|  |  |
| --- | --- |
| **Name of the Document** | **[UNITE HUB Application - Fraud Risk Management - Banks]** |
| **Version** | 1.0 |
| **Date** | 21st Apr-25 |
| **Document ID** | UH001 |

**Executive Summary:**

Developing an advanced Fraud Risk Management System leveraging a Risk rule engine for real-time fraud detection, prevention, and reporting. The system ensures regulatory compliance, mitigates financial risks, safeguards customer trust, integrates seamlessly with banking infrastructure, and reduces manual intervention, creating a secure operational environment.

**Phase 1:**

Focused on analysing NCRP complaint data under the I4C initiative, the system detects suspicious patterns in transactions and beneficiaries. It generates actionable insights and alerts banks for timely remedial action, fostering collaboration between NCRP and banks to strengthen fraud prevention and enhance financial security.

**Scope of This Document:**  
The system will encompass two core modules:

1. **I4C Complaints and Investigations** (For both Victim and Beneficiary ) , This will be Cases originating from i4c to Banks for Victim and Beneficiary.
2. **Risk Rule Engine Detection** of following Financial and Non-Financial Transactions where System will identify The below scenarios and alert the Banks on Potential Frauds.
   1. **Payment Related transactions**
   2. **Onboarding-related**
   3. **New Beneficiary Additions**

These modules will integrate reporting and analytics for actionable insights, ensuring adaptive fraud management, regulatory compliance, and a secure financial ecosystem.

**System level Workflow chart:**

**File Attached :**

****

**Brief Workflow for Complaint Handling and Dedupe in Unite Hub**

**Simplified Workflow for Complaint Handling and Deduplication in Unite Hub**

**Step 1: Complaint Data Ingestion**

* Complaints arrive at the I4C Repository through email, web portal, or API.
* The bank enters complaint details into the Unite Hub Portal (either manually or via API).
* At the same time, Unite Hub sends the data to the Net Base Registry for deduplication and quick threat checks.

**Step 2: Data Entry**

* Data Capture Specialists enter complaint details into Unite Hub for cases received by email or web portal.
* If the API is used, complaint data goes directly into Unite Hub.

**Step 3: Case Classification & Review**

* Unite Hub classify complaints as either "Victim" or "Beneficiary" cases basis cases received from Data entry portal and send to Case Review screen (Que) as separate case ids.
* Risk officers review each case, checking transaction and customer details from the bank’s core system.

**Workflow Example :**

1. Complaint Received: I4C routes the complaint to the relevant bank, including both victim and beneficiary details.
2. Matching: The bank's system checks if either the victim or beneficiary account number matches its customer base.
3. Classification:
4. If the match is on the victim field, it is a victim case.
5. If the match is on the beneficiary field, it is a beneficiary (suspect/mule) case.

**If both the victim and beneficiary accounts are in your bank, classify the case as a “beneficiary case.”**

* **Reason:** The primary regulatory and investigative action is required on the beneficiary (suspect) account to freeze funds and support the investigation.
* **Action:** Route the case to the team that handles beneficiary (suspect/mule) accounts.

**Do not duplicate the case for the victim.**  
**Always prioritize beneficiary classification in such scenarios.**

**Summary:**  
When both accounts are in your bank, treat and process it as a beneficiary case.

**Step 4: Handling Victim Transactions :**

**Actions performed in the BANK**

* **If the victim’s account is in the same bank:**
  + Put a hold on the victim’s funds.
  + Look for more suspicious transactions and alert risk officers.
  + Investigate, resolve, and update the case status.
  + Share case details with the Net Base Registry for future alerts.
* **If the victim’s account is in another bank:**
  + Review transactions and hold funds if needed.
  + Investigate, resolve, and update the case.
  + Share details with the Net Base Registry.

**Step 5: Handling Beneficiary Transactions (By Risk Officer)**

* Immediately put a hold on the beneficiary’s account.
* Investigate, resolve, and update the case in Unite Hub.
* Send case details to the Net Base Registry.

