Fall 2025

Software Requirements Specification

SENTRA

Ryaan Farrukh

Kencho Lodhen

Anand Krishna Anil Kumar

Github:

https://github.com/rfarrukh0/Sentra

Executive Summary

0.1 Background

The proposal introduces a centralized fraud detection platform designed to empower smaller fintech firms and startups to collectively combat rising fraud and scams in the digital finance sector, with features for collaborative intelligence-sharing, machine learning-based detection, and secure integration. Fraud losses in the U.S. financial sector reach as much as $20 billion annually, with smaller fintech firms and startups disproportionately affected due to lack of advanced tools. Isolated systems allow fraudsters to repeat their methods across companies, making collaboration essential.

0.2 Description

0.3 Company Value Add

Participating companies gain enhanced fraud detection capabilities without the need to individually invest in advanced infrastructure. The system also reduces operational and reputational risk by blocking fraudsters more quickly and efficiently.

0.4 End-User Value Add

Customers experience a reduced risk of financial loss and identity theft, as well as higher overall confidence in digital banking platforms, thanks to enhanced fraud prevention and industry-wide protections.

0.5 Scope

0.5.1 What is Included

- Collaborative fraud intelligence sharing
- Real-time monitoring and alerting
- Machine learning-powered anomaly detection
- Secure APIs for onboarding fintech partners
- Web dashboard for reporting and visualization

0.5.2 What is Not Included

- Direct access to raw customer data between firms
- Out-of-industry use cases (e.g., non-financial industries)
- Legacy integration with non-digital banking tools
- On-premises deployment (cloud-based only)

0.6 Justification

The two-semester scope is justified by the project's complexity: integrating diverse data sources, designing robust ML and API solutions, ensuring security and privacy compliance, and creating operational front/back-end components. The platform delivers significant value by reducing fraud, safeguarding customers, and elevating industry standards for trust and security.

Table of Contents

Section 1

1.1 Document Authors

Ryaan Farrukh
Kencho Lodhen
Anand Krishna Anil Kumar

1.2 Document Revision History

WEEK	DATE	Revisions
1	September 10 - 11, 2025	• Made the business proposal
2	September 17 – 18, 2025	• Entire SRS section 1 and section 2.1
3	Sept 24, 2025	• SRS Section 2.2-2.5 draft + revision of previous sections, Finished up SRS section 2
4	Oct 1, 2025	• Began function requirements and NFR draft
5	Oct 4, 2025	• Finished sections 2.6, and 2.7
6		•
7		•
8		•
9		•
11		•
12		•
13		•
14		•

1.3 Document Purpose

This Software Requirements Specification (SRS) defines the purpose, scope and objectives of Sentra. Sentra is a centralized fraud detection platform, and this document provides a shared reference for the team, instructors and shareholders guiding development over PRJ566 + PRJ666

1.4 Audience

The audience includes:

- Course Instructor
- Team Members
- Industry Stakeholders

1.5 Group Agreement

Team #: Group 7

Project Title: Sentra – Centralized Fraud Detection Platform

Project Time Frame: September 2025 - April 2026 2 Semesters (8 months)

Team Members

Ryaan Farrukh
Kencho Lodhen
Anand Krishna Anil Kumar

Team Leadership

Ryaan Farrukh (Project Lead)

Team Functions/Roles

Ryaan Farrukh – Project Manager and Machine Learning developer

Kencho Lodhen – Backend development and API integration

Anand Krishna Anil Kumar – UI + UX Designer and Documentation

Team Meetings

Weekly online via MS Teams (Saturday 3pm) + bi-weekly in-class check-ins.

Team Problems

Limited team size increases workload between members.

Team Commitment

The undersigned members agree to work together on the project until the end of the PRJ666 next Semester. They recognize that as a team and individually they are equally responsible for the quality of all deliverables.

