps to take after encountering fraud, leading to financial loss and emotional distress. Additionally, there is no centralized platform that provides clear guidance on fraud prevention and reporting mechanisms. Despite existing complaint channels, many victims find the process of reporting fraud unmanageable, time-consuming, and ineffective. The lack of transparency and coordination between victims and law enforcement agencies further complicates the resolution process. To address these issues, we propose the development of a “Fraud Complaint Guidelines System,” a web-based platform that educates users on fraud prevention, provides step-by-step guidance on post-fraud actions, and allows users to report fraudulent websites and phone numbers. The system will also feature a dedicated interface for police officers, enabling them to review, approve, or reject complaints efficiently. By streamlining the reporting and complaint-handling process, this system aims to enhance fraud awareness, empower victims, and strengthen law enforcement responses.

**How can we ensure that reporting fraud actually leads to meaningful action and support for victims?**

* **Purpose/Objective and Goals:**

Fraud and cybercrime have become widespread issues, affecting individuals across various sectors, from financial scams to identity theft. A major challenge is that many victims are unaware of the necessary steps to take after encountering fraud, leading to financial loss and emotional distress. Additionally, there is no centralized platform that provides clear guidance on fraud prevention and reporting mechanisms.

Despite existing complaint channels, many victims find the process of reporting fraud cumbersome, time-consuming, and ineffective. The lack of transparency and coordination between victims and law enforcement agencies further complicates the resolution process.

To address these issues, we propose the development of a “Fraud Complaint Guidelines System”, a web-based platform that educates users on fraud prevention, provides step-by-step guidance on post-fraud actions, and allows users to report fraudulent websites and phone numbers. The system will also feature a dedicated interface for police officers, enabling them to review, approve, or reject complaints efficiently. By streamlining the reporting and complaint-handling process, this system aims to enhance fraud awareness, empower victims, and strengthen law enforcement responses.

* **Literature Survey:**

1. **Title:** **Cybercrime in the Context of the Digital Age: Analysis of Threats, Legal Challenges, and Strategies (2024)**

**AUTHORS:** Tetiana Batrachenko, Iryna Lehan, Vitalii Kuchmenko, Volodymyr Kovalchuk, Olha Mazurenko

**INTRODUCTION:**

In this research paper, the authors are pointing out that in this digital era, where the rapid advancements of technology have led to new vulnerabilities. They identify cybercrime as a multifaceted issue that impacts privacy, global security, personal data, and every country’s economy. Because of this, the authors underscore that cybercrime is difficult to combat because of its borderless nature. Researchers also point out that there is no global legal framework to fight cybercrime because of the rapid evolution of cybercriminal tactics. Additionally, the paper emphasizes the societal impact of data breaches, financial losses, and threats to critical infrastructure.

**Methodology:**

* **Data Collection:** The researchers studied cybersecurity reports, statistical crime data, and international policy documents from government and private organizations. They gathered data from incident reports, white papers, and cybersecurity studies to provide a comprehensive overview of cyber threats and their impact.
* **Analysis Approach:**

The study focused on comparing existing legal frameworks and their implementation in different regions, particularly the European Union and North America. They identified gaps in cybercrime laws and explored the role of public-private partnerships in combating cyber threats. Statistical methods were used to quantify the effectiveness of current strategies.

The researchers used tools like Microsoft Excel and SPSS for statistical analysis. Comparative frameworks were developed to assess the alignment between national and international cybercrime laws

**Conclusion:**

The study concludes that mitigating cybercrime requires global cooperation, encompassing education, technological advancement, and cohesive legal frameworks. It also highlights the importance of aligning national cybersecurity policies with international standards to ensure collective security. The role of public awareness campaigns in reducing vulnerabilities is emphasized.

**Future scope:**

The authors advocate for incorporating AI and machine learning into cybersecurity frameworks to predict and counter emerging threats. They also suggest developing adaptive legal frameworks capable of responding to the dynamic nature of cybercrime.

1. **Title:** **DSmishSMS-A System to Detect Smishing SMS (2023)**

**AUTHORS:** Sandhya Mishra, Devpriya Soni

**INTRODUCTION:**

Smishing, or SMS phishing, is a form of cyberattack where scammers send fraudulent text messages to trick people into revealing sensitive information, such as passwords, credit card details, or personal data. These messages often appear to originate from trusted sources, such as banks, government agencies, or well-known companies, making them difficult to identify as fraudulent. The danger lies in how easily victims can fall prey to these schemes, especially when the messages urge immediate action, such as clicking on a link or providing login details.

Detecting smishing is challenging because the messages are typically very short, providing little text to analyse for suspicious patterns. Furthermore, scammers constantly evolve their tactics to make their messages appear more legitimate, enabling them to bypass simple detection methods. This paper highlights the importance of combining two key strategies for improved detection: analysing the message content for signs of fraud and verifying any included links to ensure they do not lead to malicious websites. This combined approach significantly improves the chances of identifying smishing attempts and protecting users from potential harm.

**Methodology:**

* **Data Collection:**

Researchers compiled a dataset of 5,858 SMS messages, including both legitimate and fraudulent (smishing) examples. These messages were gathered from public repositories such as Kaggle and user-reported databases. Additional data was sourced from telecom providers and cybersecurity platforms to ensure a diverse dataset.

* **Model Development:**

Machine learning algorithms, including Logistic Regression, Decision Trees, and Support Vector Machines (SVM), were applied to detect patterns in the SMS text. The models analysed features like URL patterns, text structure, and the presence of phishing keywords to classify messages as either safe or smishing.

* **Testing and Evaluation:**

The system was tested using real-world SMS examples to measure its performance. Metrics such as accuracy, precision, recall, and F1-score were calculated to evaluate the system's ability to identify smishing messages effectively. The system achieved an accuracy rate of 97.93%, outperforming traditional detection methods

**Conclusion:**

The two-phase system effectively detects smishing attacks, reducing false positives and improving scalability. By combining URL reputation checks with linguistic analysis, the system provides a robust defence against SMS phishing. The authors emphasize the system’s potential to protect users in real-time scenarios.

**Future scope:**

Future work includes expanding the system’s capabilities to detect multilingual phishing attacks, integrating phone number blacklists, and enhancing detection with deep learning models. The authors also propose adapting the system for cross-platform phishing detection, including email and social media platforms**.**

1. **Title:** **Fraud Detection with Natural Language Processing (2024)**

**AUTHORS:** Petros Boulieris, John Pavlopoulos, Alexandros Xenos, Vasilis Vassalos

**INTRODUCTION:**

This paper introduces Fraud NLP, a novel dataset designed to facilitate fraud detection in online banking. Leveraging the concept of user behaviour as a sequence of actions analogous to sentences in a language, this approach applies Natural Language Processing (NLP) techniques to identify suspicious activities. A key focus of Fraud NLP is preserving user privacy by analysing behavioural patterns without relying on sensitive personal data.

**Methodology:**

* **Data Collection:** Researchers gathered datasets containing fraudulent and legitimate text data from online platforms**.**
* **Tool Use:** They used Natural Language Processing techniques to analyse patterns in textual content, such as keywords or phrasing, that indicate fraud.
* **Evaluation:** The system was tested by running it on unseen data to measure its success in detecting fraud.

**Conclusion:**

The findings confirm the effectiveness of NLP-based approaches for fraud detection, providing high precision and recall rates. The proposed system respects user privacy by analysing abstract behaviour patterns rather than sensitive data. The study highlights the potential of NLP in revolutionizing fraud detection methodologies

.

**Future scope:**

Future developments include extending FraudNLP to real-time detection scenarios and incorporating multi-modal data (e.g., device fingerprints and geolocation). The authors also propose refining the system to adapt to evolving fraud tactics.

1. **Title:** **An Intelligent Cybersecurity Phishing Detection System Using Deep Learning Techniques (2022)**

**AUTHORS:** Ala Mughaid, Shadi AlZu’bi, Adnan Hnaif, Salah Taamneh, Asma Alnajjar, Esraa Abu Elsoud

**INTRODUCTION:**

This paper investigates the problem of phishing attacks, where malicious actors manipulate individuals into disclosing sensitive information, including passwords and financial details, by masquerading as legitimate sources. Current phishing detection techniques exhibit shortcomings, particularly in identifying advanced phishing campaigns. 1 To address this challenge, this paper explores the application of deep learning, a form of artificial intelligence, to achieve more accurate and efficient detection.

**Methodology:**

* **Data Collection:** A dataset of phishing and non-phishing emails or websites was compiled.
* **Deep Learning Models:** The team used advanced neural networks to train the model to recognize phishing attempts.
* **Validation:** They validated the system's effectiveness using statistical tests, comparing it to traditional detection systems

**Conclusion:**

The intelligent phishing detection system demonstrates superior performance compared to traditional approaches. Its ability to generalize across diverse phishing techniques makes it a valuable tool for cybersecurity. The study highlights the importance of continuous dataset updates to maintain effectiveness.

**Future scope:**

Future work includes integrating the system into email platforms for real-time detection and extending its capabilities to other channels, such as SMS and social media. The authors also propose exploring federated learning for collaborative model training across organizations.

1. **Title:**  **Cybersecurity Threats, Vulnerabilities, and Security Solutions Models in Banking (2022)**

**AUTHORS:** Diptiben Ghelani, Tan Kian Hua, Surendra Kumar Reddy Koduru

**INTRODUCTION:**

This paper explores the cybersecurity challenges faced by the banking sector, emphasizing the increasing risks posed by digital transformation. The authors identify key vulnerabilities, such as malware, ransomware, and insider threats, and discuss the need for comprehensive security frameworks to protect sensitive financial data

**Methodology:**

* **Data Sources:** The research team collected data from banking incident reports, threat assessments, and customer surveys.
* **Case Studies:** Real-life cases of banking fraud were analysed to identify vulnerabilities.
* **Solution Testing:** The researchers proposed security frameworks and tested their feasibility using simulations and expert feedback**.**

**Conclusion:**

The study underscores the importance of adopting a holistic approach to banking cybersecurity, balancing technological innovation with regulatory enforcement. The proposed framework provides a comprehensive solution to mitigate current and future threats.

**Future scope:**

Future research will focus on integrating AI-driven anomaly detection systems and enhancing encryption methods to address emerging challenges. The authors also propose exploring cloud-based solutions for secure data storage and real-time fraud prevention.

**Combine summary of the 5 Research Paper**

Cybercrime has become one of the biggest challenges in the digital age, evolving alongside technological advancements. It affects individuals, businesses, and governments, causing financial losses, data breaches, and eroding trust in online systems. Despite existing legal frameworks, there are significant gaps in laws and cybersecurity practices, making it critical to enhance strategies for combating cyber threats.

One approach to tackling cybercrime is the use of advanced technologies such as machine learning and deep learning. These technologies can analyse large datasets, identify suspicious patterns, and detect fraud in text-based communication, including emails and SMS. For example, systems can classify fraudulent messages and phishing attempts, helping users and organizations prevent cyberattacks before they occur.

Natural Language Processing (NLP) has also shown promise in fraud detection by analysing text for specific keywords, patterns, and anomalies that indicate fraudulent intent. By automating the detection of these patterns, systems can significantly reduce the time required to identify and mitigate cyber threats.

Another area of focus is the financial sector, which is particularly vulnerable to cyberattacks. Real-world cases highlight the need for robust security frameworks, customer education, and proactive risk management to protect sensitive data. Innovative solutions such as integrating advanced encryption, biometric verification, and real-time threat detection models can strengthen security in banking systems and reduce vulnerabilities.

However, beyond technological solutions, there is a pressing need for collaboration between governments, private organizations, and individuals. Public awareness campaigns, well-defined legal frameworks, and global cooperation are essential to create a safe and secure digital environment.

Considering these challenges and insights, it is crucial to develop an advanced fraud detection and prevention system. This system should use cutting-edge technologies such as AI, NLP, and machine learning to detect fraudulent websites, phishing attempts, and smishing messages. Additionally, it should include features for filing complaints, guiding users on how to act after fraud, and connecting with relevant authorities like the police. Such a comprehensive solution will help protect users, prevent cybercrime, and build trust in the digital space.

After reading all the research paper we found that there are lots of system developed to prevent fraud but there is no system that will guide victim and provide every information telling what to do after fraud happed.

Our contribution in this project to make a system that will guide victim and, we adding feature that will help victim to file a complaint online to nearest police station make it easy for victim.

* **Project scope and limitations:**

The “Fraud Complaint Guidelines System” is designed to provide users with essential guidance on fraud prevention, reporting fraudulent activities, and seeking appropriate legal actions. This platform aims to enhance public awareness, streamline the fraud complaint process, and facilitate direct communication between victims and law enforcement authorities.

The system will allow users to report fraudulent websites, phone numbers, and scams, ensuring that necessary actions can be taken to prevent further harm. Additionally, it will feature a dedicated portal for police officers to review, approve, or reject complaints, making the resolution process more efficient. By offering an intuitive and user-friendly interface, the platform will ensure accessibility for a wide range of users, including those with limited technical knowledge.

**Limitations:**

**Limited** **Database**: Initially, the system will rely on a predefined set of reported fraud cases and may take time to expand its database for comprehensive fraud detection and prevention.

**Law** **Enforcement** **Response** **Time**: The effectiveness of the system depends on law enforcement agencies ability to promptly review and take action on complaints, which may vary based on workload and available resources.

**Awareness and Adoption:** While the platform provides valuable resources, users must be aware of its existence and actively engage with the system to maximize its impact.

Despite these limitations, the “Fraud Complaint Guidelines System” is a significant step towards improving fraud awareness and response, making it easier for victims to take action and for authorities to manage fraud-related cases efficiently.

**System Analysis**

* **Existing systems**

Several existing platforms provide information on fraud prevention and reporting, but they have notable limitations. Websites like cybercrime.gov.in offer users the ability to report cybercrimes; however, these platforms often lack detailed guidance on preventive measures or step-by-step processes for victims to follow encountering fraud. Additionally, such systems may not provide real-time updates or personalized notifications related to emerging fraud trends.

Social media channels and awareness campaigns by government agencies also play a role in informing the public about fraud. However, these sources can be easily overlooked in users’ feeds, leading to missed critical updates. Similarly, while some mobile applications exist for cybercrime reporting, they suffer from limited adoption, complicated interfaces, and inadequate integration with law enforcement systems.

The Fraud Complaint Guidelines System addresses these gaps by offering a user-friendly web platform where users can not only report fraudulent activities but also access comprehensive guidance on preventive measures. The system features a dedicated portal for police officers to manage and respond to complaints, real-time alerts about ongoing fraud trends, and educational resources, thereby ensuring a more holistic and efficient approach to fraud prevention and resolution.

* **Scope and limitations of existing systems**

**Scope:**

* Existing fraud reporting platforms, such as cybercrime.gov.in, allow users to report cybercrimes and fraudulent activities online.
* Government websites and portals provide general information on cyber safety and legal procedures related to fraud.
* Social media platforms are used by law enforcement agencies to spread awareness about recent fraud trends and safety tips.
* Some mobile applications enable users to receive alerts and updates on cyber threats, providing a channel for real-time information dissemination.
* Law enforcement agencies can access reports submitted by users, facilitating investigation and resolution processes.

**Limitations:**

* Lack of Comprehensive Guidance: Existing systems primarily focus on reporting fraud but do not provide step-by-step guidance on preventive measures or what victims should do immediately after encountering fraud.
* Complex Reporting Process: The complaint submission process on some platforms can be complicated, discouraging victims from reporting cases.
* Limited Real-Time Updates: Current systems may not offer real-time notifications about new fraud patterns, leaving users vulnerable to emerging threats.
* Poor User Engagement: Social media updates can easily be missed by users, and mobile applications may face adoption issues due to limited awareness and complex interfaces.
* Inadequate Law Enforcement Integration: Many platforms lack efficient mechanisms for police officers to manage, approve, or reject complaints systematically.
* The Fraud Complaint Guidelines System aims to overcome these limitations by providing a centralized, user-friendly platform that offers complete fraud prevention guidance, streamlined reporting processes, real-time fraud alerts, and a dedicated portal for law enforcement agencies to manage complaints efficiently.
* **Project perspective, features**

The Fraud Complaint Guidelines System is designed from the perspective of enhancing user awareness, engagement, and accessibility in the fight against fraud. The system provides comprehensive guidance on fraud prevention, offers step-by-step instructions on what to do after experiencing fraud, and allows users to report fraudulent activities such as scam websites and phone numbers.