**Step 6: Ongoing Deduplication & Risk Monitoring**

* The Net Base Registry is always monitoring for suspicious activity, such as:
  + New accounts being opened
  + Payment transactions
  + Addition of new beneficiaries
* The registry creates case IDs and alerts risk officers in real time for any suspicious actions.

All complaints from I4C get unique case IDs and are queued in Unite Hub, where risk officers have full access to review all customer and transaction details.

**1.I4C Complaints and Investigations**

**1a. Data Exchange and Workflow Overview for Risk Management Tool Integration with i4C Unite Hub Portal**

Currently, data from i4C is provided to banks in three distinct forms:

1. **Mail**
2. **Portal** (i4C Web Portal)
3. **API** (Currently available for ongoing transactions).

Additionally, i4C provides a **Suspect Registry** to banks, delivered as a database and API integration is work in progress at i4c.

The **i4C Suspect Registry** is a centralized database maintained by the Indian Cyber Crime Coordination Centre that contains details of suspected cybercriminals, including their mobile numbers, email addresses, bank account numbers, UPI IDs, and social media profiles. It is used by law enforcement agencies and financial institutions to identify, track, and prevent cyber fraud by providing real-time access to information about individuals and accounts linked to suspicious or fraudulent activities.

**I4C Complaint Scenarios:**

i4C sends complaint data to banks for two potential roles:

1. **Victim** – The account holder has been defrauded.
2. **Beneficiary** – The account holder’s account is suspected of being used to receive fraudulent funds.

Under the i4C initiative, the detailed information shared with banks plays a critical role in fraud investigations. For example, when an account holder is a customer of Equitas Bank, the bank must conduct an in-depth analysis considering both victim and beneficiary scenarios. This involves examining transactional data, cross-verifying beneficiary details, and identifying anomalies or suspicious patterns. Equipped with tailored insights, the bank can efficiently assess risks, take remedial measures, and enhance its fraud prevention mechanisms. This collaborative framework ensures comprehensive security and builds trust among financial stakeholders

**Data Entry Interface for i4C Complaints**

**Purpose:**

To provide a dedicated data entry portal within the Unite Hub Portal, allowing data entry specialists or bank staff to manually enter i4C fraud complaints. This portal ensures that all relevant details about each fraud case—such as customer information, transaction details, and the nature of the complaint—are accurately captured and stored in the system. By having a structured and user-friendly interface, the portal helps data entry specialists efficiently log and update cases, reducing errors and ensuring consistency.

This process makes sure that every fraud complaint is properly recorded and tracked, enabling the risk management team to monitor, investigate, and resolve cases effectively. It also keeps the database current and organized, supporting smooth workflow and reliable reporting until an automatic system is available.

**Key Points:**

* Manual Entry: Staff can type in i4C fraud complaints directly into the Unite Hub Portal.
* No Gaps: All fraud cases are tracked, so nothing is missed during the transition.
* Accurate Records: All complaints are kept in one place for easy checking and reporting.

**Functionality to be Available When API Connection Is Established:**

* Fraud complaints will be sent automatically from the reporting system to the Unite Hub Portal.
* Staff will not need to enter cases by hand.
* Cases will appear instantly, making the process faster and easier.

**Manual Input Screen (For Bank assigned Staff) Unite Hub Portal**

**Examples of data entry fields in the Portal**

* **Case Source:** Pre-filled as "i4C Complaint" (with a dropdown option if other sources exist).
* **i4C Reference ID:** Unique ID from the i4C portal (mandatory field).
* **Customer Details:**
  + Name, contact number, account number.
  + Victim/Beneficiary label (dropdown).
* **Fraud Transaction Details:**
  + Transaction type (NEFT, UPI, IMPS, RTGS, etc.).
  + Amount, date, reference number.
  + Beneficiary account details (if available).
* **Complaint Summary:** Brief description of the fraud (e.g., "Unauthorized UPI transfer").
* **Attachments:** Option to upload screenshots/documents from i4C.
* **Submit Button:** Saves the case to the risk management tool’s database.

**Detailed field list available in the Annexures Sheet name “Input and other fields”**

**Validation Rules:**

* Auto-check for duplicate i4C Reference IDs to prevent redundancy.

