**UX/UI Design Requirements for Financial Crime Case Management System**

**1. Overview and Introduction**

**1.1 Purpose**

The purpose of this document is to outline detailed requirements for the UX/UI design of a Financial Crime (FinCrime) Case Management System. This system will be used to detect, manage, and investigate AML, ABC, fraud, tax evasion, and other financial crime alerts. The design must provide an intuitive, efficient, and highly customizable interface for compliance officers, investigators, and managers.

**1.2 Scope**

The scope covers key dashboards such as:

* **Home Page Overview**
* **Transaction Dashboards**
* **Alerts Management**
* **Rules Management**
* **Cases Management**
* **Data Analytics**
* **Reports**
* **Settings**

The goal is to ensure that each dashboard and its subsections provide visual clarity, data transparency, and seamless navigation to users.

**Home Page Overview (Page 1-3)**

The **Home Page Overview** provides a central dashboard where users can quickly assess the overall state of the financial crime management system. This page should offer a clear and organized view of key metrics and allow users to navigate to other parts of the system efficiently.

**1.1 Key Metrics**

The key metrics section should provide a summarized view of essential financial crime data such as total inflows, outflows, customer counts, and risk profiles.

**Sub-sub-sections:**

* **Total Inflow/Outflow/Revenue**:
  + **Design**: Display **line graphs** and **bar charts** to represent the trends in inflows and outflows, and use a **total revenue figure** at the top of the graph.
  + **Functionality**: Allow users to view data over customizable time frames (daily, weekly, monthly, or yearly).
  + **Interactivity**: Enable users to hover over specific data points to get detailed breakdowns of inflow/outflow sources (e.g., fiat or crypto transactions).
* **FinCrime Transaction Counts**:
  + **Design**: Use a **pie chart** or **bar graph** to show the breakdown of financial crime-related transactions (e.g., AML alerts, fraud alerts, PEP hits).
  + **Functionality**: Include **drill-down** functionality where clicking on a section of the chart takes the user to more granular data (e.g., list of transactions).
* **Entities Count & Amounts Transacted**:
  + **Design**: A **stacked bar chart** to show the count of entities categorized by risk tier (low, medium, high, ultra-high risk).
  + **Functionality**: Provide hover-overs for amounts transacted per entity group and drill-down into transaction summaries for each risk tier.
* **Risk Profiles**:
  + **Design**: Use a **donut chart** to show the distribution of customers/entities across different risk profiles (Low, Medium, High, Ultra-High).
  + **Functionality**: Allow users to click on any risk profile segment to view a **detailed list of customers/entities** in that risk tier.
* **Quick Links**:
  + **Design**: Place **icon-based buttons** at the top of the page for quick navigation to Alerts, Cases, Rules, and Reports.
  + **Interactivity**: These icons should have **tooltips** that briefly describe each section when hovered over.

**2. Dashboard (Page 4-8)**

The **Dashboard** section provides a detailed view of transactions, alerts, PEP hits, and sanctions across geographical regions and asset classes. It allows users to analyze the system’s real-time activity and adjust filters for better insight into specific regions, assets, or entities.

**2.1 Geography-Wise Transaction Overview**

The **Geography Dashboard** provides a global perspective on transaction activity.

**Sub-sub-sections:**

* **Design**: A **heatmap** displaying transaction volumes per country or region.
  + **Functionality**: The heatmap should change color intensity based on transaction volumes, with darker colors representing higher volumes.
  + **Interactivity**: Clicking on a country/region should show a **detailed list of transactions** originating from or directed to that geography.
* **Filters**:
  + **Region**: Users should be able to filter transactions by specific countries, states, or cities.
  + **Currency**: A filter for transaction type (fiat vs. cryptocurrency).
  + **Transaction Direction**: Users should be able to filter by inflow vs. outflow for each geography.

**2.2 Asset-Wise Transaction Breakdown**

This dashboard focuses on asset class transactions, especially for cryptocurrencies and fiat.

**Sub-sub-sections:**

* **Design**: Use **stacked bar charts** that show the distribution of transaction volumes by asset class (e.g., Bitcoin, Ethereum, Stablecoins, Fiat).
  + **Interactivity**: Allow users to click on each asset class to see detailed transactions involving those assets.
  + **Hover-Over Details**: On hover, show **detailed statistics** like transaction count, value, and top countries or customers involved.