**Key Features:**

* Notifications:

Users receive tailored alerts about new fraud trends, scams, and safety on their email address

* Real-Time Updates:

Instant notifications about emerging fraud cases, critical updates, and the status of submitted complaints, helping users stay informed and vigilant.

* Feedback Mechanism:

Users can provide feedback on reported cases, prevention tips, and the overall system, enabling continuous improvement based on user needs and experiences.

* Integration with Law Enforcement Databases:

Seamless integration with police and government databases ensures the accuracy of reported information and streamlines the complaint-handling process for quicker resolutions.

* Accessibility Features:

The platform is designed to be inclusive, featuring compatibility with screen readers, text-to-speech options, and other assistive technologies, making it accessible to users with disabilities.

The Fraud Complaint Guidelines System provides a comprehensive, user-friendly solution that empowers individuals to prevent, report, and recover from fraudulent activities, while also supporting law enforcement in handling fraud cases efficiently.

* **Stakeholders**
* Citizens (Victims and General Public): Everyday individuals who are potential victims of online scams, financial fraud, identity theft, and phishing attacks. For example, online shoppers who might encounter fake e-commerce websites or individuals receiving fraudulent calls posing as bank representatives.
* Law Enforcement Agencies (Police and Cybercrime Units): Cybercrime cells like India’s Cyber Crime Portal (cybercrime.gov.in), which handle cases related to online fraud, financial scams, and cyberbullying. Local police departments that verify and investigate fraud complaints, ensuring timely legal action against offenders.
* Regulatory and Government Authorities: Government bodies like the Reserve Bank of India (RBI), which issues guidelines on safe digital transactions, and the Ministry of Home Affairs, which oversees cybercrime prevention initiatives. These authorities use data from fraud reports to create better policies and awareness programs to protect citizens.
* Cybersecurity Firms and Experts: Organizations like CERT-In (Indian Computer Emergency Response Team) and private cybersecurity firms that monitor cyber threats and provide insights into emerging fraud techniques. Their expertise ensures the system remains updated with the latest fraud prevention strategies and security measures.
* Community Organizations and NGOs: NGOs working to promote digital literacy and cybersecurity awareness, especially among rural populations, senior citizens, and low-income communities.

**Requirement Analysis**

* **Function requirement**
* User Registration and Login:

Users can register by providing personal details such as name and Email. They can log in using secure credentials to access their dashboard for fraud reporting, complaint and guidance.

* User Profile Management:

Users can view their profile information, and reported phone numbers and websites as well as complaints and evidences they had provided while complaining.

* Fraud Reporting and complaining:

Users can report fraudulent websites, phone numbers by filling out a report form and for fraudulent activities by filling out a complaint form. The system will provide acknowledgment and track the status of complaints.

* Police Officer Portal:

A dedicated portal for police officers to review, approve, or reject complaints, manage case progress, and communicate with users.

* Fraud Prevention Resources:

The system provides educational resources, including articles and videos, on how to prevent fraud and steps to take after becoming a victim.

* **Performance Requirements:**
* Response Time:

The system should process and display complaint submission confirmations within 2-3 seconds of user input.

* Dashboard Load Time:

User dashboards should load within 5 seconds, even when displaying multiple reports and updates.

* Notification Delivery:

Status updates (via email) regarding complaint processing should be delivered within 10 seconds of updates.

* Database Query Speed:

Queries related to reported fraud cases and user data should return results in less than 2 seconds under normal load.

* **SECURITY REQUIREMENTS:**
* User Authentication and Authorization:

Secure login mechanisms using hashed passwords, ensuring only authorized users can access their dashboards.

* Data Encryption:

Sensitive user data, including complaint details, will be encrypted to ensure privacy and prevent unauthorized access.

* Role-Based Access Control (RBAC):

Role-based access will ensure that only police officers can view and manage complaint details, while users can access only their reports.

* Input Validation and Data Sanitization:

All user inputs will be validated and sanitized to prevent SQL injection and other cyberattacks.

* Secure Communication:

The platform will use HTTPS for secure data transmission between users and the server.

* Audit Logs:

Comprehensive logs will track user activities, including complaint submissions and police actions, to detect suspicious behaviour.

**Design System**

* **Design Constraint**

Technology Stack Constraints

1. **Backend Technology (Jakarta EE - Servlets & JSP)**

The system relies on Jakarta EE, meaning all backend functionalities implemented using Java and Jakarta EE libraries. The project follows a servlet-based architecture, to handle communicationbetween Databases and JSP and helping to separate backend and frontend by implementing servlet for backend and JSP for frontend.

1. **Database (MySQL):**

The database follows a structured relational mode, MySQL is used, queries used for performance,

especially for searching, filtering, and retrieving large amounts of user-reported fraud data.

1. **File Storage (Server-Side for Evidence Files)**

Storing user recordings and evidence files on the server increases storage requirements and may impact performance as the number of cases grows., Security Risks and for Dynamic File Serving, we store the all the file on computer and retrieve the file using servlet.

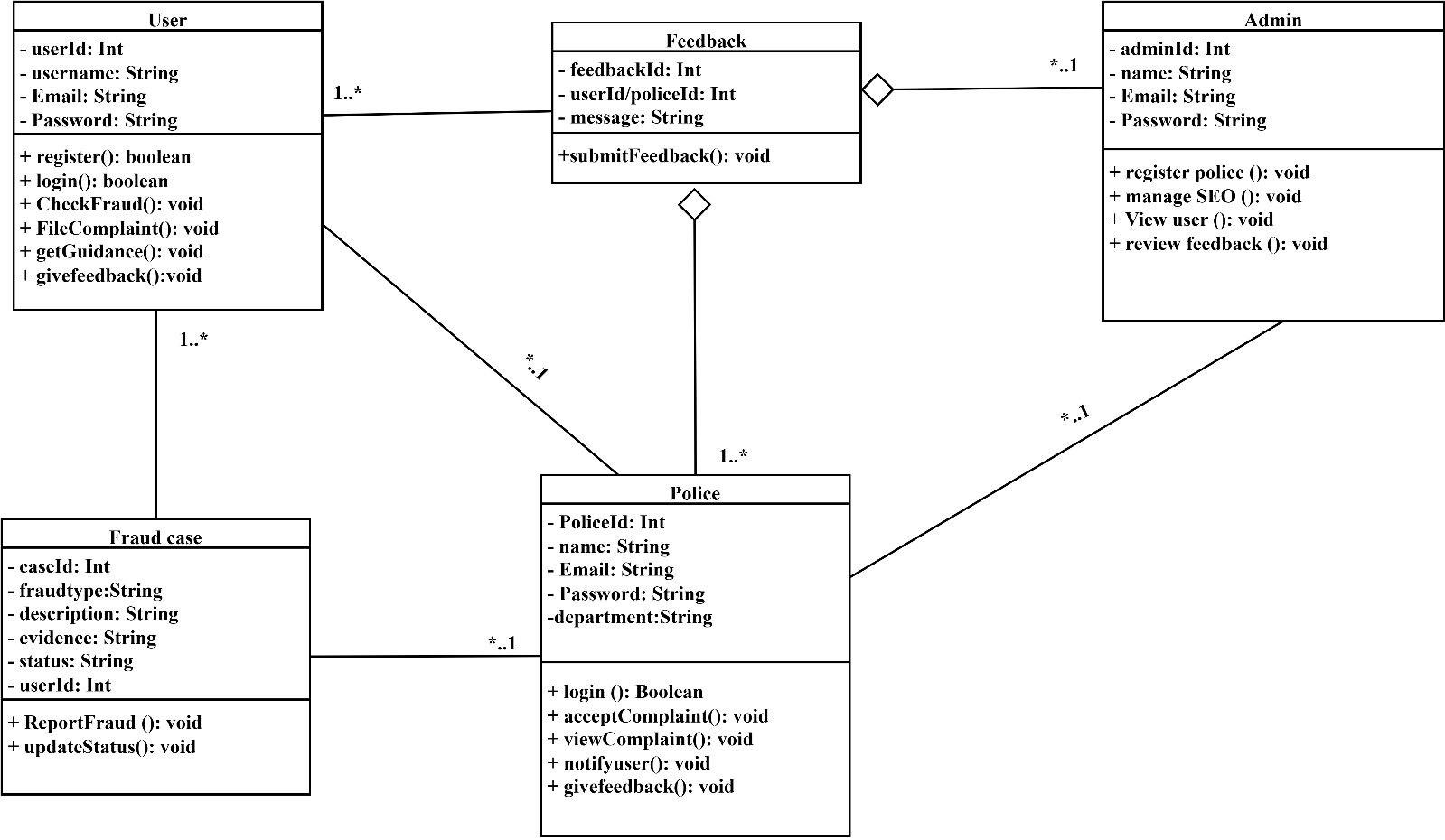
1. **Notification Service (Email via Jakarta Mail API)**

The system depends on email notifications, meaning SMTP server to send case related update to and sending alerts to user.

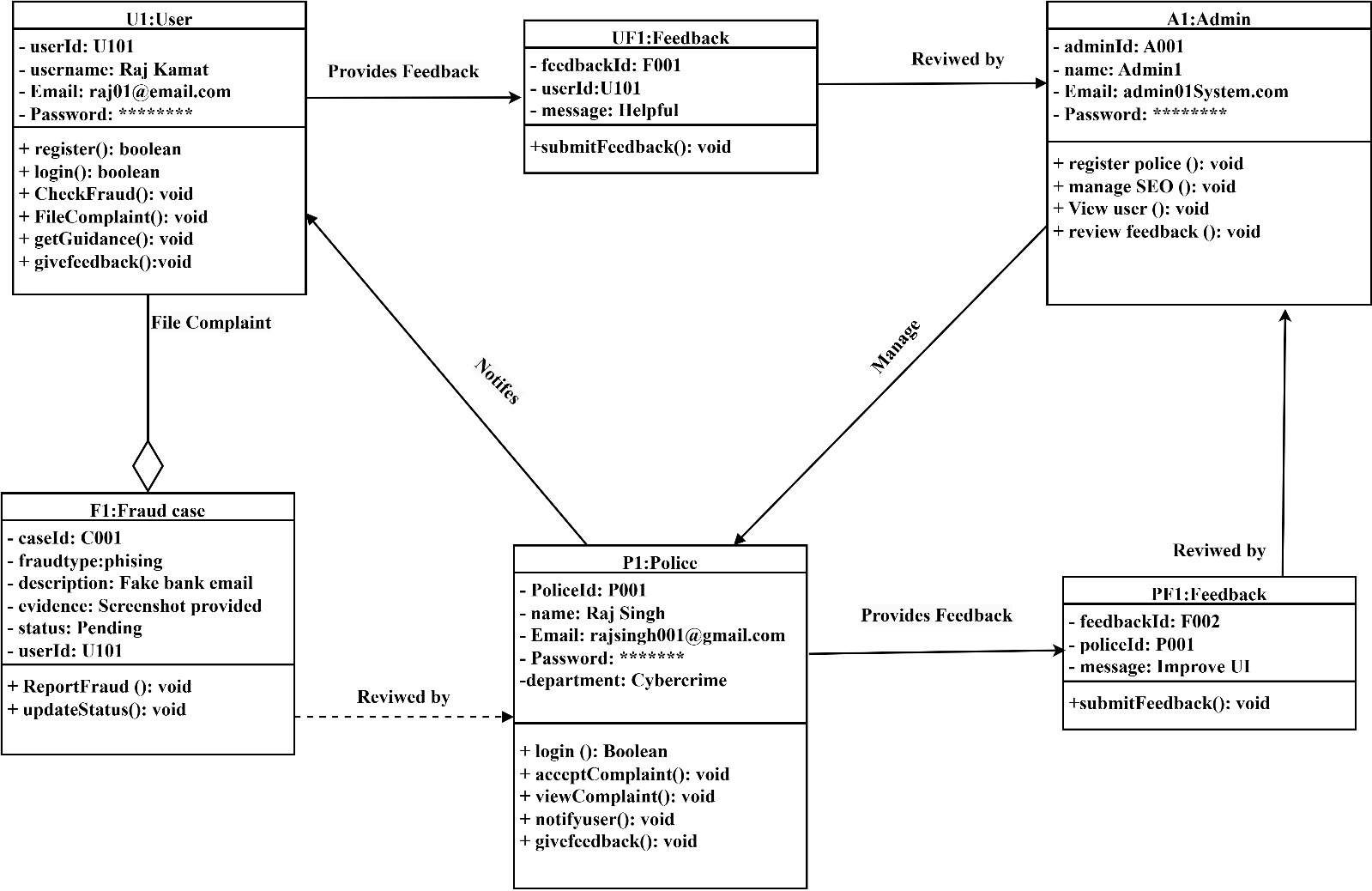
* **System Model**

**UML Diagram: -**

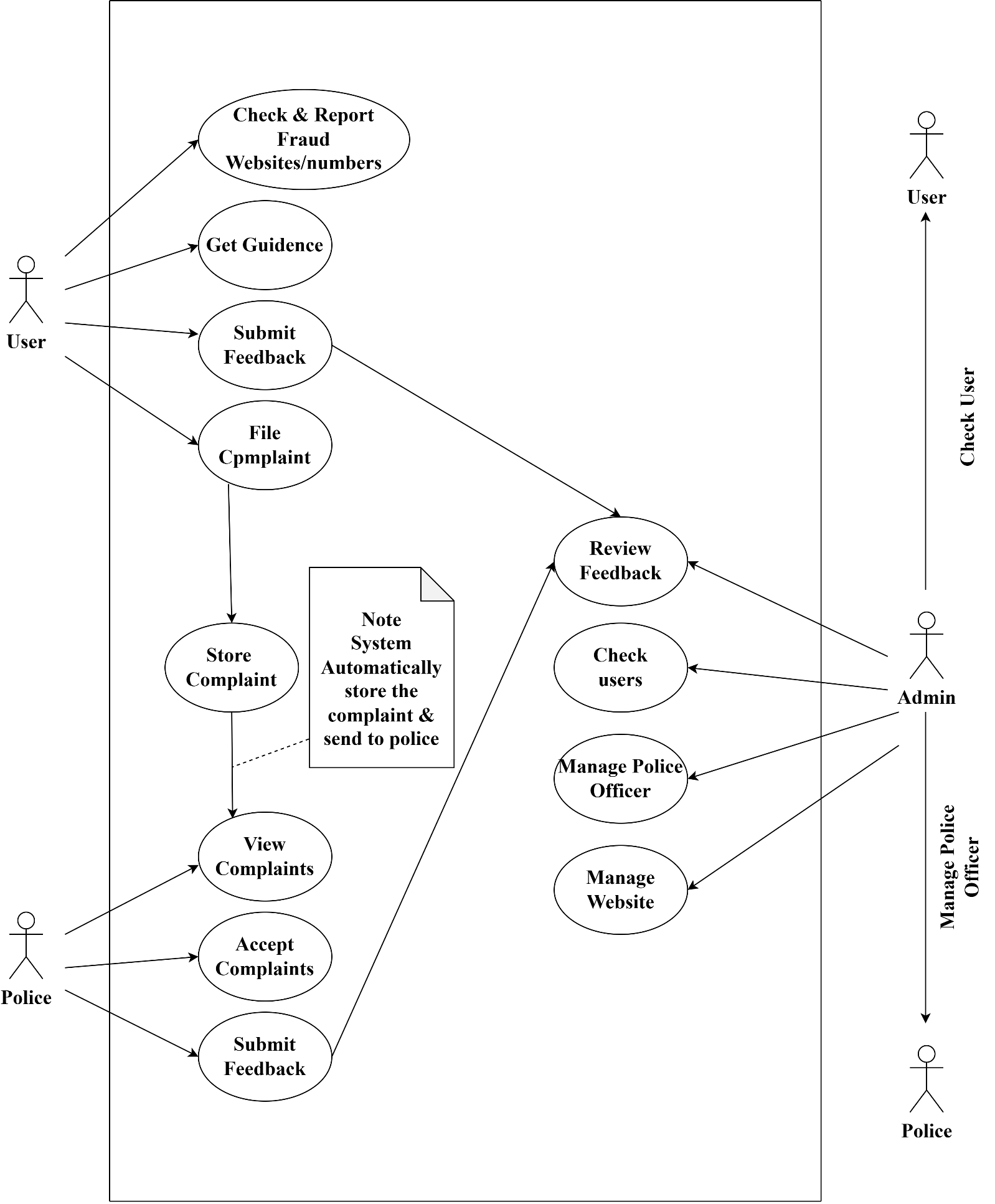
1. Class Diagram:

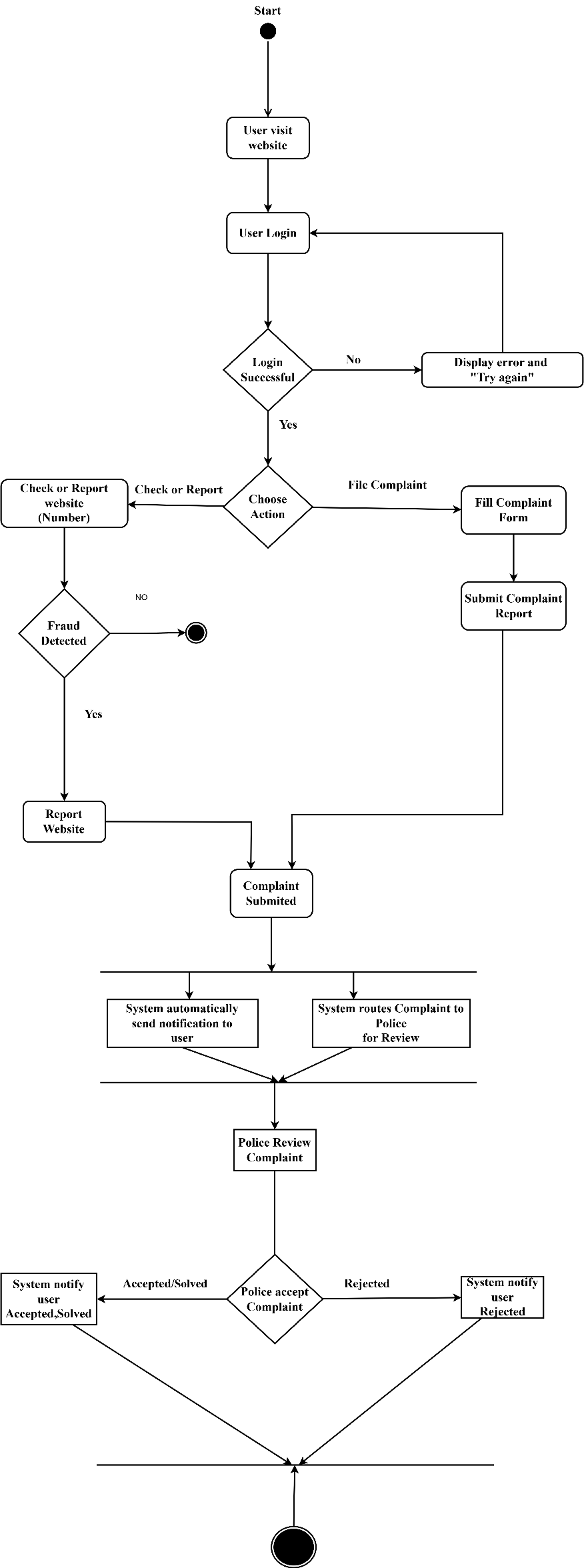
****

1. ObjectDiagram:

****

1. Ues Case Diagram:

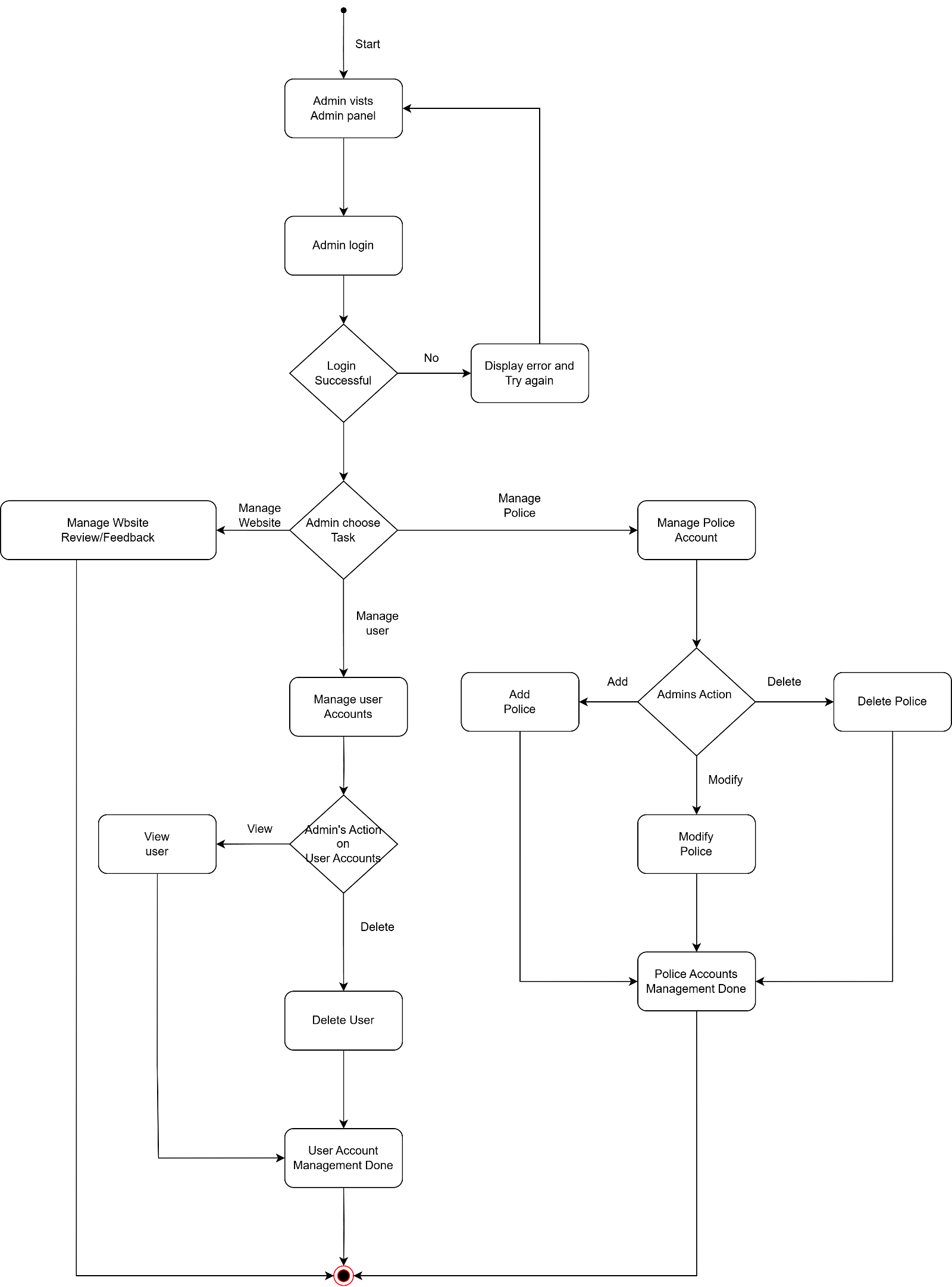




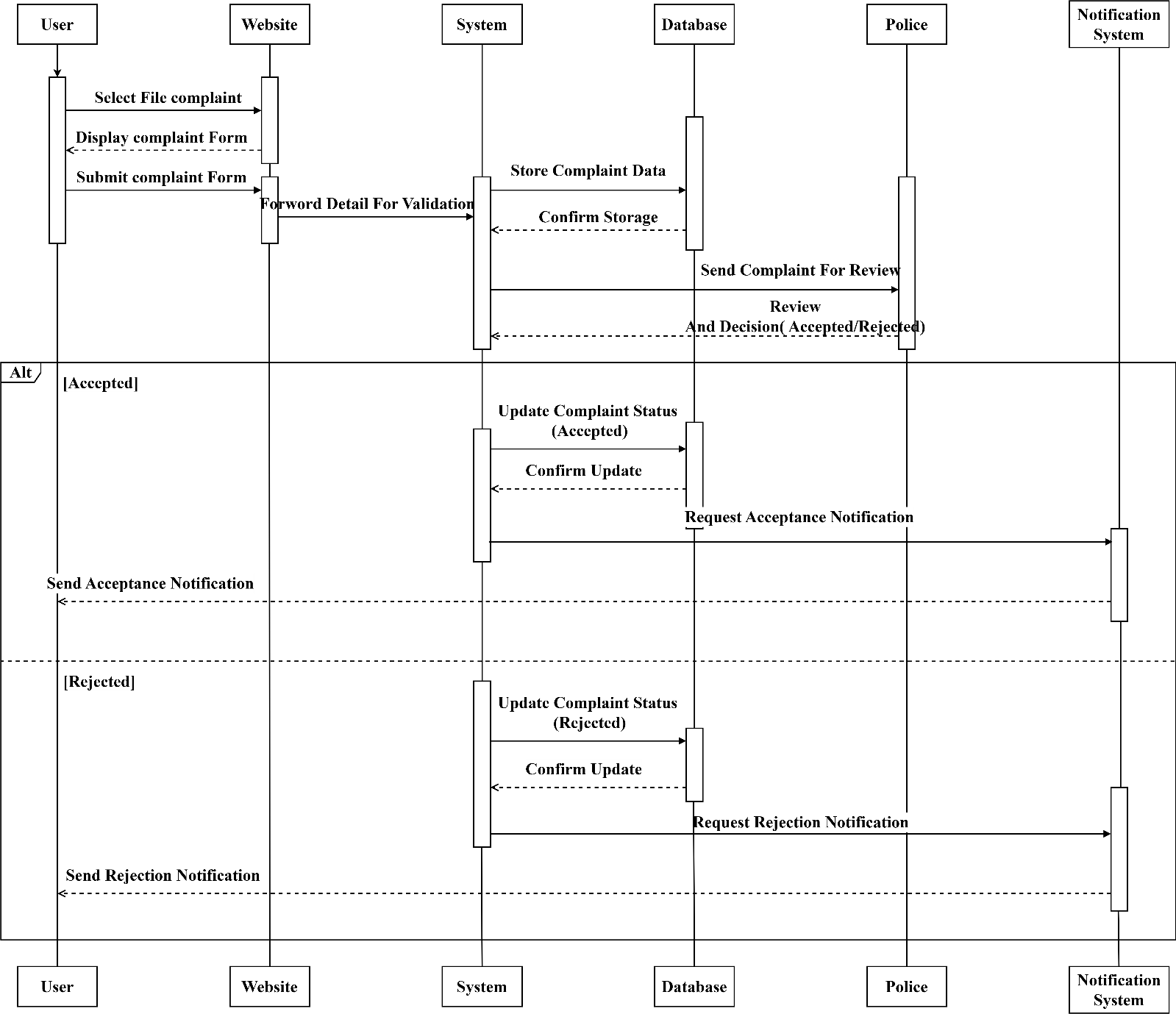
1. Activity Diagram:

1.User

2.Admin



1. Sequence diagram:



* **Data Model**:

The relational data model in MySQL organizes data into structured tables, where each table represents an entity and consists of rows (records) and columns (attributes). Each table has a primary key that uniquely identifies each record, ensuring data integrity. Relationships between tables are established using foreign keys, which reference primary keys from related tables. This model supports operations such as data retrieval, insertion, and updating through SQL. In this project we had to use 12 tables

(admin, alerts, fraud\_data, google\_safe\_browsing, police\_feedback, police\_officers, reports, seo\_settings, use, user feedback, complaints, evidence,)

1 admin-

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Not Null | Type | Key |
| admin\_id | Not Null | int | Primary key |
| password | Not Null | varchar (255) | -- |
| username | Not Null | varchar (100) | Unique |

2 alerts-

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Not Null | Type | Key |
| id | Not Null | int | Primary key |
| headline | Not Null | varchar (255) | -- |
| message | Not Null | text | -- |
| created\_by | Not Null | varchar (50) | -- |
| created\_at | Null | timestamp | -- |

3 fraud\_data-

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Not Null | Type | Key |
| id | Not Null | int | Primary key |
| fraud\_url\_or\_number | Null | varchar (500) | Unique |
| category | Null | varchar (50) |  |
| source | Null | varchar (50) |  |
| risk\_level | Null | varchar (20) |  |
| added\_on | Null | timestamp |  |

4 google\_safe\_browsing-

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Not Null | Type | Key |
| id | Not Null | int | Primary key |
| url | Not Null | varchar (500) | Unique |
| verified\_fraud | Null | enum('Yes','No') |  |
| last\_checked | Null | timestamp |  |

5 police\_feedback-

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Not Null | Type | Key |
| feedback\_id | Not Null | int | Primary key |
| p\_id | Null | int | Foreign key |
| subject | Not Null | varchar (255) |  |
| message | Not Null | text |  |
| created\_at | Null | timestamp |  |

6 police\_officers-

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Not Null | Type | Key |
| p\_id | Not Null | int | Primary key |
| name | Not Null | varchar (100) |  |
| batch\_id | Not Null | varchar (50) | Unique |
| password | Not Null | varchar (255) |  |
| police\_station | Not Null | varchar (150) |  |
| city | Not Null | varchar (100) |  |
| created\_at | Null | timestamp |  |
| email | Not Null | varchar (255) | Unique |

7 user-

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Not Null | Type | Key |
| iduser | Not Null | int | Primary key |
| name | Not Null | varchar (100) |  |
| email | Not Null | varchar (100) |  |
| password | Not Null | varchar (1000) |  |
| submission\_date | Null | timestamp |  |

8 reports-

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Not Null | Type | Key |
| idreports | Not Null | int | Primary key |
| no\_orurl | Not Null | varchar (1000) |  |
| date | Not Null | date |  |
| description | Not Null | longtext |  |
| userID | Not Null | int | Foreign key |

9 seo\_settings-

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Not Null | Type | Key |
| id | int | Not Null | Primary key |
| title | varchar (255) | Null |  |
| description | text | Null |  |
| keywords | text | Null |  |

10 user\_feedback-

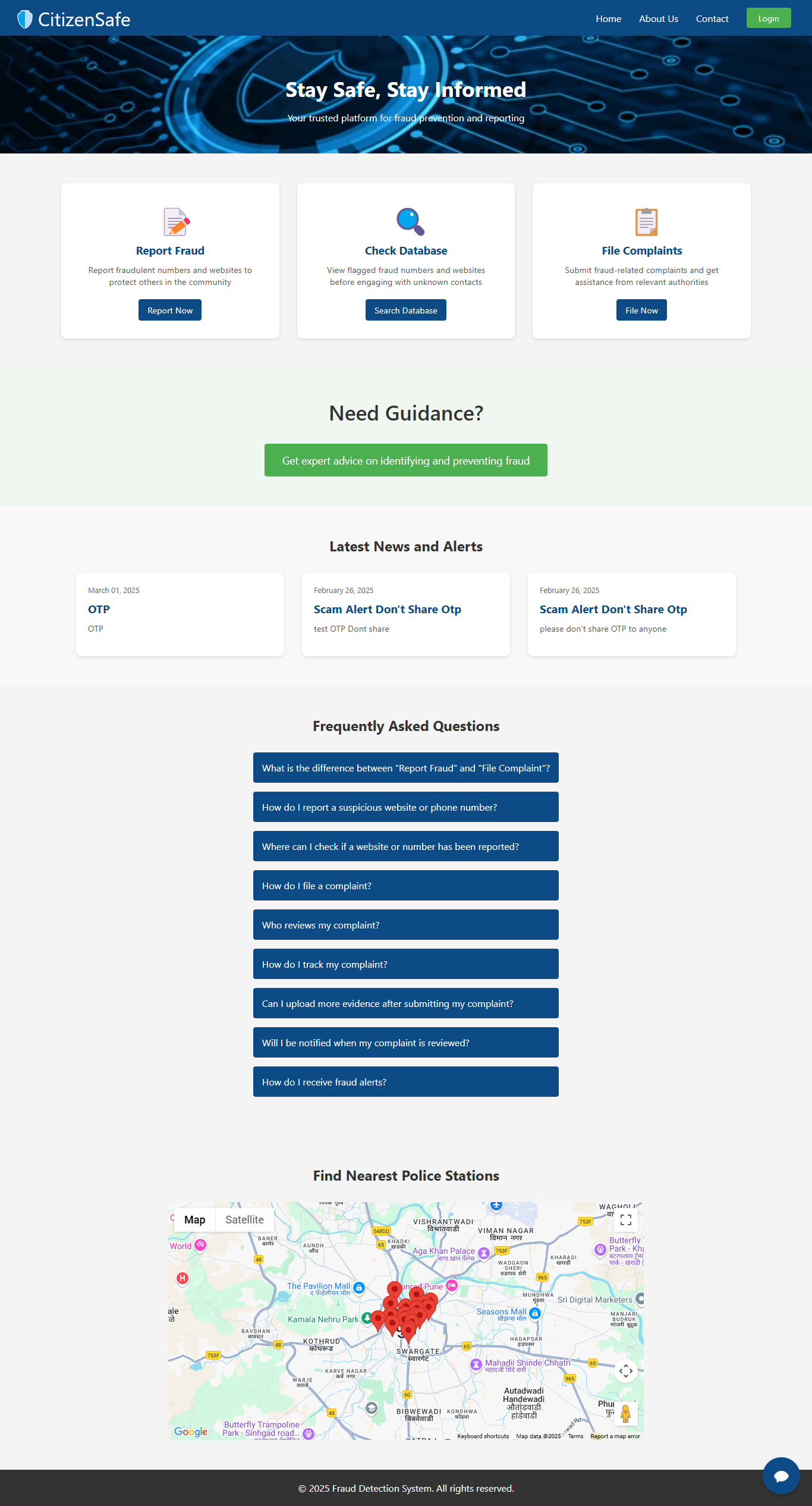
|  |  |  |  |
| --- | --- | --- | --- |
| Name | Not Null | Type | Key |
| feedback\_id | Not Null | int | Primary key |
| user\_id | Null | int | Foreign key |
| subject | Not Null | varchar (255) |  |
| message | Not Null | text |  |
| created\_at | Null | timestamp |  |