**Workflow Steps**

1. **Manual Entry (Current Process):**
   * Bank staff logs into the i4C portal, reviews the complaint, and copies relevant details into the risk management tool’s input screen.
   * Example: A customer reports a fraudulent ₹50,000 IMPS transfer via i4C. The staff enters the case manually with the i4C Reference ID i4C-2025-1234.
2. **Duplicate Check:**
   * The system cross-checks the i4C Reference ID against existing cases.
   * If a match is found, a warning appears: *"Case i4C-2025-1234 already exists [Case ID: RM-5678]. Link to existing case?"*
3. **Case Tagging & Assignment:**
   * The case is automatically tagged as "High Risk" or "Low Risk" based on amount, transaction type, etc.
   * Assigned to a risk officer based on location (e.g., Mumbai cases go to Mumbai team) and workload rules.
   * There should be a back end maintenance for mapping tagging and assignment
4. **Dashboard Display:**
   * Risk officers see the case in their queue with a **"Source: i4C (Manual)"** label.
   * Key details: Customer name, fraud amount, transaction type, i4C Reference ID.

**Future API Integration (Once Enabled by i4C)**

1. **Automated Case Creation:**
   * i4C’s system sends fraud alerts directly to the bank’s risk tool via API.
   * The case is auto-created with fields like:
2. **Case Screen Post-API Integration:**
   * **Source:** Automatically labeled "i4C (API)".
   * **Linked Cases:** Displays related cases (e.g., if the same beneficiary account appears in multiple complaints).
   * **Alerts:** Auto-generated if the i4C Reference ID matches an existing case.

**Benefits**

* **Manual Phase:** Ensures no delay in processing i4C complaints while API integration is pending.
* **API Phase:** Eliminates manual entry errors and speeds up case creation.
* **Unified View:** Combines manual and API-sourced cases in one dashboard for risk officers.

**Example Workflow:**

* Today: Staff manually enters an i4C UPI fraud case (₹75,000) with Reference ID i4C-2025-9012.
* Post-API: Similar cases will auto-populate, and the system will flag duplicates using the i4C Reference ID.

**\*Detailed list of fields required for inputting is available in annexures to this document.**

**2a. Case Queuing System – Unite Hub Portal**

2a. Case Queuing System – Unite Hub Portal

1. Capturing the Case

* The case queue management system receives fraud cases from two primary sources:
  + Direct Complaints: For example, complaints forwarded by external agencies like i4C (Indian Cyber Crime Coordination Centre) or customer complaints received via email, web forms, or phone calls.
  + New Detections: The Unite Hub’s rule-based risk engine continuously monitors payment transactions (such as UPI, NEFT, IMPS, RTGS, fund transfers) and onboarding activities (such as new account openings and new beneficiary additions). When suspicious activity is detected according to predefined rules, the system automatically generates a new case.
* For new detections, each case is cross-checked against the consolidated complaints base in the Unite Hub registry, which integrates both i4C complaints and prior rule-based detections, to identify potential matches or repeat patterns.
* Each complaint or detection is saved as a separate case with a unique case ID in the secure database.
* Example: If a customer reports an unauthorized UPI transfer and the risk engine also detects a suspicious NEFT transaction, both incidents are recorded as separate cases with distinct case IDs.

For new detections, cases are matched against a consolidated complaints base within the Unite Hub registry, which includes both i4C complaints and detections from the rule-based risk engine.

**2. Sorting and Risk Tagging of the Case**

* Each case is labelled as either:
  + *Victim*: The person who lost money (e.g., a customer whose account was debited without authorization).
  + *Beneficiary*: The person who received the funds (e.g., the account that got the transferred money).
* The system also tags each case for risk level (such as high risk or low risk) based on rules and criteria maintained in the back end. For example, cases with large amounts, multiple linked frauds, or involving VIP customers are tagged as high risk.
* All tagging and categorization are driven by master data and configurable rules set up in the back end, making the process consistent and easily adjustable.