**2.3 Transaction Screening**

The **Transaction Screening Dashboard** shows the number of transactions flagged, passed, or under investigation.

**Sub-sub-sections:**

* **Design**: A **pie chart** or **stacked bar chart** showing the status of transactions (screened, blocked, under investigation, passed).
  + **Progress Bar**: Indicate how many of the flagged transactions are still under investigation or require resolution.
  + **Drill-Down**: Clicking on any segment (e.g., “blocked transactions”) should take the user to the list of blocked transactions and their associated cases.

**2.4 PEPs & Sanctions**

This section tracks transactions involving **Politically Exposed Persons (PEPs)** and entities on sanctions lists.

**Sub-sub-sections:**

* **Design**: A **bar graph** showing the number of transactions involving PEPs and sanctioned entities by country.
  + **Filters**: Include filters for PEP status, country, risk level, and time period.
  + **Interactivity**: Clicking on a bar should show the transactions involving that specific PEP or sanctioned entity, with links to case details.

**3. Alerts Dashboard (Page 9-13)**

The **Alerts Dashboard** provides a comprehensive analysis of all financial crime alerts generated by the system, categorized by volume, severity, and type. It tracks the aging of alerts and highlights pending investigations.

**3.1 Alert Aging & Volume**

This dashboard tracks aging alerts and volume metrics over time.

**Sub-sub-sections:**

* **Design**: Use a **bar chart** to display alert aging (e.g., alerts unresolved for 1-7 days, 7-14 days, etc.) categorized by severity.
  + **Hover-Over**: When hovering over each bar, show the exact number of alerts in that time range and their risk rating.
  + **Filters**: Include filters for severity (critical, medium, low) and time period (last 24 hours, 7 days, 30 days).

**3.2 Alert Volume by Scenarios**

This dashboard shows the volume of alerts categorized by **AML scenarios**, such as **structuring**, **layering**, and **smurfing**.

**Sub-sub-sections:**

* **Design**: **Stacked bar charts** visualizing alerts generated by financial crime typologies (AML, fraud, sanctions).
  + **Interactivity**: Users should be able to click on a specific alert type to view the detailed list of alerts triggered by that scenario.

**3.3 Trigger of Hits (Alert Causes)**

This section identifies the primary causes for alerts being triggered (e.g., large transactions, mismatched KYC data, high-risk entities).

**Sub-sub-sections:**

* **Design**: A **pie chart** illustrating the causes of alert hits (e.g., transaction value, PEP hits, mismatched KYC).
  + **Interactivity**: Clicking on a section should take users to the list of transactions that triggered those alerts.
  + **Hover-Over Details**: Display the number and percentage of alerts triggered by each cause.

**3.4 Alerts by Product Type**

This section categorizes alerts by product type, such as fiat transfers, crypto transfers, and credit transfers.

**Sub-sub-sections:**

* **Design**: Use a **bar chart** to show the number of alerts triggered by each product type.
  + **Drill-Down**: Allow users to click on each product category to view the underlying transactions and alerts.

**4. Rules Dashboard (Page 14-17)**

The **Rules Dashboard** allows the system administrator or compliance team to configure and manage detection rules based on AML, ABC, and other typologies for detecting financial crimes.

**4.1 Rule Creation & Management**

This section allows users to create rules for detecting suspicious activities based on typologies provided by regulators like FATF, AUSTRAC, and FinCEN.

**Sub-sub-sections:**

* **Design**: Use a **wizard-based interface** for rule creation, guiding the user step-by-step in selecting conditions such as:
  + **Transaction Type**
  + **Risk Rating**
  + **Amount Threshold**
  + **Entity Type**
* **Editable Rule List**: Display existing rules in a **table view** with options to activate, deactivate, or edit each rule.
  + **Visual Cues**: Use icons or color codes to indicate the status of each rule (e.g., active, inactive, pending review).

**4.2 Rule Performance**

This dashboard shows how effective the existing rules are by tracking the number of alerts they generate.