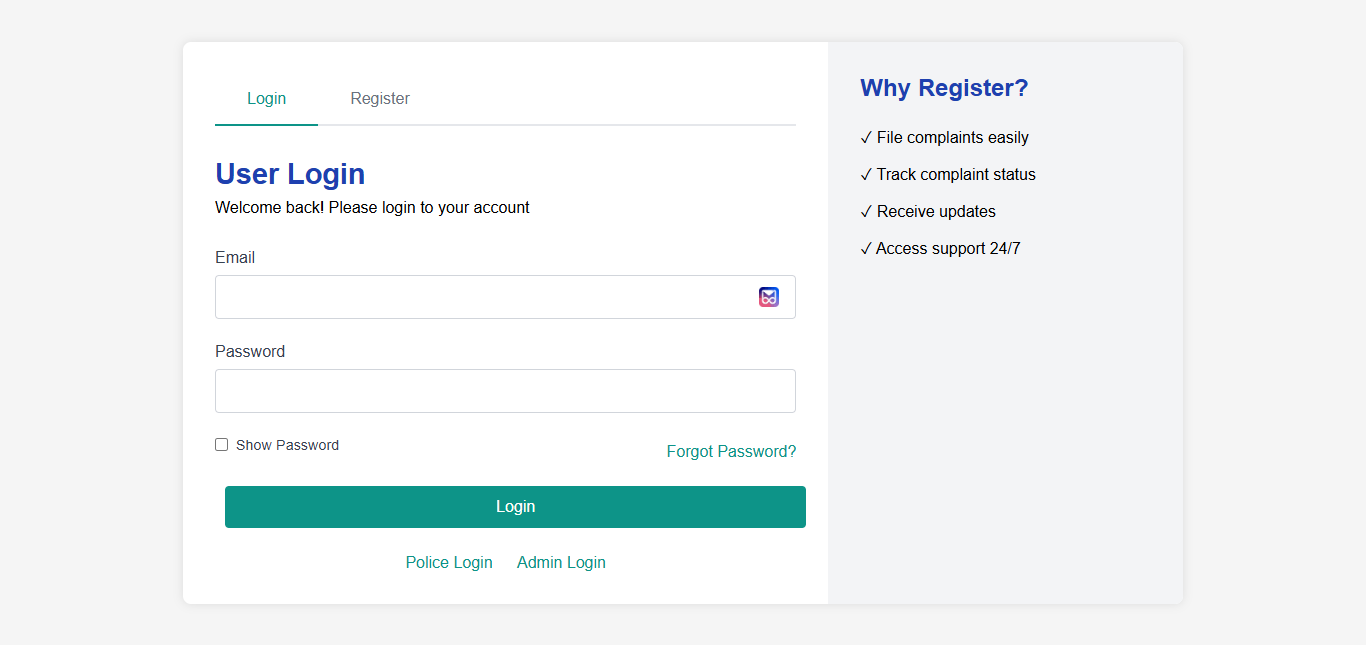
11 evidence-

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Not Null | Type | Key |
| evidence\_id | Not Null | int | Primary key |
| complaint\_id | Not Null | int | Foreign key |
| evidence\_type | Not Null | enum('document','recording') |  |
| name | Not Null | varchar (255) |  |
| path | Not Null | varchar (255) |  |
| file\_type | Not Null | varchar (50) |  |
| duration\_seconds | Null | int |  |
| upload\_date | Null | timestamp |  |

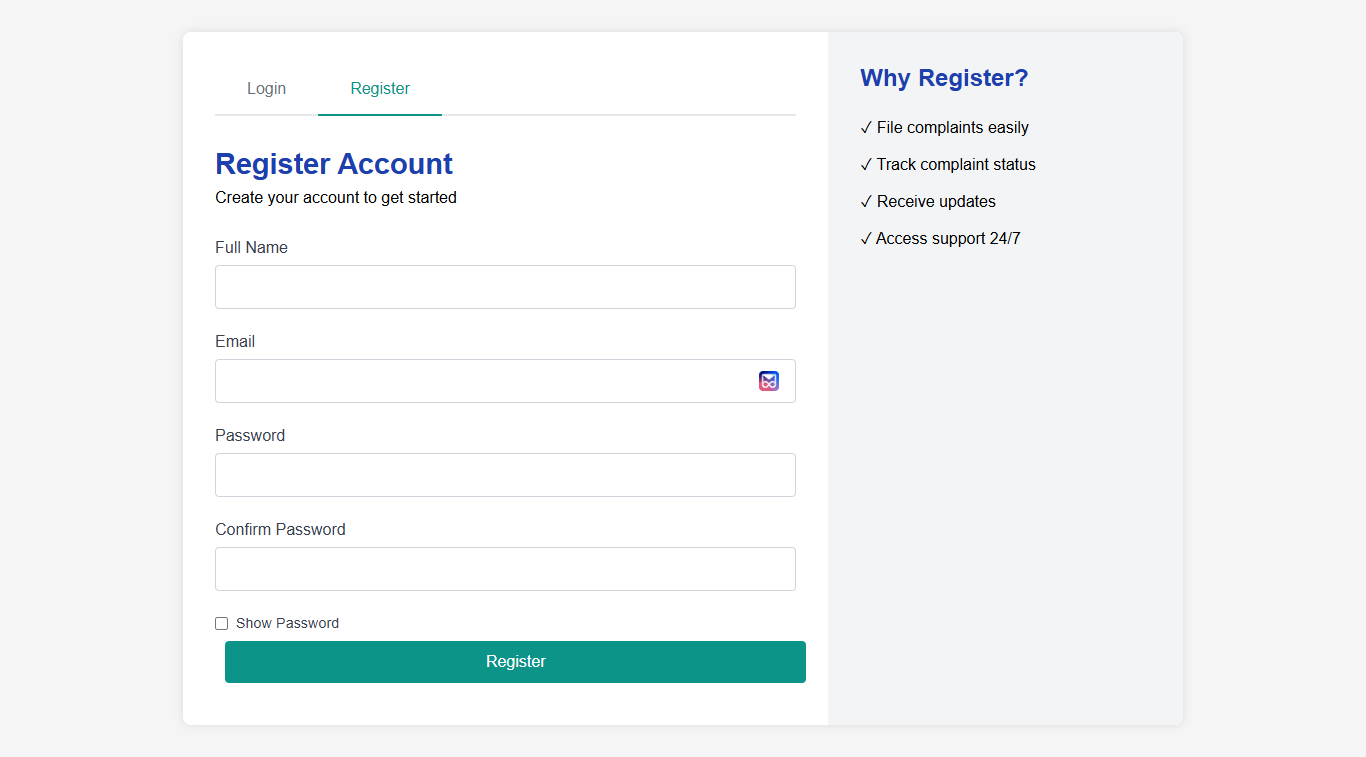
12 complaints-

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Not Null | Type | Key |
| idcomplaint | Not Null | int | Primary key |
| iduser | Not Null | int | Foreign key |
| name | Not Null | varchar (1000) |  |
| contact | Not Null | varchar (45) |  |
| type | Not Null | varchar (100) |  |
| incident\_date | Not Null | date |  |
| description | Not Null | longtext |  |
| submission\_date | Null | timestamp |  |
| status | Null | varchar (20) |  |
| nearest\_police\_station | Not Null | varchar (255) |  |
| feedback | Null | text |  |
| police\_id | Null | int | Foreign key |
| case\_report\_path | Null | varchar (255) |  |

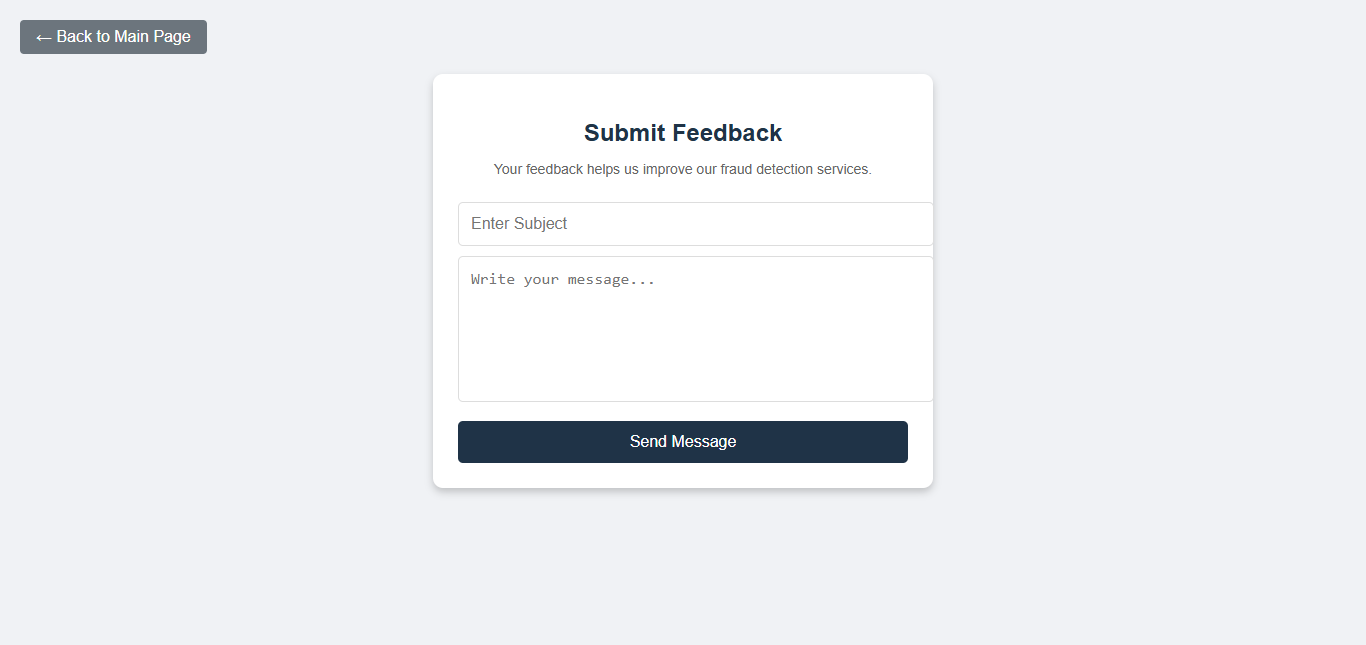
* **User Interface (UI)**
* **User UI**
* ****Landing Page -
* Login Page -