**3. Mapping and Assigning Cases to the Right Risk Officer**

* The assignment of cases to risk officers is fully automated and based on master data and mapping rules maintained in the back end.

A Few Examples are :

* + *Location Mapping*: Cases are assigned to risk officers based on the customer’s location, as per the location mapping maintained in the system.
  + *Risk Level Mapping*: High-value or high-risk cases are mapped to senior or specialized risk officers as defined in the back end.
  + *Customer Type Mapping*: Cases involving business customers, retail customers, or merchants are routed according to pre-set mappings.
  + *Workload Balancing*: The system checks each risk officer’s current workload and assigns new cases accordingly, as per back-end configuration.
* All these assignment rules can be updated centrally in the back end, allowing for quick adaptation to changing requirements or team structures.

**4. Displaying Cases to Risk Officers**

* When risk officers log in, they see a dashboard showing:
  + Case ID, source of the case (i4C complaint or risk engine detection), customer name, transaction details (such as UPI ID, NEFT/IMPS/RTGS reference number), fraud amount, risk level, and status.
  + Sorting and filtering options: View only high-risk cases, sort by oldest, or see cases by customer type or source.
  + Visual indicators: High-risk cases may be highlighted in red for quick attention.
* The display and prioritization of cases are also based on rules maintained in the back end.

**5. Tracking Progress in the Case Queue**

* Each case displays its current status:
  + ***New*:** Just received, not yet reviewed.
  + ***In Progress***: Under investigation.
  + ***Pending Approval*:** Awaiting supervisor review.
  + ***Closed*:** Investigation complete and resolved.
* Risk officers can forward cases to other teams (like legal or compliance) or escalate to senior staff if needed, as allowed by the workflow rules in the back end.
* Example: If a risk officer finds a case involves multiple victims of unauthorized IMPS transactions, they can link related cases for a coordinated investigation.

**6. Urgent Alerts and Notifications**

* For urgent or high-risk cases, the system sends real-time alerts via SMS or email to risk officers or managers for immediate action, as defined in the alerting rules in the back end.
* Example: If a fraud case involves a large NEFT transfer or a repeat offender, an alert is sent to both the risk officer and their supervisor.

**Additional Functional Features :**

* **Real-Time Monitoring:**  
  The system watches all payment transactions (UPI, NEFT, IMPS, RTGS, fund transfers) around the clock. If it spots something suspicious, like a large late-night transfer, it creates a case instantly.
* **Automated Case Prioritization:**  
  Urgent cases (such as those involving VIP or sensitive accounts) are automatically moved to the top of the review queue, so they get attention first.
* **Collaboration Tools:**  
  Risk officers can add comments, upload documents, and update case status, making it easy for the whole team to stay informed and work together.
* **Reporting and Analytics:**  
  Managers can quickly see stats like how many cases are open, how many were resolved recently, and the average time to close a case. This helps them spot issues and improve performance.
* **Customizable Assignment Rules:**  
  The rules for assigning and prioritizing cases can be updated anytime in the backend, so the system can adapt quickly to new fraud trends—without any downtime.

**LOVs field list to be maintained in the back end (Master Maintenance)**

* *Refer Annexures*

**3a.UNIRISK (Risk Rule Engine )**

The UNIRISK Rule Engine, part of the UNITE HUB Platform, connects to the Net Base Registry (real-time I4C complaints) and Unite Hub Registry (consolidated risk data) to instantly identify suspicious activities—including new account openings, beneficiary additions, and payment transactions. It automatically generates case IDs for detected risks, links them to previous I4C complaints where relevant, and displays all alerts to the risk officer on the Case Action screen.

**UNIRISK (Risk Rule Engine)**

**1. When Someone Opens a New Account**

**What UNIRISK Does:**  
Instantly checks the new customer’s details against Unite Hub registry suspicious cases.

**Example:**  
If a person tries to open an account using an Mobile number or ID that was reported in an I4C fraud complaint, UNIRISK immediately alerts the fraud team so they can review and take appropriate action.