**Sub-sub-sections:**

* **Design**: Use a **line graph** to track how many alerts were generated by each rule over time.
  + **False Positives vs. Valid Hits**: A **pie chart** should display the percentage of false positives vs. actual suspicious activity flagged by each rule.
  + **Interactivity**: Clicking on a rule should display the **alerts generated** and their outcomes (e.g., dismissed, escalated to a case).

**5. Cases Dashboard (Page 18-22) - Continued**

The **Cases Dashboard** is crucial for managing and tracking investigations related to financial crime alerts, including AML, fraud, sanctions, and tax evasion cases. The dashboard should offer a clear, concise view of each case's status, details, and activities, ensuring that investigators can efficiently monitor case progress.

**5.1 Case Overview**

This section provides an overview of all active, pending, or closed cases, displaying key information such as reference numbers, status, and creation dates.

**Sub-sub-sections:**

* **Design**: A **table view** listing all cases with columns for:
  + **Internal Reference Number**
  + **Case Creation Date**
  + **Status**: Pending, In Progress, Completed
  + **Entity Type**: Individual, Company, Trust, Association, etc.
* **Functionality**:
  + Users should be able to sort cases by **status**, **date**, or **entity type**.
  + Provide **quick action buttons** (e.g., View Details, Escalate, Add Notes).
  + Allow for **filters** based on time periods, case type (AML, fraud), or case priority.

**5.2 Case Structure**

This section allows users to visualize the structure of each case, showing the relationships between different entities (individuals, companies, etc.) involved in the case.

**Sub-sub-sections:**

* **Design**: Use a **network graph** or **organizational chart** to display relationships between the main entity and associated parties.
  + **Entity Types** should be represented with unique icons or thumbnails (e.g., icons for individuals, companies, trusts).
* **Functionality**:
  + Clicking on any entity should provide a **pop-up** with detailed information about that entity, including its role in the case (main subject or related party).
  + The graph should highlight **key connections** (e.g., financial links between companies, shared addresses).

**5.3 Case Details & Activities**

This section tracks detailed information about the case, including ongoing activities, investigator notes, KYC checks, and status updates for related parties.

**Sub-sub-sections:**

* **Design**: A **detailed case summary** showing:
  + **Entity Name** and **Role** (main entity, related party).
  + **Status** for each party (KYC verified, pending, high-risk).
  + **Pending Actions**: Number of KYC checks, investigations, or alerts to be resolved.
* **Functionality**:
  + A **timeline view** of activities and case updates.
  + **Notes section** where investigators can log updates or conclusions.
  + **Interactive buttons** to take action on pending items (e.g., request documents, mark as complete).

**5.4 Visualization**

This sub-section provides a visual overview of the case, highlighting the connections between transactions, entities, and alerts involved in the case.

**Sub-sub-sections:**

* **Design**: Use a **visual chart** or **flow diagram** to show how transactions link to different entities, accounts, or flagged activities.
  + **Color-Coding**: Use distinct colors to represent alert severity, transaction direction (inflow/outflow), or risk level.
* **Functionality**:
  + Clicking on a transaction or entity should display **detailed data** (e.g., transaction amount, date, related alerts).
  + Provide a **zoom feature** to explore deeper connections between entities or transactions.

**6. Your Data (Analytics Dashboard) (Page 23-25)**

The **Your Data** dashboard provides advanced analytics on customer behavior, transactions, and profiles. It enables investigators and compliance officers to monitor trends and flag suspicious activities based on risk ratings, IP behavior, and transaction patterns.

**6.1 Customer Profile Information**

This section provides detailed customer profiles, including KYC data, transaction history, and risk ratings.

**Sub-sub-sections:**

* **Design**: A **table view** displaying:
  + **Customer Name**
  + **Date of Birth**
  + **Risk Rating**: Low, Medium, High, Ultra-High
  + **Transaction History**: Number and total value of transactions
* **Functionality**:
  + Allow users to click on a **customer name** to access the **full profile** with additional data (e.g., KYC documents, alerts triggered).
  + Enable **sorting** and **filtering** by risk rating, transaction count, or alert status.

**6.2 Behavior Analytics**

This section tracks behavioral patterns such as login activity, IP address changes, and device usage.