Name	Date	Signature
Ryaan Farrukh	September 18, 2025	R.F
Kencho Lodhen	September 18, 2025	K.L
Anand Krishna Anil Kumar	September 18, 2025	A.K

Section 2

2.1 Project Proposal

2.1.1 Project Background

As financial services are rapidly digitized, such rapid digitization opens a broader attack surface for fraud. In 2024, consumers reported $12.5B worth of fraud losses to the U.S. Federal Trade Commission, which is up 25% YoY-and the FBI's IC3 has recorded more than $16 billion in cybercrime-related losses [1][2]; this figure is the highest ever reported. Such figures are likely to be underestimations because they are based on voluntary reporting.

Reports within the financial service industry have also shown increases, for example, 1 in 20 verification attempts are flagged as fake and a 21% rise in fraud attempts [3][4]. This highlights just how quickly fraudulent tactics-such as synthetic IDs, credential stuffing, and deepfakes have evolved.

Existing Solutions (what and who they're for):

- ***FICO Falcon Fraud Manager*** - An enterprise-grade platform providing real-time monitoring across transaction types, blending AI/ML models trained with insights gained from the Falcon Intelligence Network, which pulls information from 10,000+ institutions to improve detection whilst reducing false positives. Very powerful, but usually only adopted by large financial institutions. [5]
- ***SAS Fraud Managem****ent* - A comprehensive fraud platform that features machine learning, cross payments and events, real-time scoring and decisioning and alert/case management. Strong capabilities, usually placed in enterprise environments. [6]
- ***Kount (An Equifax Company)*** - AI/ML risk scoring and millisecond decisions. Leverages the Identity Trust Global Network (tens of billions of annual interactions) to assess risk using device, identity, and behavioral signals. More common in e-commerce/fintech onboarding and payments. [7]
- ***NICE Actimize (Enterprise Fraud Management / IFM-X)*** - Real-time cross-channel fraud prevention with AI-driven analytics and end-to-end case management with widespread adoption through mid-to-large financial institutions. [8]

Feature Comparison: focus on beneficial features

Product	Target Users	Cost/ Accessibility	Ease of Intergration	Intelligence pool	Typical deployment	Intergration with small FinTech
FICO Falcon	Huge firms	High	Complex	Yes	Enterprise	None
SAS Fraud Mgmt	Large enterprise	High	Complex	Not stated	Enterprise	Limited
Kount	Large Fintech	Medium	Moderate	Minimal	Cloud	Moderate
NICE Actimize	Mid-large banks	High	Complex	Not stated	Enterprise	Limited
Sentra	Small fintech	Low, Startup friendly	Easy, Simple APIS	Yes, Open cross firm sharding	Cloud	Strong

The existing offerings are all very effective, but they are mostly enterprise centric. Some of them use vendor-run networks (FICO, Kount) for sharing, but access is tied to purchasing their entire enterprise platforms, making them quite costly and complicated for small firms. There is little that pertains to open, collaborative sharing geared toward small fintech. Sentra fills this very gap with simple, privacy-respecting, cross-firm intelligence sharing and right-sized integrations for startups and small institutions. [5][7]

2.1.2 Problem Statement

Who has the problem?

- **Primary:** Smaller fintechs/startups that do not have the advantage of large bank budgets, data network effects and operational manpower.
- **Secondary:** Their customers (in terms of identity theft and direct financial loss) and regulators/industry (systemic risk and reputational loss). Record-level national loss figures and sector-specific spikes show the burden is meaningful and rising. [1][2][3]

Why is it important?

Losses keep increasing and the attacks are becoming increasingly sophisticated (synthetic identities, deepfakes, real-time payment scams), eroding customer confidence and increasing operational and regulatory pressure on smaller providers. [4]

Why existing solutions don’t solve it for small fintech?

- Fit and complexity: These platforms are built for very large enterprise deployment.[6][8]
- Access to pool: Where networks do exist (e.g., Falcon Intelligence Network; Kount's Identity Trust Global Network), they are tied to those vendors' stacks, creating a barrier for small teams trying to build an open, cross-firm hub. [5][7]
- Isolation in practice: Many solutions still stress single-institution monitoring; vendor pages say nothing about shared, peer-to-peer intelligence exchanges designed for small fintech participation. [6][8]

2.1.3 Product Vision

Sentra is a cloud-based centralized fraud detection platform for smaller fintech firms that:

- Allows for a collaborative intelligence regarding fraud (preservation of the privacy of patterns, entities, and behavior/device fingerprints) so repeated attacks will be blocked among participants.
- Provides ML-based anomaly detection in real time together with risk scores through secure APIs, along with a dashboard for analysts/compliance to investigate the alerts and trends.
- Emphasizes integration as well as security and compliance (encryption in transit/at rest, audit trails, and data minimization).