**2. When a Dormant Account Is Reactivated**

**What UNIRISK Does:**  
Checks if the account or user trying to reactivate is flagged for fraud.

**Example:**  
If someone tries to reactivate an old account and their details match a blacklisted entity (unite Hub Registry ) in the I4C registry, UNIRISK notifies the risk officer for further investigation.

**3. When a New Beneficiary Is Added**

**What UNIRISK Does:**  
Verifies the beneficiary’s account number or UPI ID against fraud and suspect lists (Unite hub Registry )

**Example:**  
If a customer adds a beneficiary whose account was used in a previous fraud, UNIRISK alerts the risk team so they can decide the next steps.

**4. When Any Payment or Transfer Happens**

**What UNIRISK Does:**  
Monitors every transaction in real time, looking for suspicious patterns.

**Example:**  
If a customer suddenly trans fers a large sum to a new beneficiary late at night, and this matches a known fraud pattern, UNIRISK sends an alert to the risk team before any money leaves the account, so they can review the transaction.

**5. Case Creation and Linking**

**What UNIRISK Does:**  
Automatically creates a new case for every suspicious activity and links it to any past related fraud complaints.

**Example:**  
If a flagged beneficiary in a new payment was already reported in a previous I4C complaint, UNIRISK links the new case to the old one and displays this to the risk officer, helping them see the full history and act accordingly.

UNIRISK acts as an early warning system, alerting the risk team to suspicious activities so the Bank can take action to prevent fraud.

**4a. Case Action screen :**

**Customer Details Screen with Matching Details**

**Purpose:**  
Displays all relevant information about victims and suspects (beneficiaries), and highlights matches with internal/external fraud registries.

**Key Features:**

* **Victim & Beneficiary Information:**
  + Names, addresses, contact details, account numbers, KYC status.
  + Whether the victim or beneficiary account is with Equitas or another bank.
* **Registry/Alert Matching:**
  + Flags if the account matches entries from I4C, internal watchlists, or other banks’ alerts (e.g., mule accounts).
* **Scenario Highlights:**
  + ***Victim Transactions:***
    - **Equitas to Equitas:** Both victim and beneficiary are Equitas customers. Full details for both are shown, and the system highlights if either is flagged.
    - **Equitas to Other Bank:** Victim is Equitas customer, beneficiary is with another bank. Victim’s details are shown; beneficiary’s details are displayed as available. If flagged, the system prompts for external notification to the other bank for further action[2](https://www.equitasbank.com/unauthorized-transaction/)[13](https://www.equitasbank.com/strapi-dev/uploads/ESFB_Customer_Compensation_Policy_73b79f2584.pdf).
  + ***Beneficiary (Suspect) Transactions:***
    - **Suspect Account with Equitas:** Shows full details and flags if the account is under investigation or matched in fraud registries.

**2. Transaction Details (Statements)**

**Purpose:**  
Provides a detailed, chronological view of all relevant transactions, supporting deep-dive investigation and pattern analysis.

**Key Features:**

* **Transaction List:**
  + Date, time, amount, type (credit/debit), source/destination accounts, reference numbers.
  + For Equitas-to-Equitas, both sides of the transaction are visible.
  + For Equitas-to-other-bank, outgoing transaction is visible; incoming details depend on information sharing from the other bank.
* **Suspicious Activity Highlighting:**
  + Flags transactions that triggered rule engine alerts, such as:
    - **Suspicious Payment Transactions:** Unusual patterns, high-value or rapid transfers, etc.
    - **Newly Opened Accounts:** Accounts recently onboarded and immediately involved in high-risk transactions[8](https://www.equitasbank.com/strapi-dev/uploads/Niyo_Equitas_Tn_C_March_23_c11f24f4cf.pdf)[12](https://www.equitasbank.com/strapi-dev/uploads/FREOSAVE_Equitas_Tn_C_March_23_7e7581f4c9.pdf).
    - **Newly Added Beneficiaries:** Beneficiaries added shortly before suspicious transactions.
    - **Money Mule Transactions:** Transactions showing typical mule behavior, such as rapid in-and-out fund flows or links to multiple flagged accounts.
* **Drill-Down Capability:**
  + Investigators can click for more details, including counterparty info and transaction purpose.
* **Visual Indicators:**
  + Color-coding or icons for high-risk transactions as identified by the rule engine.