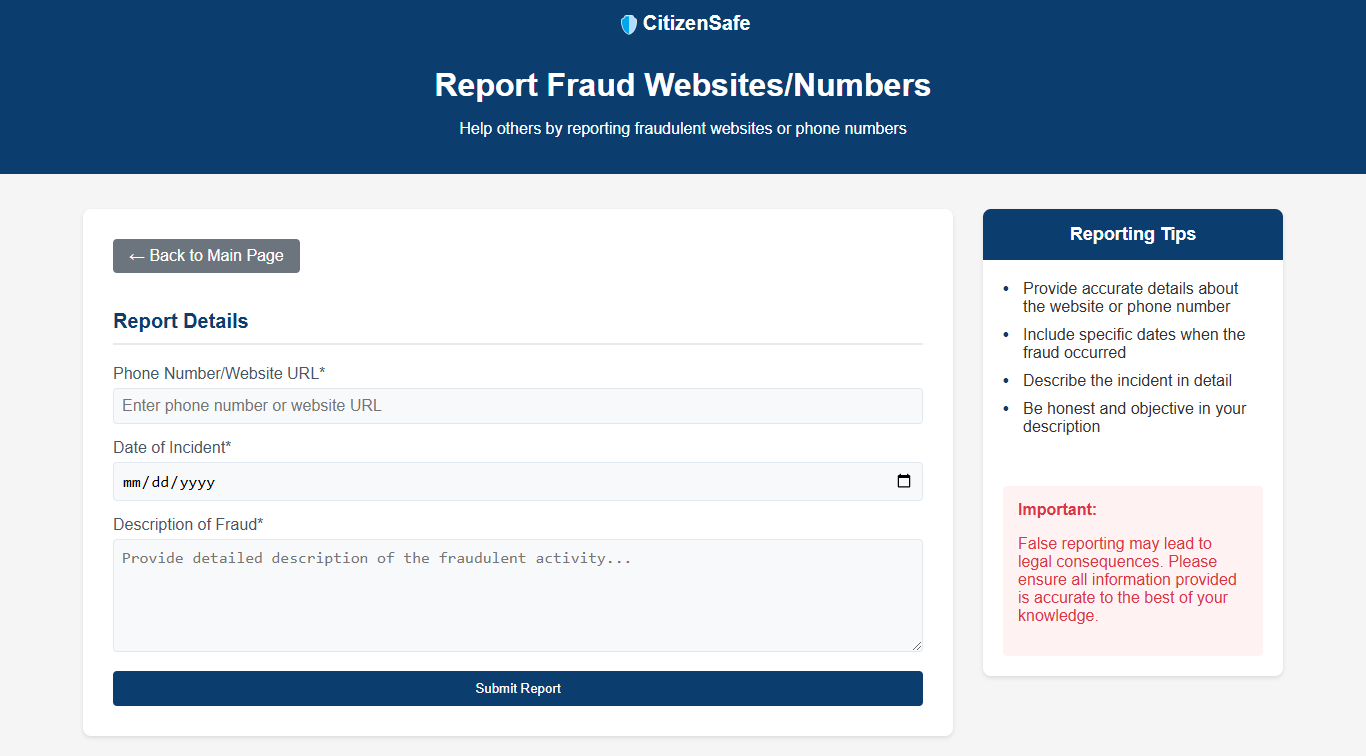
* Registration Page -



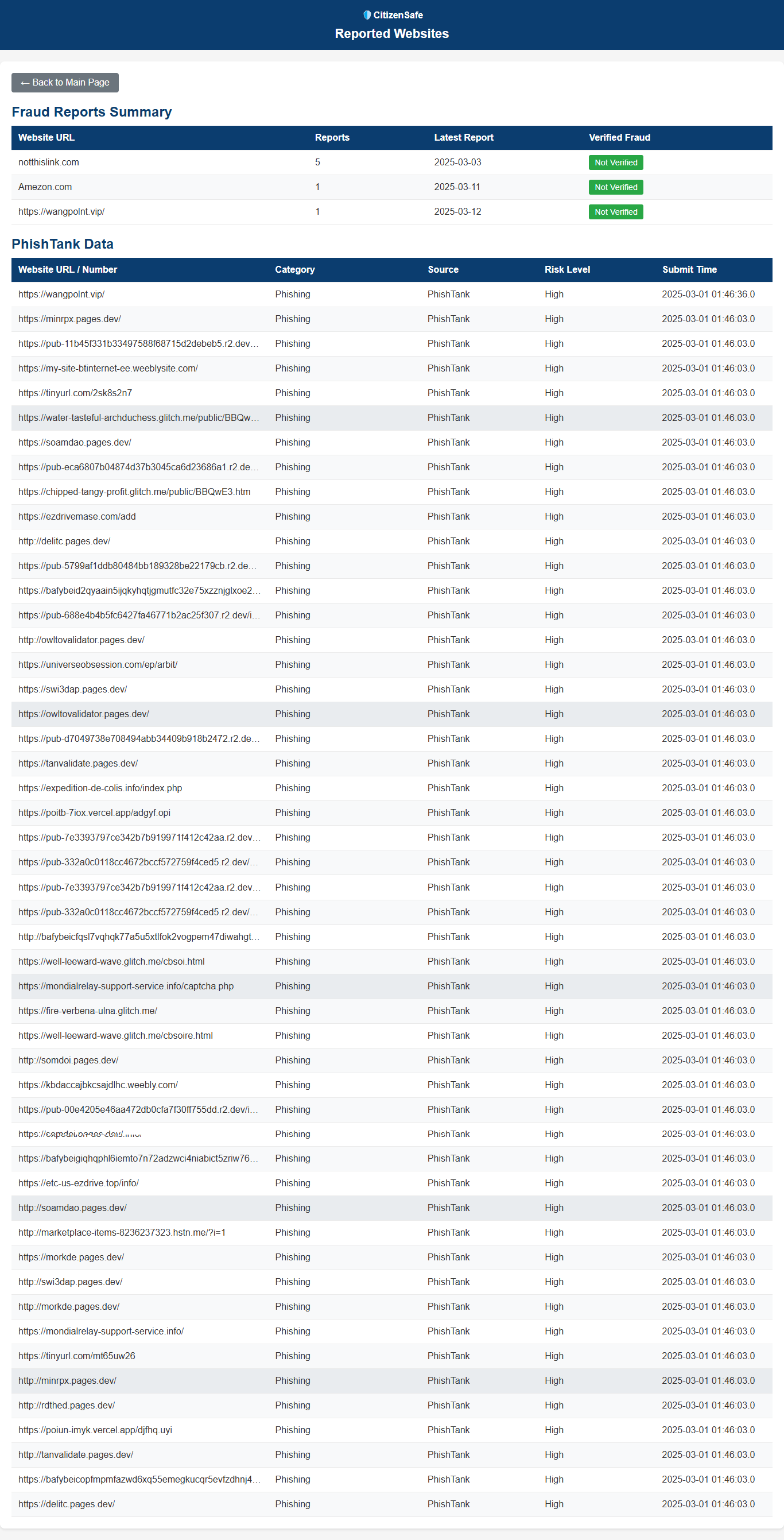
* Feedback Page -



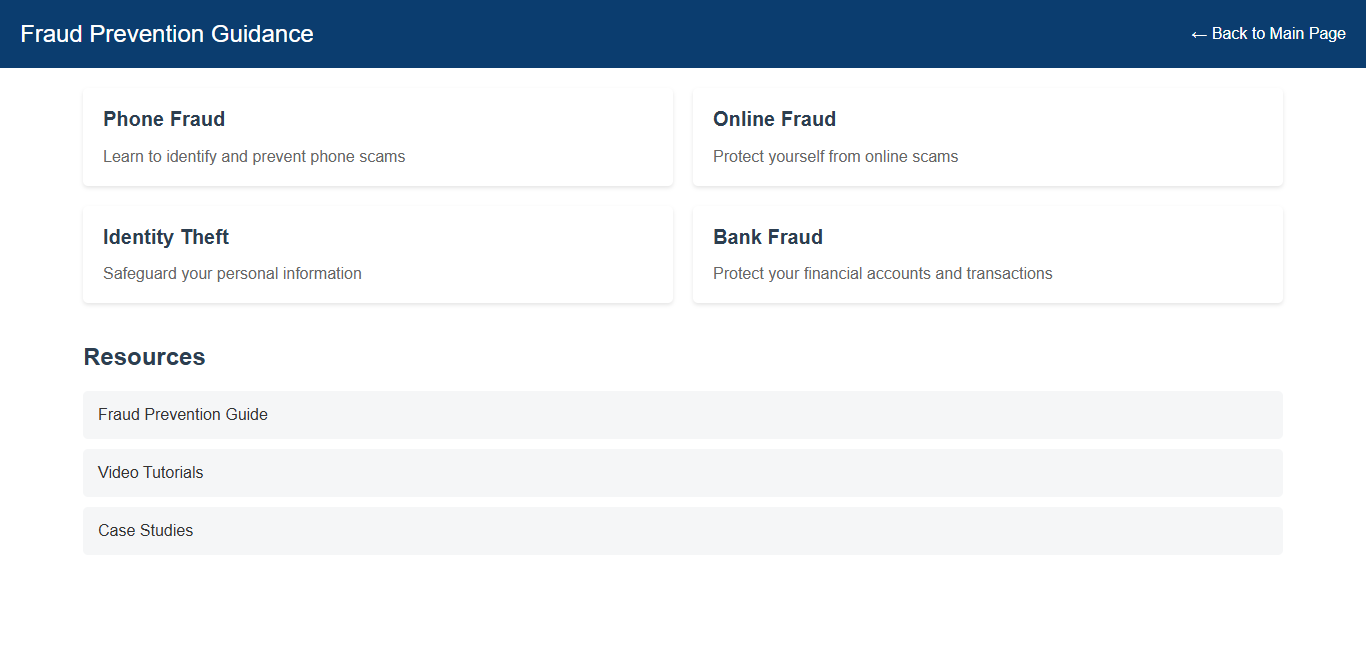
* Report Fraud Page -



* Fraud Database Page -

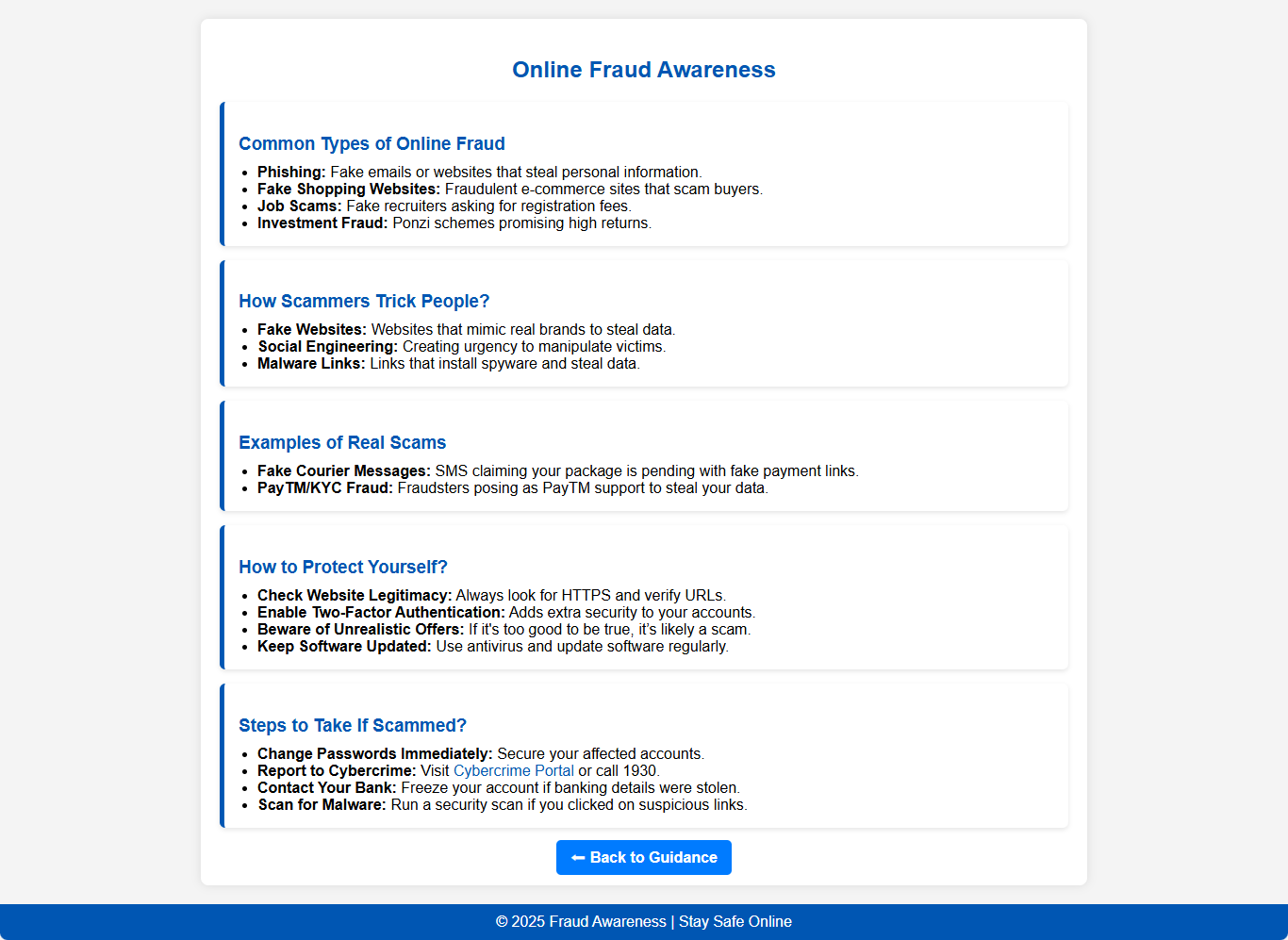


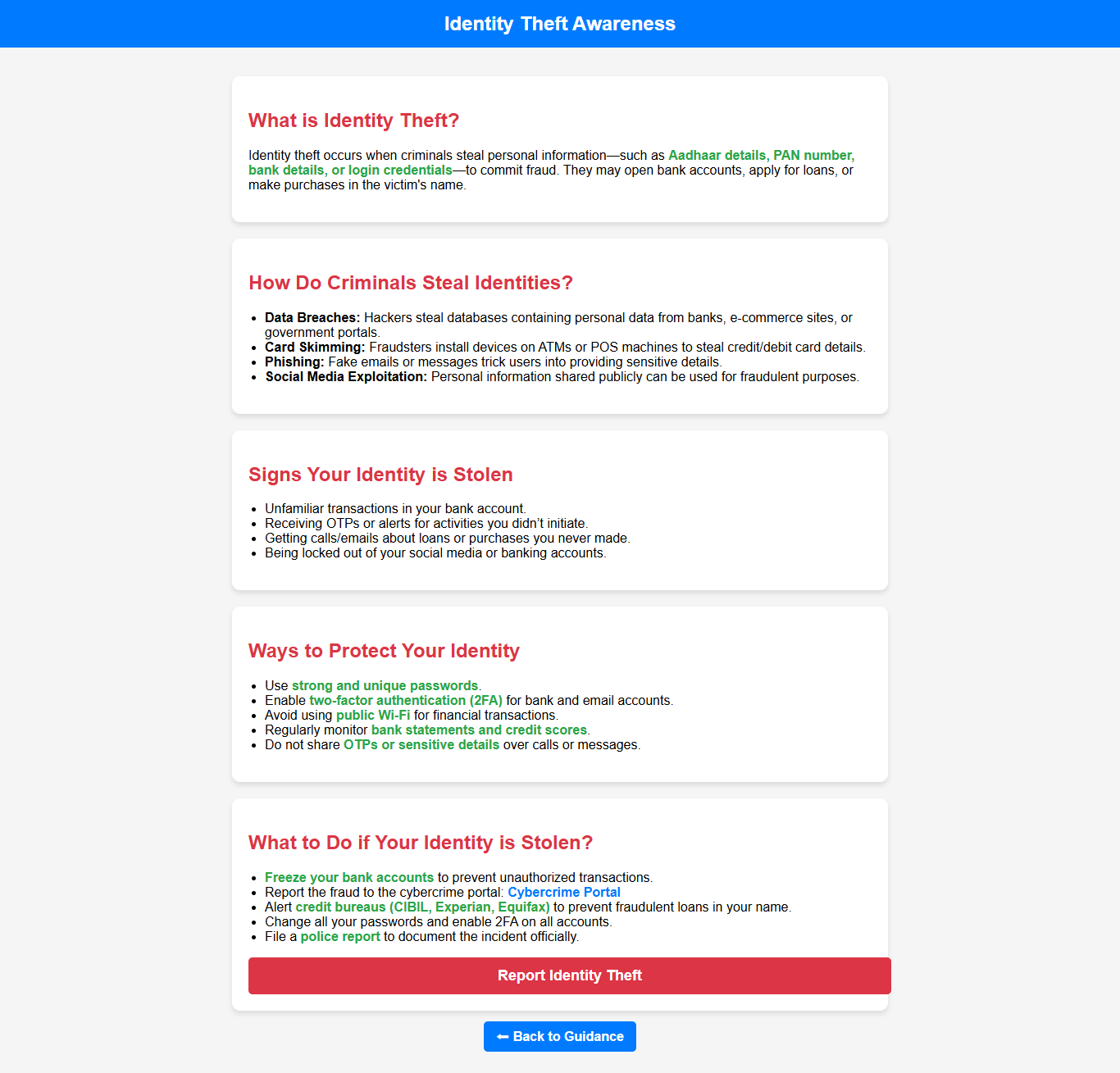
* Guidance Page -



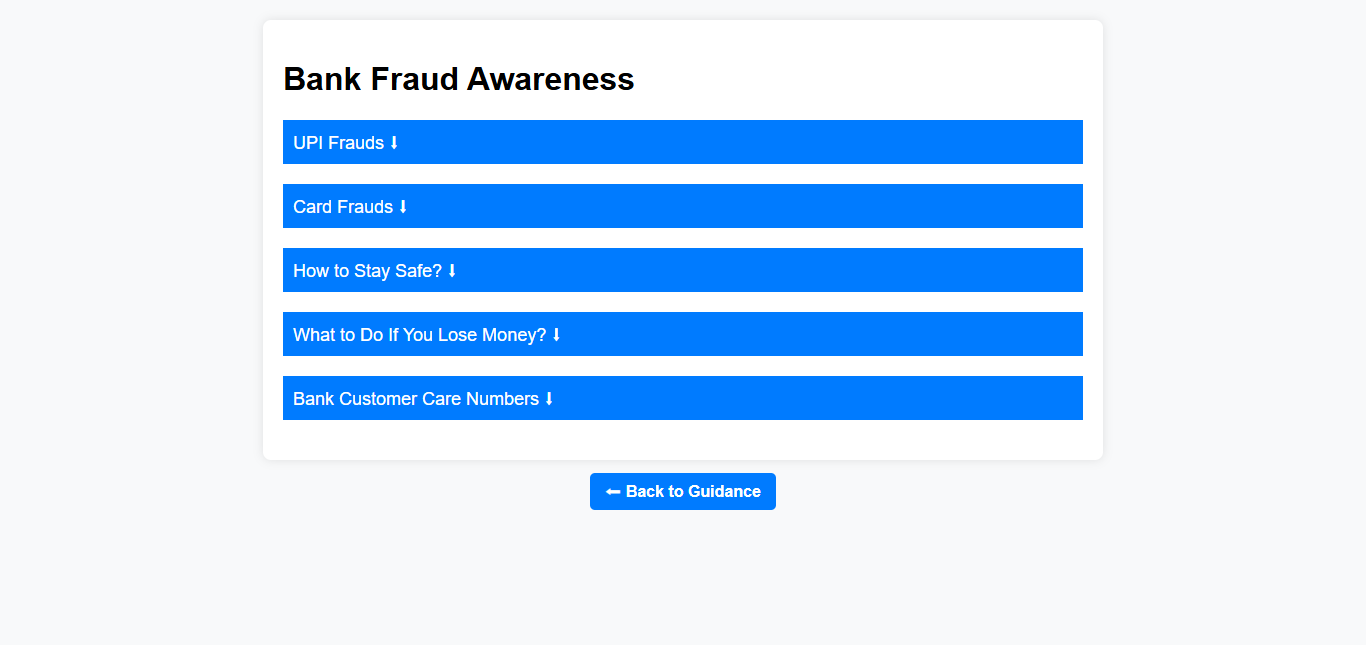
* Phone Fraud Guide –



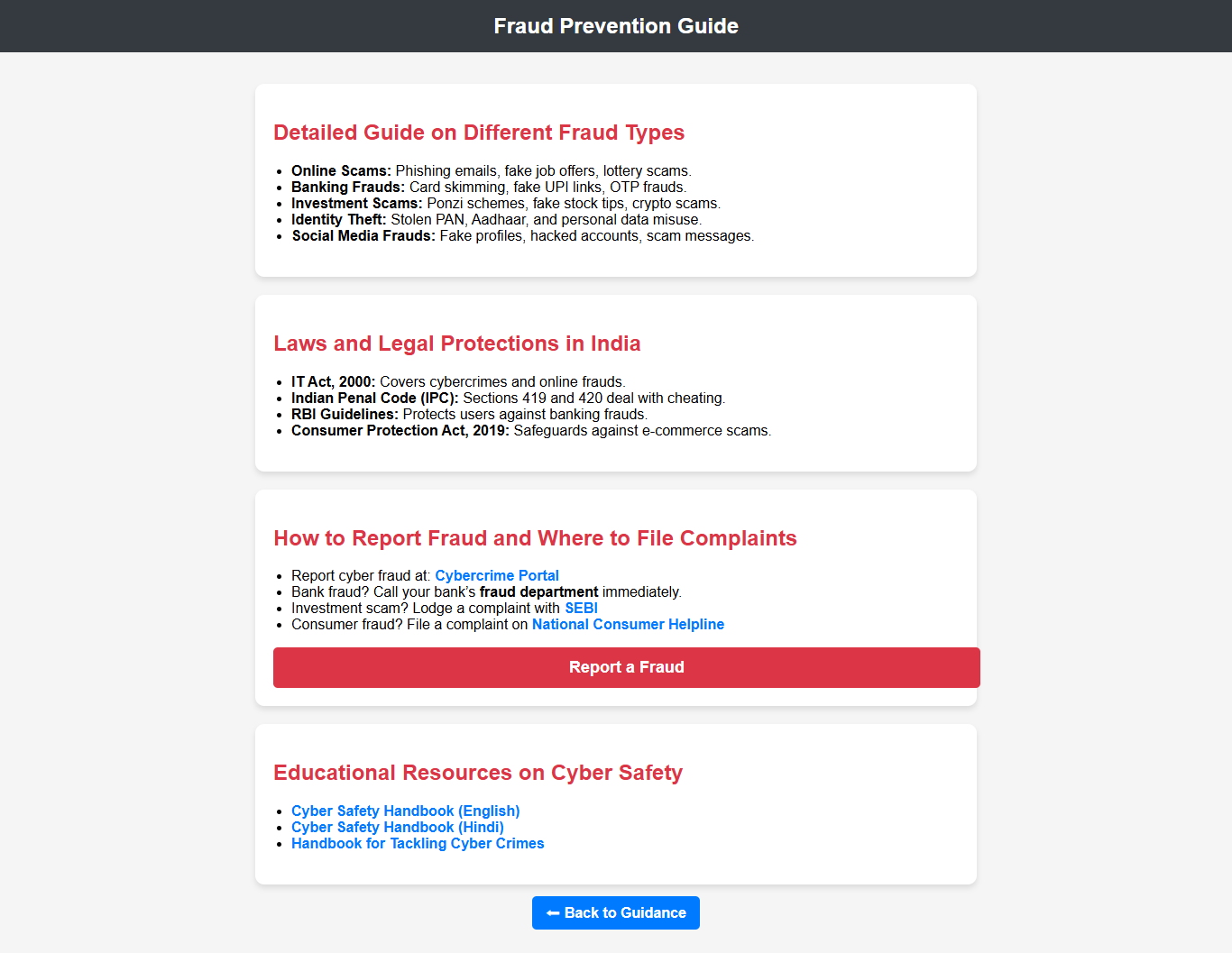
* Online Fraud Guide –
* Identity Fraud Guide:



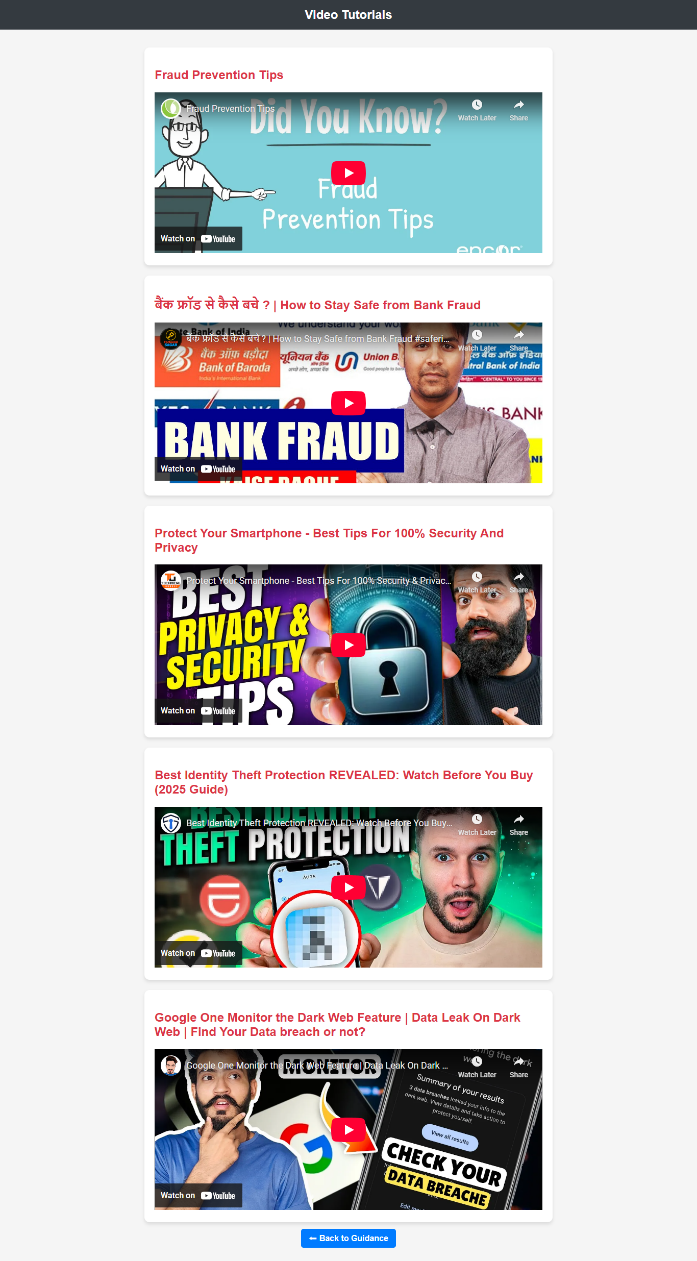
Bank Fraud Guide-



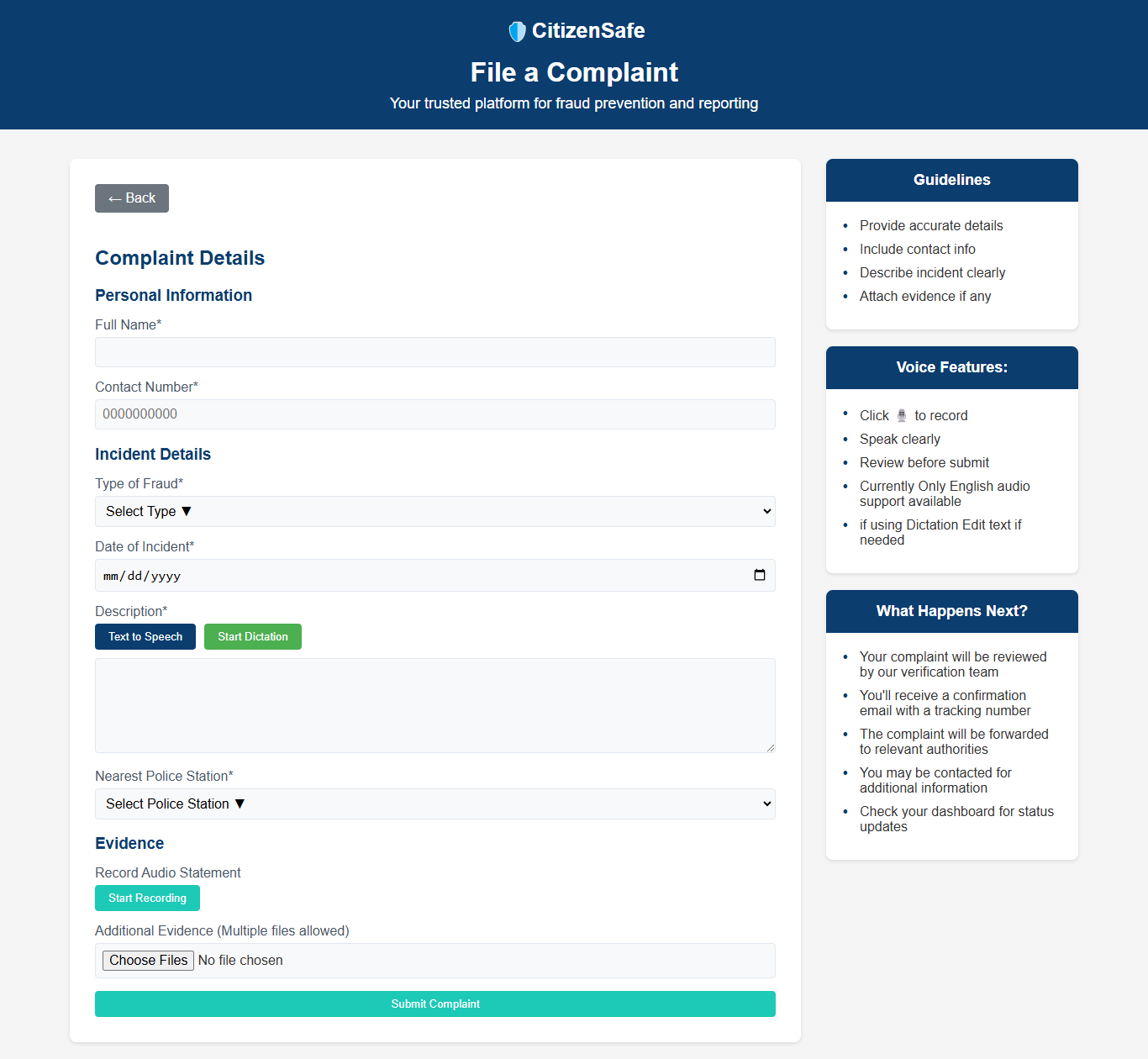
* Fraud Prevention guide -



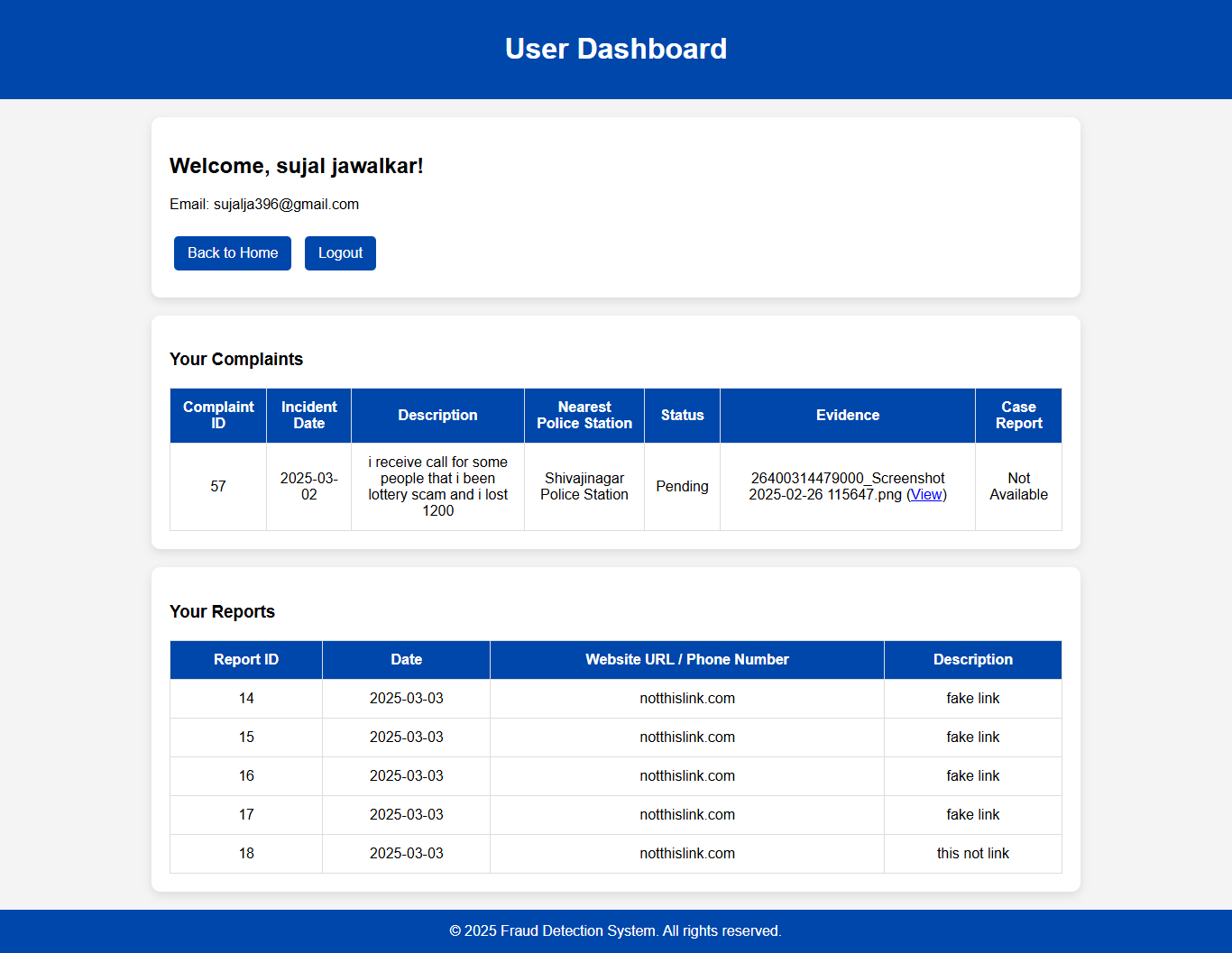
* Video Tutorials –



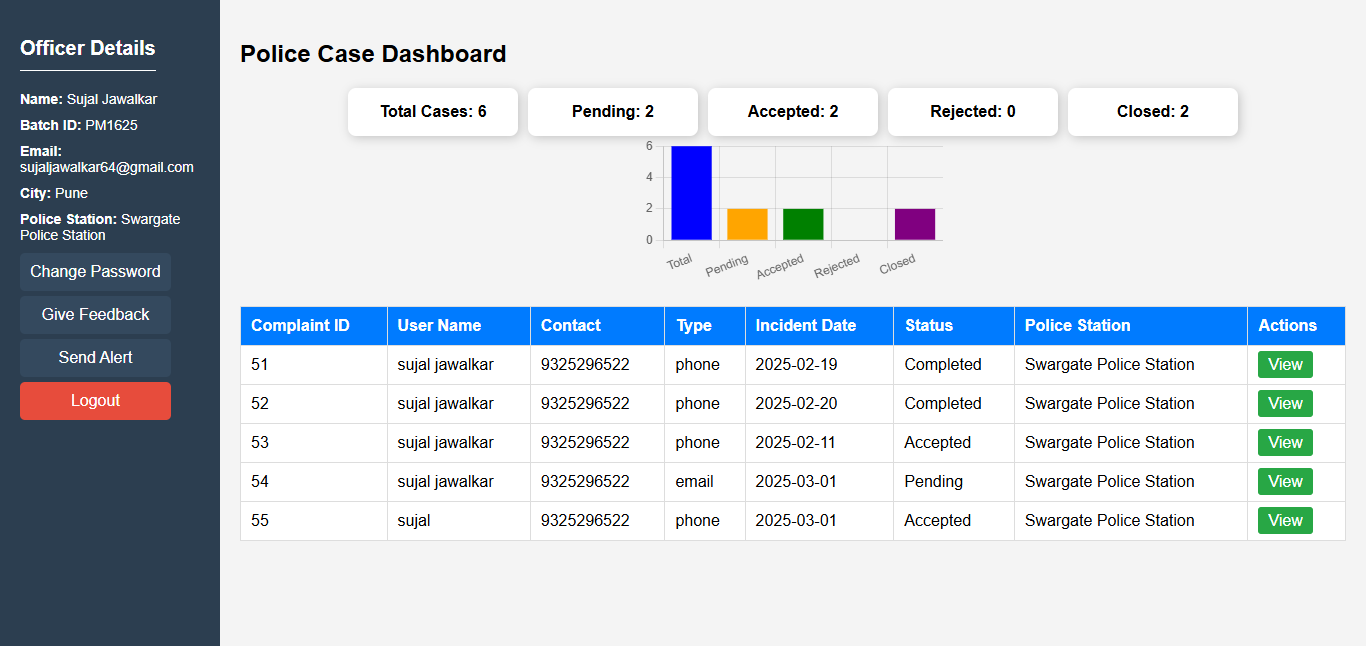
* Case Studies Page-



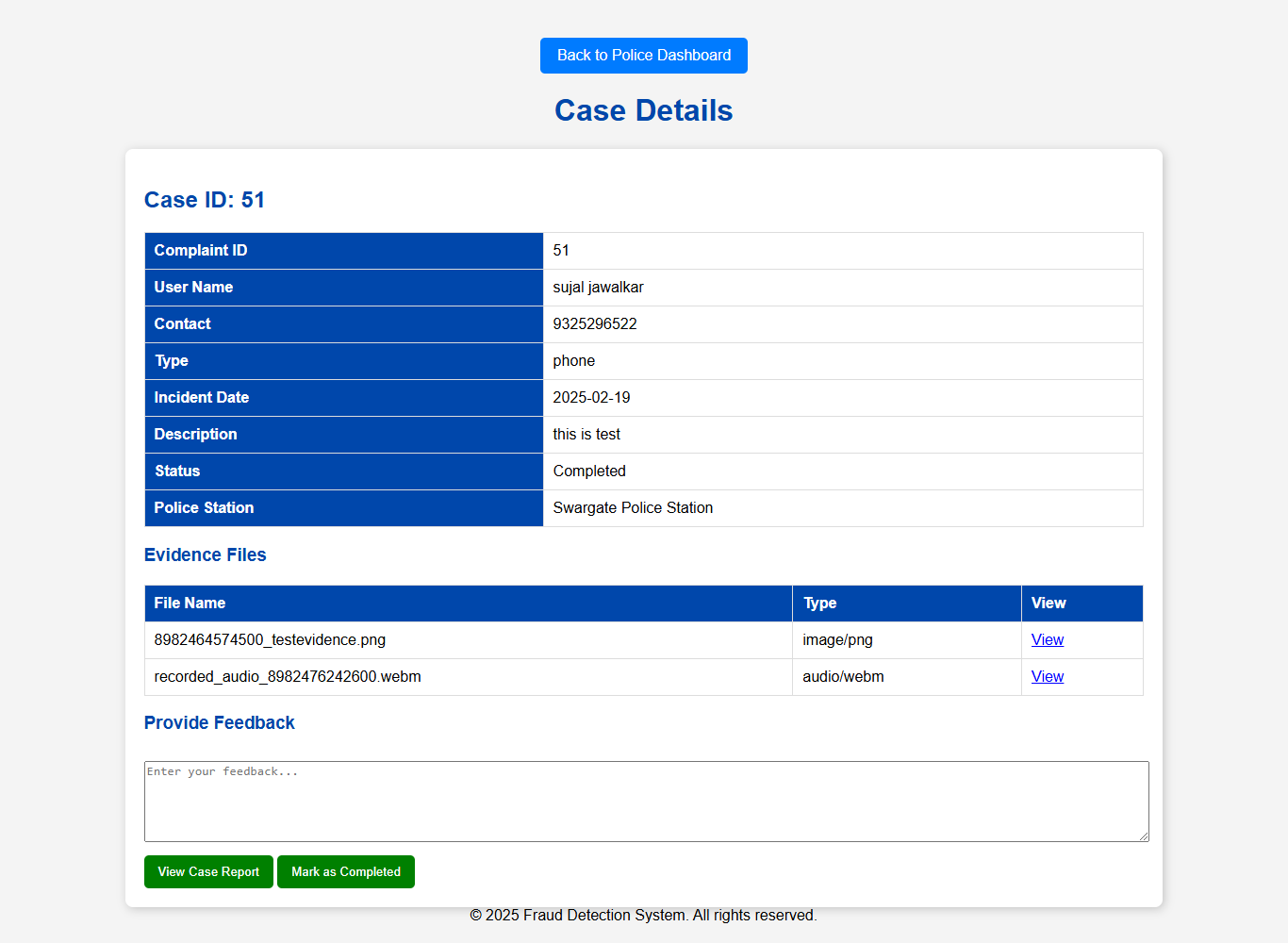
Dashboard Page



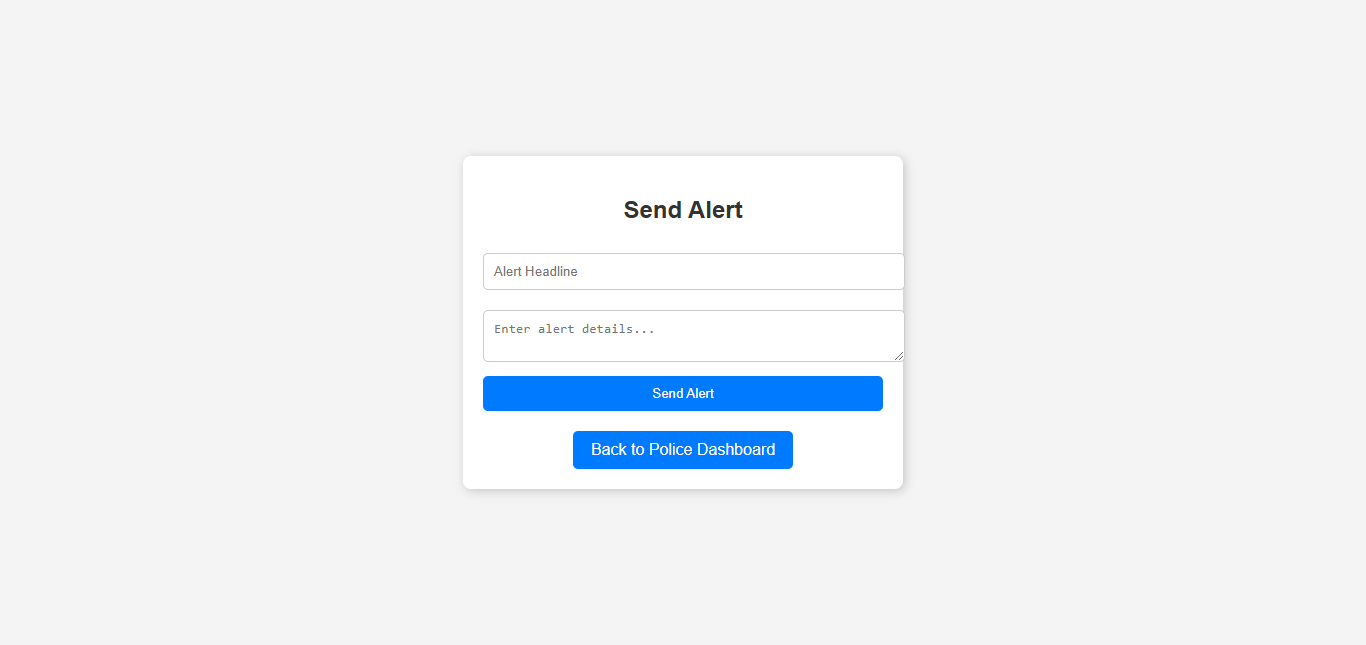
* Police UI

Police Dashboard Page

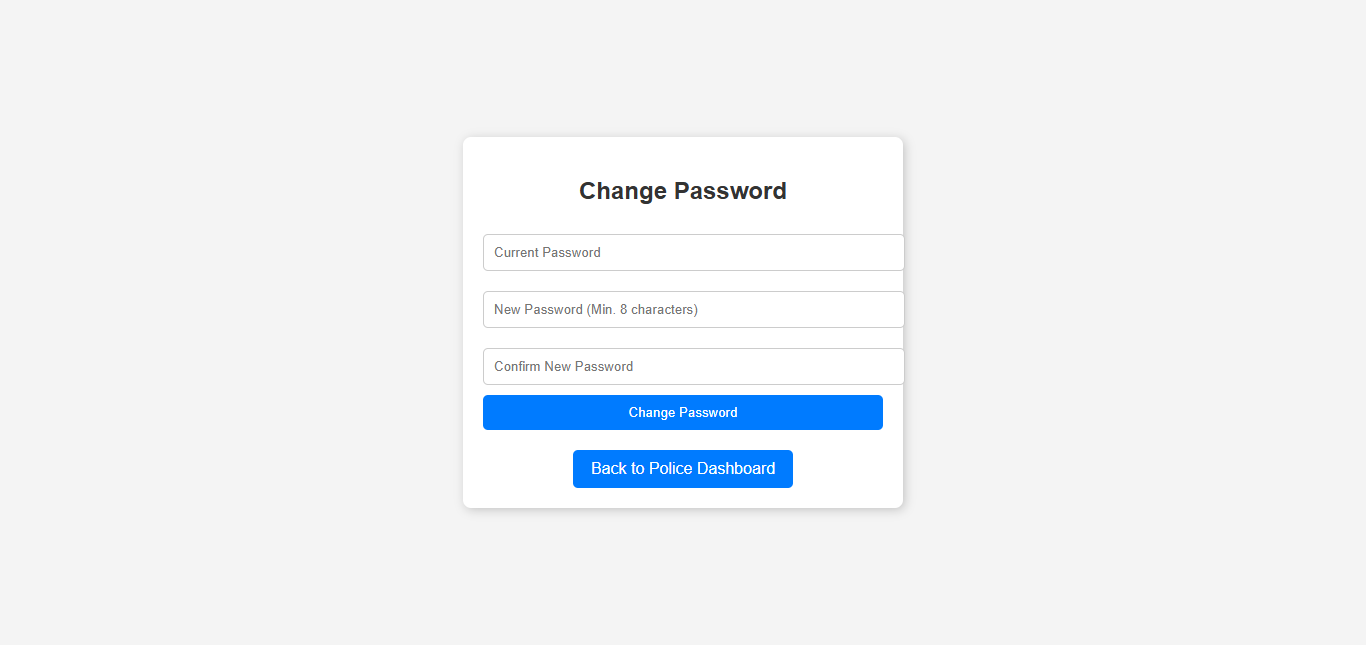
View Case Report/Information page



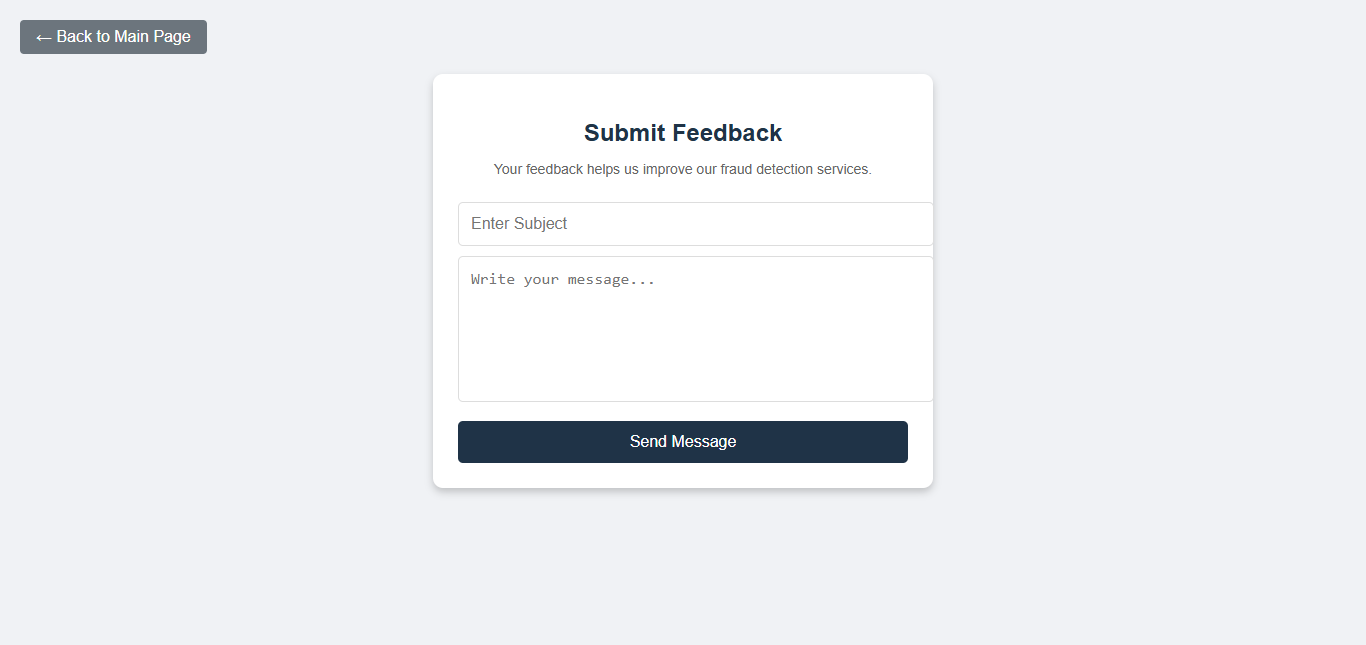
Send Alert Page



Change Password Page



Police Feedback Page



* Admin UI

Admin Login

**Implementation details**

* **Hardware:**

Device name DESKTOP-U2CD0F9

Processor Intel(R) Core (TM) i3-1005G1 CPU @ 1.20GHz 1.19 GHz

Installed RAM 20.0 GB (19.8 GB usable)

System type 64-bit operating system, x64-based processor

* **Tool & Software:**
* **Eclipse**
* **SQL Workbench**

**OUTPUT AND REPORT TESTING**

* **Test Plan**
* Introduction

This test plan ensures the reliability, security, and functionality of the Fraud Detection Website by covering manual and automation testing for core modules:

* Complaint Page
* Registration Page
* Login Page
* Report Page

Testing includes functional, UI, security, performance, and usability testing.

* **Testing Approach**
* Manual Testing

Functional Testing: Verifies correct system behavior.

UI Testing: Ensures responsiveness and consistency.

Security Testing: Tests for vulnerabilities (SQL Injection, XSS).

Performance Testing: Tests system load handling.

Usability Testing: Ensures ease of use.

* Automation Testing

Automates regression and high-priority test cases using Selenium, TestNG, JMeter, and Postman.

Runs tests on a CI/CD pipeline (Jenkins/GitHub Actions).

Generates reports using Extent Reports/Allure.