Vision: The most trusted fraud-intelligence hub for small fintech that turns an isolated defense into collective defense and reduces time-to-signal from weeks to minutes.

Main value: Losses and false negatives are reduced through pooled network effects, while costs/complexities lessen for smaller teams, improving customer protection and customer trust.

2.2 Stakeholders and Users

Internal:

- Project Lead (Ryaan Farrukh): Manages team activities, coordinates project timelines, ensures all deliverables meet QA standards and communicates with faculty.

- Backend Developer (Kencho Lodhen): Develops the fraud detection engine, handles integration with APIs and manages backend infra.
- UI/UX Designer (Anand Krishna Anil Kumar): Designs web dashboards, ensures user friendly interfaces and maintains clear project documentation.
- Testing and QA (shared): Each team member is responsible for individual and shared testing including unit and integration testing. Each member will also contribute to the validation and training of ML models.

External:

- Partner Fintech businesses: Benefits directly from shared fraud intelligence by reducing losses and risk.
- Incubators/Accelerators: Interested in supporting and innovative fraud prevention solution that can strengthen future fintech startups allowing higher success rates.
- Developers at Partner Firms: Intergration with our solution with existing fintech systems.
- Regulators: Ensures that platform complies with financial regulations and standards.
- End customers (indirect): Customers experience safer transactions and reduced risk of theft.

2.3 Project Scope

In Scope

- Development of Sentra's centralized fraud detection platform.
- Design and implementation of ML models for detection and risk scores.
- Creation of secure APIs for fintech firms to integrate with.
- Development of a web dashboard to monitor, report and visualize anomalies and data.
- Incorporation of encryption and data minimizations to reduce overall risk.
- Full system documentation from system design, architecture and usage guides.

Out of Scope

- On premises deployment (Our solution will be cloud based).
- Legacy systems integration beyond APIs.
- Development of any mobile application for end consumers.
- Services for non-financial industries.

2.4 System Risks

Privacy Risk

- Exposure of sensitive financial and customer data if encryption or access controls are not properly developed and implemented.

Integration Risk

- Partner fintech firms may use different data forms or incompatible APIs causing onboarding and integration issues, furthering workloads and possibly delayed deadlines.

Model Risk

- ML models may produce false positives/negatives reducing reliability and accuracy to determine real fraud attempts.

Adoption Risk

- Small fintechs may hesitate to share sensitive information due to competition, cost or uncertainty in solution.

Scalability Risk

- Large volumes of data processing could overwhelm resources if cloud services and scaling are not properly optimized or configured resulting in high latency or system downtimes.

Security Risk

- Potential for breaches or exploitation by attackers in attempts to manipulate fraud signals and/or to bypass detection systems

Regulatory Risk

- Lack of compliance with global and national stands could result in fines, reputation damage or at worse consequences such as being shut down altogether

2.5 Operating Environment

Hosting Environment

- Sentra will be deployed on a secure cloud infra (AWD, Azure or GCP) to maintain scalability requirements and uptime

Client Access

- End users will access the system through a web-based dashboard that runs on standard browsers (Chrome, Edge, Firefox, Safari)
-

Integration

- Partner firms will connect through a REST API secured with TLS encryption and OAuth authentication

Supported Platforms

- Platform APIs will be designed to integrate with modern tech stacks (Python, Node.js Java)

Security

- The development and operating environment must comply with the financial security requirements such as PCI DSS (Payment Card Industry Data Security Standard) and data regulations such as GDPR (General Data Protection Regulation)

Data Managment

- Logs, fraud alerts and models will all be secured in an encrypted large-scale database hosted in the cloud with automated backups.