**3. Decision Making Screen (LOVs & Remarks Section)**

**Purpose:**  
Enables risk officers to take action, record decisions, and manage workflow, including reassignment of cases.

**Key Features:**

* **List of Values (LOVs):**  
  Dropdown menus for standardized actions, such as:
  + “Freeze Account”
  + “Escalate to Law Enforcement”
  + “Notify Other Bank” (for Equitas-to-other-bank scenarios)
  + “Close Case – No Fraud”
  + “Request More Information”
* **Remarks Section:**  
  Free-text area for documenting findings, rationale, and next steps.
* **Case Submission & Workflow:**
  + Submit the case for review or closure.
  + Reassign the case to another user’s queue (e.g., for specialist review or workload balancing).
  + Track status: Pending, Under Investigation, Resolved, Escalated.
* **Audit Trail:**  
  Logs all actions and decisions for compliance and future reference

**Example Scenario Coverage Table :**

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario Type | Victim Account | Beneficiary Account | Key Actions/Notes |
| Equitas to Equitas | Equitas | Equitas | Both parties visible; full investigation in-house |
| Equitas to Other Bank | Equitas | Other Bank | Notify other bank; share info as per protocol for investigation que |
| Beneficiary (Suspect) at Equitas | Any | Equitas | Full details shown; flagged if matched in registry , also check for Mule transactions. |
| Rule Engine: Suspicious Payment | Any | Any | Transaction flagged for review |
| Rule Engine: New Account | Equitas | Any | Recent onboarding flagged if involved in suspicious txns |
| Rule Engine: New Beneficiary | Equitas | Any | Recent addition flagged if involved in suspicious txns |
| Rule Engine: Money Mule | Any | Equitas | Pattern-based flagging; triggers deeper investigation |

**\*The Scenarios and Rules will be expanded once onboarded with the Bank**

**Additional Requirement for Case Decision Screen While submitting the case :**

When a risk officer submits a case on the Case Decision Screen, a pop-up message should appear with the following prompt:

**Pop-Up Message:***"Do you want to move this Case ID to the Unite Hub Registry base?"*

**Options:**

* Yes (proceeds to move the case to the Unite Hub Registry)
* No (submits the case without moving it to the Unite Hub Registry)

**Additional Notes:**

* The pop-up should appear immediately after the risk officer clicks the "Submit" button for the case.
* The risk officer must select either "Yes" or "No" to continue.
* If "Yes" is selected, the case is transferred to the Unite Hub Registry base as part of the workflow.
* If "No" is selected, the case is submitted as usual but not moved to the Unite Hub Registry.

**Visual Indicators :**

The Case decision screen should have good Visual indicators which are quick, easy-to-see symbols or highlights that help users understand the status of a fraud case, transaction, or account at a glance—without reading all the details.

**Example:**

**For Cases:**

* Show if a case is closed, still under review, or urgent and needs quick attention.

**For Transactions:**

* Highlight if a transaction looks suspicious, involves a new account, a new beneficiary, or shows signs of money mule activity.

**For Accounts and People:**

* Indicate if a person or account is on a national fraud list, is linked to other cases, or has special notes or warnings.

**Basic Features for the Case Decision Screen**

* **Dashboard:** A main page showing all important case details.
* **Real-Time Alerts:** Instant messages or highlights when something needs urgent attention.
* **Clickable Details:** Ability to click on any symbol or transaction for more information.
* **Related Cases Panel:** Shows if this case is linked to others, with quick status checks.
* **Action Buttons:** Simple options to take action (like freeze, report, notify, close, or reassign cases).
* **Remarks Box:** A space to add notes or comments about your findings.
* **Audit Log:** A history of who did what and when for every case.
* **Search and Filter:** Tools to quickly find and sort cases by name, account number, transaction ID, or status.

The UI/Ux Team can decide the best way of representing this.