* **Test Environment**

|  |  |
| --- | --- |
| Frontend | JSP, HTML, CSS, JavaScript |
| Backend | Java (JSP & Servlets) |
| Database | MySQL |
| Browser | Chrome |
| Device | Desktop |

* **Test Scenarios**

|  |  |  |
| --- | --- | --- |
| Module | Test Scenario | Manual & Automation |
| Registration | Register with valid details | Manual |
| Registration | Register with invalid details | Manual |
| Login | Login with valid credentials | Manual & Automation |
| Login | Login with invalid credentials | Manual & Automation |
| Complaint Page | Submit a complaint with text and check Function validation | Manual |
| Report page | Submit a report with text and check Function validation | Manual & Automation |

* **Manual testing**

**1** **Registration Page - Test Cases (Positive):**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TC**  **ID** | **TC\_Name** | **Tester name** | **Objective** | **Precondition** | **Steps to Follow** | **Test Data** | **Expected Result** | **Actual Result** | **Status** |
| REG-01 | Registration Page Load | Sujal | Verify that the registration page loads correctly | User must navigate to the registration page | 1. Open the browser. 2. Enter the URL for the registration page. 3. Wait for the page to load. | N/A | The page should load with all fields visible. | The page should load with all fields visible. | Valid |
| REG-02 | Required Fields Validation | Sujal | Ensure mandatory fields are validated | User must be on the registration page | 1. Click the "Register" button without filling any fields. | N/A | The system should display validation messages ."Please fill out fields." | The system display validation messages ."Please fill out fields." | Valid |
| REG-03 | Email Format Validation | Sujal | Ensure only valid email formats are accepted | User must be on the registration page | 1. Enter an incorrect email format (e.g., "email.com", "user@"). 2. Click "Register". | Invalid email formats ,"email.com", "user@" | The system should show an error message like "Please include an @ in the email address. 'email.com is missing an @". | The system shows an error message like "Please include an @ in the email address. 'email.com is missing an @". | Valid |
| REG-04 | Password and Confirm Password Match | Sujal | Ensure passwords match during registration | User must be on the registration page | 1. Enter different passwords in the "Password" and "Confirm Password" fields. 2. Click "Register". | Different passwords | The system should show an error message like "Passwords do not match. Please re-enter." | The system shows an error message like "Passwords do not match. Please re-enter." | Valid |
| REG-05 | Successful Registration | Sujal | Ensure users can successfully register | User must be on the registration page | 1. Enter valid details. 2. Click "Register". | Valid user details | The system should create an account and redirect to login page should show "Registration successful! Please log in." | The system created an account and redirect to login page should show "Registration successful! Please log in." | Valid |
| REG-06 | Email Confirmation | Sujal | Ensure users receive a confirmation email after registration | User must register successfully | 1. Complete registration with valid details. 2. Check the registered email. | Valid email | The system should send a confirmation email with a welcome message | The system should send a confirmation email with a welcome message | Valid |
| REG-07 | Duplicate Email Check | Sujal | Ensure users cannot register with an already registered email | User must be on the registration page | 1. Enter an email already used for registration. 2. Click "Register". | Existing email | The system should show an error message like "Email already registered. Please log in.". and redirect to login page | The system shows an error message "Email already registered. Please log in.". and redirected to login page | Valid |

**2 Login Page - Test Cases (Positive):**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TC\_ID** | **TC\_Name** | **Tester Name** | **Objective** | **Precondition** | **Steps to Follow** | **Test Data** | **Expected Result** | **Actual Result** | **Status** |
| LOG1 | Login Page Load | Khushdil | Verify that the login page loads correctly | User must navigate to the login page | 1. Open the browser. 2. Enter the URL for the login page. 3. Wait for the page to load. | N/A | The page should load with all fields visible. | The page loads with all fields visible. | Valid |
| LOG2 | Required Fields Validation | Khushdil | Ensure mandatory fields are validated | User must be on the login page | 1. Click the "Login" button without entering any details. | N/A | The system should display validation messages for required fields like "Please fill out fields". | The system display validation messages for required fields like "Please fill out fields". | Valid |
| LOG3 | Email Format Validation | Khushdil | Ensure only valid email formats are accepted | User must be on the login page | 1. Enter an incorrect email format (e.g., "email.com", "user@"). 2. Click "Login". | Invalid email formats | The system should show an error message like "Please include an @ in the email address. 'email.com is missing an @". | The system shows an error message like "Please include an @ in the email address. 'email.com is missing an @". | Valid |
| LOG4 | Incorrect Credentials | Khushdil | Verify login fails for incorrect credentials | User must be on the login page | 1. Enter an incorrect email and password. 2. Click "Login". | Invalid email & password | The system should show an error message like "User not found. Please register". | The system shows an error message like "User not found. Please register". | Valid |
| LOG5 | Incorrect Password | Khushdil | Verify login fails for incorrect Password | User must be on the login page | 1. Enter an correct email and incorrect password. 2. Click "Login". | Invalid email/password | The system should show an error message like "Invalid email or password". | The system shows an error message like "Invalid email or password". | Valid |
| LOG6 | Successful Login | Khushdil | Ensure users can log in with valid credentials | User must be on the login page | 1. Enter a valid email and password. 2. Click "Login". | Valid email/password | The system should log in the user and redirect them to the dashboard. | The system should log in the user and redirect them to the dashboard. | Valid |
| LOG7 | Password Reset Link | Khushdil | Verify password reset functionality | User must be on the login page | 1. Click "Forgot Password?". 2. Enter a registered email. 3. Click "Submit". | Registered email | The system should send a OTP to the user's email. | The system sends a OTP to the user's email. | Valid |

**3 Report Page - Test Cases (Negative):**

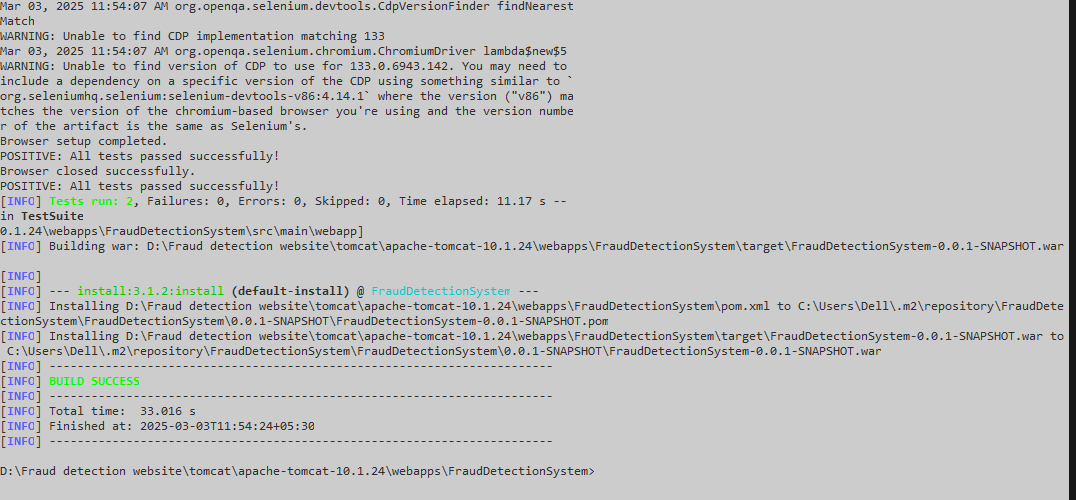
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TC\_ID** | **TC\_Name** | **Tester Name** | **Objective** | **Precondition** | **Steps to Follow** | **Test Data** | **Expected Result** | **Actual Result** | **Status** |
| R01 | Page Load Verification | Khushdil | Verify that the report fraud page loads correctly | User is on the website and User must be logged in | Open the "Report Fraud" page | N/A | The page should load with all fields visible | The page load with all fields visible | Valid |
| R02 | Required Fields Validation | Khushdil | Check if required fields validation is working | Report Fraud form is open | Try submitting the form without filling in any details | N/A | System should display validation messages for required fields | System displays validation messages for required fields | Valid |
| R03 | Phone Number Format Validation | Khushdil | Ensure only valid phone numbers can be submitted | Report Fraud form is open | Enter an invalid phone number (e.g., "1234", "abcdef") and submit | "1234","abcdef” | System should show an error message like "Enter a valid phone number" | Form submitted without error | Invalid |
| R04 | Successful Fraud Report Submission | Khushdil | Ensure that valid reports are submitted correctly | Report Fraud form is open | Enter valid details and click "Submit" | Valid phone number/website | System should display a success message and store the report in the database | System displays an error message and did not store the report in the database | Invalid |
| R05 | Confirmation Message After Submission | Khushdil | Check if confirmation is displayed after submitting | Report Fraud form is open | Submit a valid report | Valid Report Data | System should display details of submitted report | System displays an error message | Invalid |

1. **Complaint Page - Test Cases (Positive):**

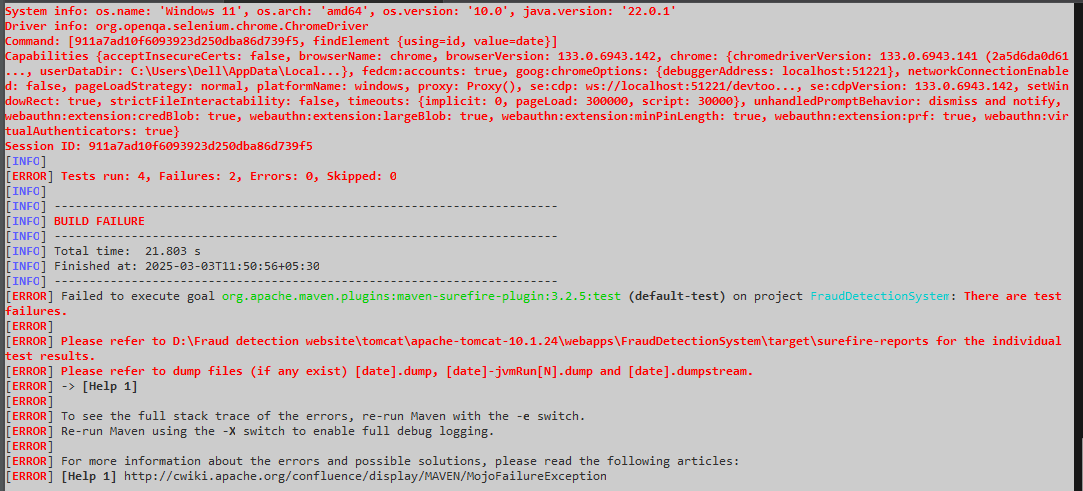
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TC\_ID** | **TC**  **Name** | **Tester Name** | **Objective** | **Precondition** | **Steps to Follow** | **Test Data** | **Expected Result** | **Actual Result** | **Status** |
| C1 | Complaint Page Load | Sujal | Verify that the complaint page loads correctly | User must be logged in | 1. Open the browser. 2. Enter the URL of the complaint page. 3. Wait for the page to load. | N/A | The page should load with all fields visible. | The page load with all fields visible. | Valid |
| C2 | Required Fields Validation | Sujal | Ensure mandatory fields are validated | User must be on the complaint page | 1. Click the "Submit" button without entering any details. | N/A | The system should display validation messages for required fields."Please fill out fields." | The system displays validation messages for required fields."Please fill out fields." | Valid |
| C3 | Valid Phone Number Format | Sujal | Ensure only valid phone numbers are accepted | User must be on the complaint page | 1. Enter an invalid phone number (e.g., "1234", "abcdefgh"). 2. Click "Submit". | Invalid phone numbers | The system should show an error message like "Please enter a valid contact number". | The system shows an error message like "Please enter a valid contact number". | Valid |
| C5 | File  Upload | Sujal | Verify the upload functionality for files | User must be on the complaint page | 1. Click on the "Upload Evidence" option. 2. Select a valid audio file (.mp3, .wav). 3. Click "Submit". | Valid files like .mp3, .wav, jpeg,  png,  pdf | The system should accept the file and allow submission. | The system accepts the file and allow submission. | Valid |
| C7 | Successful Complaint Submission | Sujal | Ensure users can successfully submit a complaint | User must be on the complaint page | 1. Fill in all required details. 2. Click "Submit". | Valid complaint details | The system should display a success message with case details and store the complaint in the database. | The system displays a success message with case details and store the complaint in the database. | Valid |
| C8 | Complaint Reference Number Generation | Sujal | Verify that a unique reference number is generated | User must submit a complaint successfully | 1. Submit a complaint with valid details. 2. Observe the confirmation message. | Valid complaint details | The system should generate and display a unique reference number for tracking. | The system generates and display a unique reference number for tracking. | Valid |
| C10 | Email Confirmation | Sujal | Verify that users receive an email confirmation after submitting a complaint | User must submit a complaint successfully | 1. Submit a complaint. 2. Check the registered email. | Valid email | The system should send a confirmation email with complaint details. | The system sends a confirmation email with complaint details. | Valid |
| C11 | Redirection After Submission | Sujal | Ensure users are redirected after submitting a complaint | User must submit a complaint successfully | 1. Submit a complaint. 2. Observe the page response. | Valid complaint details | The system should redirect the user to a case details page and 2 buttons of Dashboard and submit another complaint . | The system redirect the user to a case details page and 2 buttons of Dashboard and submit another complaint . | Valid |

* **Automation Testing**

Positive test

****

Negative test:

****

**Conclusion & Recommendations**

The Fraud Complaint Guidelines System is a comprehensive digital platform designed to guide users in fraud prevention, reporting fraudulent activities, and seeking assistance from law enforcement. This system significantly reduces the time and effort required for individuals to find reliable information on fraud prevention and provides a streamlined process for reporting fraudulent websites, phone numbers, and scams. The dedicated police portal ensures efficient management of complaints, enabling law enforcement to review, approve, or reject cases promptly. With an intuitive user interface, the system empowers users to take proactive steps against fraud, enhancing overall digital safety and awareness.

The system addresses critical challenges associated with traditional fraud reporting methods, such as lack of accessibility, delayed complaint resolution, and limited public awareness. Features like real-time notifications, secure communication channels, multilingual support, and role-based access control ensure the platform is user-friendly, secure, and inclusive.

**Recommendations:**

* Public Awareness Campaigns:

Launch awareness programs to educate users on the importance of fraud prevention and how to use the platform effectively.

* Collaboration with Financial and Telecom Sectors:

Partner with banks and telecom companies to quickly identify and block fraudulent transactions and suspicious phone numbers.

* Integration with National Cybercrime Portals:

Link the system with national cybercrime portals for faster complaint escalation and resolution.

* Regular Security Updates:

Conduct regular security audits and updates to protect the system from evolving cyber threats.

* Advanced Analytics:

Implement data analytics to identify emerging fraud patterns and provide law enforcement agencies with actionable insights.

* Mobile Application Development:

Develop a mobile application for easier access, enabling users to report fraud and receive alerts on the go

**Future Scope**

**Key Future Enhancements:**

* Advanced Personalization: AI-Driven Recommendations: Implement AI algorithms to deliver personalized fraud prevention tips and alerts based on user behaviour, past reports, and regional fraud trends.
* Predictive Analytics: Use predictive models to anticipate emerging fraud patterns and warn users in advance, enabling proactive fraud prevention.

**Integration with Emerging Technologies**:

* Blockchain Technology: Utilize blockchain for secure storage of complaint data, ensuring transparency and tamper-proof tracking of case progress.
* AI-Powered Chatbots: Introduce intelligent chatbots and virtual assistants to provide real-time user support, guide users through the fraud reporting process, and answer common queries.

**Expanded Communication Channels:**

* Social Media Integration: Enable reporting and fraud alerts through popular social media platforms like Facebook, Twitter, WhatsApp, and Telegram for broader reach.
* Voice-Based Support: Incorporate voice-based notifications and assistance, making the platform accessible to users with limited literacy skills or visual impairments.

**Mobile App Enhancements:**

* Offline Access: Allow users to download essential fraud prevention guides, complaint forms, and status updates for offline access.
* Location-Based Alerts: Use GPS-enabled features to notify users of fraud incidents or risks specific to their geographic location, along with nearby police stations or cyber cells for immediate help.

**Collaboration and Partnerships:**

* Integration with National Portals: Collaborate with national cybercrime reporting portals and law enforcement agencies for seamless complaint transfers and faster resolution.
* Financial and Telecom Partnerships: Work with banks and telecom providers to automatically flag suspicious transactions and block fraudulent numbers reported through the platform.

**Enhanced Security Features:**

* Multi-Factor Authentication (MFA): Implement advanced security measures like biometrics and OTP-based logins to protect user accounts.
* Real-Time Threat Intelligence: Integrate with threat intelligence platforms to provide real-time alerts about large-scale fraud attempts or cyber threats

**Bibliography and References**

Batrachenko, T., Lehan, I., Kuchmenko, V., Kovalchuk, V., & Mazurenko, O. (2024). Cybercrime in the context of the digital age: analysis of threats, legal challenges, and strategies. In *Multidisciplinary Science Journal* (Vol. 6). Malque Publishing. https://doi.org/10.31893/multiscience.2024ss0212

Boulieris, P., Pavlopoulos, J., Xenos, A., & Vassalos, V. (2024). Fraud detection with natural language processing. *Machine Learning*, *113*(8), 5087–5108. https://doi.org/10.1007/s10994-023-06354-5

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). *Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking*. https://doi.org/10.22541/au.166385206.63311335/v1

Mishra, S., & Soni, D. (2023). DSmishSMS-A System to Detect Smishing SMS. *Neural Computing and Applications*, *35*(7), 4975–4992. https://doi.org/10.1007/s00521-021-06305-y

Mughaid, A., AlZu’bi, S., Hnaif, A., Taamneh, S., Alnajjar, A., & Elsoud, E. A. (2022). An intelligent cyber security phishing detection system using deep learning techniques. *Cluster Computing*, *25*(6), 3819–3828. https://doi.org/10.1007/s10586-022-03604-4