2.6 Functional Requirements

2.6.1 Requirements Gathering Process

To identify all the functional and nonfunctional requirements for our solution, we simulated interviews with key personnel. These personas reflect real users who will interact or benefit from the system we create.

Person 1: Fraud Analyst (External User)

- Role: Reviews alert and investigates them
- Goal: Needs accurate and quick alerts to act quickly
- Frustrations: Current systems produce too many false alerts and too cluttered

Sample Interview Q&A

- *Q: How quickly do you need alerts?*
  A: "Within seconds, otherwise the fraudster can get away"
- *Q: What information do you need in an alert*
  A: "Transaction details, risk scores and why it was flagged"
- *Q: What is frustrating in dashboards*
  A: "Too many extra screens, I need a clean and simple dashboard"

Keywords -> Requirements

- "Within seconds" -> NFR1: System should return fraud risk scores within 2 seconds
- "Risk score and reasons" -> FR6: APIs should return risk scores and reasons
- "Clean and simple" -> FR8: Dashboard should show alert simple with summary

Person 2: Compliance Officer (External User)

- Role: Makes sure fraud reporting meets legal and regulatory requirements
- Goal: Needs accurate and exportable reports and full audit trails.
- Frustrations: Manual reporting wastes time and the logs are incomplete

Sample Interview Q&A

- *Q: What do you need most for compliance?*
  A: “Exportable reports with timestamps.”
- *Q: What helps with audits?*
  A: “Complete logs of every fraud event and action.”

Keywords -> Requirements

- “Exportable reports” -> FR10: Generate compliance reports
- “Complete logs” ->FR4: Store all alerts and logs in a secure database with audit trails.
- “Compliance” -> NFR5: Comply with PCI DSS and GDPR.

Person 3: Fintech Developer (External User)

- Role: Integrates our APIs into partner systems
- Goal: Needs simple and secure APIs
- Frustrations: Enterprise systems are too complex and difficult to integrate

Sample Interview Q&A

- Q: *What matters most when integrating APIs?*
  A: “They must be secure and return info fast”
- Q: *What slows you down?*
  A: “Inconsistencies in code and poor documentation”

Keywords -> Requirements

- “Secure and fast” -> FR7: APIs should use OAuth 2.0/TLS and respond within 2 seconds.
- “Poor documentation” -> NFR8: Dashboard and APIs should be intuitive and consistent.

Person 4: Project Lead (Internal User)

- Role: Oversees the project and ensures the stability of our system
- Goal: Needs to be scalable and reliable for multiple partners
- Frustrations: Downtime reduces partner trust and scaling issues increases cost

Sample Interview Q&A

- Q: *What is critical for system stability?*
  A: “The system must be scalable for lots of partners”
- Q: *How much downtime is allowed?*
  A: “Almost none, we aim for 99.9% uptime”

Keywords -> Requirements

- “Scale for lots of partners” -> NFR6: System should scale to support 50+ partners.
- “99.9% uptime” -> NFR3: System should provide 99.9% uptime excluding maintenance.
- “Without crashing” -> NFR2: Cloud environment should scale to handle load.

2.6.2 Functional Requirements (FR)

- **FR1:** The system will check transactions in real time to catch anything suspicious.
- **FR2:** If an account or activity looks risky, the system will flag it and create an alert.
- **FR3:** Fintech partners can share fraud info in an anonymous way through the platform.
- **FR4:** Alerts and logs will be stored safely, with records kept for auditing.
- **FR5:** The system will have APIs that partners can use to send data and get results.
- **FR6:** The APIs will give back a fraud score and explain why a transaction was flagged.
- **FR7:** The APIs will be protected with secure login and encryption.
- **FR8:** The dashboard will show alerts in a simple and clear layout.
- **FR9:** The dashboard will let users filter and search alerts by things like partner, date, or score.
- **FR10:** The system will create reports that can be downloaded for compliance or review.
- **FR11:** Different roles will be supported (admin, analyst, partner).
- **FR12:** The system will give admins tools to manage partner firms and users.