**Automated Updater to i4c:**

Once a case is submitted and reviewed in the Unite Hub Portal, there should be an automated process that updates the I4C system with all relevant case details. This integration ensures that:

* **Case Data Sync:** As soon as a case is finalized and submitted by bank staff in the Unite Hub Portal, all key information (such as complaint reference number, victim/beneficiary details, transaction data, notice type, acknowledgement number, IFSC code, lien amount, etc.) is automatically pushed to the I4C platform without manual intervention.
* **Real-Time Communication:** The update happens instantly, reducing delays and ensuring I4C always has the latest case status for coordinated fraud response and investigation.
* **Audit Trail:** Every automated update is logged for compliance and audit purposes, including timestamps and user IDs.

**Report Download Feature**

* **Download Option:** The Unite Hub Portal should provide users (with appropriate permissions) the ability to download case reports.
* **Customizable Reports:** Users can select the desired columns (e.g., victim name, complaint number, transaction details, IFSC code, lien amount, etc.), date range, and file format (Excel/CSV).
* **Easy Access:** A “Download Report” button should be available on the portal’s case review or reports screen, allowing users to generate and save reports for further analysis, compliance, or sharing with authorities.
* **Download History:** The portal may also maintain a history of downloaded reports for user reference and audit tracking.

**Summary Table of Features:**

|  |  |
| --- | --- |
| **Feature** | **Description** |
| Automated Updater | Automatically sends submitted case data from Unite Hub Portal to I4C, with full audit logging. |
| Report Download | Allows users to export case data in Excel/CSV, with customizable columns and download history. |

**LOVs field list to be maintained in the back end (Master Maintenance)**

*Refer Annexures*

**5a UNITE HUB Registry :**

**1. Centralized Case Storage and Data Integration**

The Registry should act as a single hub for storing all case details received from various sources over time.  
**Examples:**

* When a customer files a fraud complaint through the i4C portal, the details should be automatically stored in the Registry.
* Integration with i4C Suspect Registry: Cases from the i4C Suspect Registry should be stored in the Unite Hub Registry using an API integration if and when the API is available. Until such time as the API is implemented, the system should support manual uploads of suspect registry data to ensure that all relevant information is captured in the central database.
* Once data entry for I4C cases is completed on the Unite Hub input screen, the information should flow in real time to the Unite Hub Registry. This immediate transfer is essential to ensure that threat alerts are instantly available to banks for prompt action. Real-time integration with the I4C platform enables any financial fraud complaint or suspicious entry to be routed directly to the relevant bank’s backend systems, allowing for rapid detection, investigation, and remedial action. This process supports the banking sector’s need for timely threat alerts, helping to freeze suspicious accounts and prevent fraudulent transactions before funds can be siphoned off through mule accounts or other fraudulent means. – We can call this as **Net Base registry**

**2. Flexible Data Input: Uploads and APIs:**

The Registry should be able to receive data through both manual uploads and automated API integrations.  
**Examples:**

* A fraud analyst / Risk officer can upload a spreadsheet containing a list of newly identified mule accounts (negative base). Based on User maintenance.
* The system can automatically receive daily updates from external fraud databases, ensuring that the Registry is always current.

This flexibility ensures that both structured (automated feeds) and unstructured (manual uploads) data are captured, reducing the risk of missing critical information

**3. Common Registry: Case Linking, Deduplication, and Management**

The Unite Hub Registry should function as a centralized, common repository for all fraud-related cases, supporting automated linking of related cases, deduplication, and efficient case management. The following functionalities should be included:

* **Automated Linking of Related Cases:**  
  The registry should automatically identify and link cases that reference the same beneficiary (suspect) account, contact number, or UPI ID across multiple fraud complaints or reports.  
  *Example:* If two different victims report unauthorized transfers to the same beneficiary account, the registry should recognize this and link both cases under a unified investigation, ensuring all relevant information is consolidated.
* **Onboarding and Beneficiary Addition Monitoring:**  
  When new accounts are opened or new beneficiaries are added, the registry should check if their details (such as account number, mobile number, or email) appear in existing cases or suspect lists.  
  *Example:* If a newly added beneficiary matches a bank account already involved in previous cases, the registry should flag and link these events, helping investigators see potential connections.
* **Payment Transaction Tracking:**  
  The registry should track payments made to beneficiaries and cross-reference them with existing cases or suspect lists.  
  *Example:* If a payment is made to a beneficiary who is already part of an ongoing investigation, the registry should automatically associate this new transaction with the existing case, maintaining a comprehensive record.
* **Case Deduplication:**  
  The registry should detect and merge duplicate cases involving the same beneficiary, account, or transaction details, ensuring investigators do not work on parallel or redundant investigations.  
  *Example:* If multiple complaints are filed about the same suspect from different sources, the system should merge them into a single case file, preserving all associated data and audit trails.
* **Comprehensive Case Management:**  
  The registry should provide a unified view of all actions, status changes, and linked events for each case, supporting efficient investigation, resolution, and reporting.  
  *Example:* Investigators should be able to see the full history of a beneficiary, including all cases, transactions, and actions taken, in one place.

These features will ensure the Unite Hub Registry serves as a robust, centralized platform for managing fraud cases enabling proactive detection of connections, efficient investigation, and comprehensive oversight across the organization.

**4. Real-Time Case Status Mapping**

The Registry should intelligently map and update the closure status of cases in real time, pulling updates directly from the Unite Hub Case Closure screen.  
**Example:**

* When an investigator closes a case after confirming it was a false alarm, the status should update instantly in the Registry, so other teams know not to pursue further action.

This real-time visibility ensures that everyone is working with the latest information, improving coordination and reducing redundant efforts

**5. User Uploads for Positive and Negative Bases**

Users should be able to upload positive (trusted or verified entities) and negative (known or suspected fraudsters) datasets at any time.  
**Examples:**

* Uploading a list of verified vendors (positive base) helps the system avoid flagging legitimate transactions.
* Adding a new list of blacklisted phone numbers (negative base) allows the risk engine to catch fraud attempts using these numbers immediately.

This feature enables the Registry to adapt quickly to new threats and incorporate the latest intelligence, making fraud detection more effective

**6. Comprehensive Audit Trail and Compliance**

The Registry should maintain a full record of all actions, status changes, and data uploads, providing a transparent audit trail.  
**Example:**

* Every time a case is updated, closed, or merged, the system should log who made the change and when. This is crucial for internal reviews and regulatory audits.

Such documentation supports compliance with industry standards and regulatory requirements, such as those set by the Reserve Bank of India or international best practices

**7. Seamless Integration and Collaboration**

By consolidating all fraud-related information in one place and enabling real-time updates, the Registry should support efficient collaboration across teams and facilitate information sharing with relevant stakeholders, including law enforcement if required.  
**Example:**

* If a case escalates and needs to be reported to authorities, all relevant details, history, and supporting documents can be exported directly from the Registry, speeding up the process and ensuring nothing is missed.

The Unite Hub Registry should provide a unified, up-to-date, and secure platform for managing fraud cases. With centralized storage, flexible data input, automated risk assessment, real-time status mapping, user uploads, comprehensive audit trails, and seamless collaboration, the Registry should empower Banks to prevent, detect, and resolve fraud more effectively and efficiently.

**Reporting and Analytics**

The Reports module will deliver critical insights and performance tracking:

* **Strike Rate:** Measure rule engine effectiveness by tracking how many alerts result in actual scams (e.g., 5/10).
* **Actioning Strike Rate:** Assess how effectively risk officers address alerts (e.g., 4/5).
* **Total Funds Saved:** Quantify savings due to alerts across the alert, bank, and daily levels.
* **Regular Reports:** Automate daily, weekly, and monthly fraud alerts, trends, and investigation outcomes.

**Turnaround Time (TAT) and Pendency Tracking**

TAT and pendency are key metrics for managing fraud cases effectively. They will be shown in both the case queue and the reports module.

**Conditions to match i4c Details with Banks database :**

**Refer Annexures**

**Annexures :**

**Refer the excel file / Word document shared with this Document folder as Zip file “Input and other fields”**