2.7 Nonfunctional Requirements

Performance and Reliability

- **NFR1:** Fraud scores will come back within a few seconds.
- **NFR2:** The system will handle lots of requests at once without slowing down.
- **NFR3:** The system will stay up most of the time with very little downtime.

Security

- **NFR4:** All communication and stored data will be encrypted.

- **NFR5:** The system will follow standard rules in the finance industry to keep data safe.

Scalability

- **NFR6:** The system can grow to support more fintech partners as needed.

Usability

- **NFR7:** The dashboard will be easy to use with clear navigation and filters.
- **NFR8:** The system will come with simple, consistent documentation for partners using the APIs.

Data Management

- **NFR9:** Logs and alerts will be kept safely for reporting and audits.
- **NFR10:** Backups will be kept so data isn't lost if something goes wrong.

2.8 UI/UX Interface Mock-ups

References (Section 2)

[1] Federal Trade Commission, "New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024," Mar. 10, 2025. [Online]. Available: https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

[2] Federal Bureau of Investigation, "FBI Releases Annual Internet Crime Report," Apr. 23, 2025. [Online]. Available: https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

[3] Veriff, "Top fraud trends in digital banking for 2025 – and how to stay one step ahead," Jul. 30, 2025. [Online]. Available: https://www.veriff.com/fraud/learn/top-fraud-trends-in-digital-banking-for-2025-and-how-to-stay-one-step-ahead

[4] Veriff, "The growing threat of deepfakes in financial services and why a trust infrastructure is the future," Aug. 20, 2025. [Online]. Available: https://www.veriff.com/identity-verification/the-growing-threat-of-deepfakes-in-financial-services-and-why-a-trust-infrastructure-is-the-future

[5] FICO, "FICO® Falcon® Fraud Manager," [Online]. Available: https://www.fico.com/en/products/fico-falcon-fraud-manager

[6] SAS, "SAS Fraud Management," [Online]. Available: https://www.sas.com/en_us/software/fraud-management.html

[7] Kount (Equifax), "Fraud Detection Software / Identity Trust Platform," [Online]. Available: https://kount.com/fraud-detection-software

[8] NICE Actimize, “Enterprise Fraud Management,” [Online]. Available: https://www.niceactimize.com/fraud-management

Section 3

3.1 Data Flow Diagrams

3.2 Iser Stories and related Use Case Scenarios

3.3 Activity Diagrams

3.4 Business Rules

Business Rule #	Description	Activity Diagram	Related UCS	UI Mock-up
BR1		AD1	UC1	UI 2.7.2
BR2		AD2	UC2	UI 2.7.3
BR3		AD3	UC3	UI 2.7.4
BR4		AD3	UC3	UI 2.7.4
BR5		AD5	UC4	UI 2.7.6
BR6		AD6	UC5	UI 2.7.6
BR7		AD7	UC6	UI 2.7.7
BR8		AD8	UC7	UI 2.7.8
BR9		AD8	UC7	UI 2.7.8
BR10		AD8	UC7	UI 2.7.8
BR11		AD8	UC7	UI 2.7.8
BR12		AD8	UC7	UI 2.7.8
BR13		AD9	UC8	UI 2.7.9
BR14		AD9	UC8	UI 2.7.9
BR15		AD9	UC8	UI 2.7.9
BR16		AD9	UC8	UI 2.7.9
BR17		AD10	AD9	UI 2.7.9
BR18		AD10	AD9	UI 2.7.9
BR19		AD10	AD9	UI 2.7.9
BR20		AD11	UC10	UI 2.7.10
BR21		AD11	UC10	UI 2.7.11
BR22		AD11	UC10	UI 2.7.11
BR23		AD12	UC11	UI 2.7.10
BR24		AD13	UC12	UI 2.7.12

Section 4 – Domain Class

Section 5 – Database

Section 6 – Project Management

6.1 Work Breakdown Structure

6.2 Milestones & Acceptance Criteria

Section 7 – Product Backlog & Implementation Schedule

Section 8 – Client/Faculty Sign-off