**Sub-sub-sections:**

* **Design**: Use **line graphs** and **bar charts** to show:
  + **Login Activity**: Unusual login times or repeated failed login attempts.
  + **IP Address Changes**: Track locations from which the user logs in.
* **Functionality**:
  + Highlight **abnormal behaviors** (e.g., login attempts from multiple locations in a short time).
  + Provide alerts for **suspicious behavior**, allowing investigators to view a detailed breakdown.

**6.3 Transaction Analytics**

This section analyzes transaction activity, including the types of transactions conducted, their frequency, and the risk rating associated with each transaction.

**Sub-sub-sections:**

* **Design**: Use **stacked bar charts** to show the breakdown of transaction volumes by:
  + **Risk Rating**: Low, Medium, High.
  + **Transaction Type**: Fiat vs. cryptocurrency, transfers, withdrawals, deposits.
* **Functionality**:
  + Allow users to **filter transactions** by date, amount, or risk rating.
  + Provide a **drill-down** feature that shows individual transactions when clicking on a specific bar.

**7. Reports Dashboard (Page 26-29)**

The **Reports Dashboard** provides users with the ability to generate regulatory reports such as SMRs (Suspicious Matter Reports), CDDs (Customer Due Diligence), and TTRs (Transaction Threshold Reports). It also enables advanced reporting based on various financial crime typologies.

**7.1 SMR Generation**

This section allows users to generate Suspicious Matter Reports (SMRs) based on transaction activity and customer risk profiles.

**Sub-sub-sections:**

* **Design**: A **form-based interface** where users can select:
  + **Report Type**: AML, Fraud, Financing of Terrorism, Tax Evasion.
  + **Reason for SMR**: ATM/Cheque Fraud, Advanced Fee Scam, Credit Card Fraud, etc.
* **Functionality**:
  + Allow users to select **specific transactions** or customers as the basis for the SMR.
  + Include options to **export the report** in PDF, CSV, or Excel formats.
  + Provide a **comment section** for investigators to add detailed notes before submission.

**7.2 Report Reason Breakdown**

This section provides a breakdown of the most common reasons for generating SMRs, CDDs, or other regulatory reports.

**Sub-sub-sections:**

* **Design**: Use **bar charts** to display the number of reports generated for specific reasons (e.g., money laundering, tax evasion, phishing).
  + **Interactivity**: Users should be able to click on a reason to see a list of the underlying reports.
* **Functionality**:
  + Filters for **date ranges**, **report types**, and **customer risk levels**.
  + Allow users to **drill down** into individual reports based on the reason they were generated.

**7.3 Advanced Reporting**

This section allows for the generation of customized reports based on more complex filters and criteria.

**Sub-sub-sections:**

* **Design**: A **custom report generator** that allows users to define:
  + **Report Criteria**: Customer type, transaction amount, risk level.
  + **Time Period**: Weekly, monthly, quarterly, annually.
* **Functionality**:
  + Provide an **export function** for all reports, with the ability to save report templates for future use.
  + Include **visualizations** in the reports, such as bar charts or pie charts, summarizing key metrics.

**8. Reports Dashboard (Page 26-29)**

The **Reports Dashboard** provides compliance teams with the tools to generate and export various reports, including Suspicious Matter Reports (SMRs), Customer Due Diligence (CDD), Transaction Threshold Reports (TTR), and International Funds Transfer Instructions (IFTI). These reports are essential for regulatory reporting and internal monitoring.

**8.1 SMR Generation**

This section enables the generation of **Suspicious Matter Reports** (SMRs), allowing users to generate detailed reports based on predefined criteria.

**Design Requirements:**

* **Dropdown filters** for selecting report type (AML, fraud, tax evasion, financing of terrorism, etc.).
* **Radio buttons** to select the underlying reason for the SMR, such as:
  + **Money laundering**
  + **Financing of terrorism**
  + **Proceeds of crime**
  + **Offence against a Commonwealth, State or Territory law**
  + **Person/agent not who they claim to be**
  + **Tax evasion**
* Users should be able to **choose the reason** for the report, such as:
  + ATM/cheque fraud
  + Avoiding reporting obligations
  + Corporate/investment fraud
  + Credit card fraud
  + Counterfeit currency
  + Internet fraud
  + Phishing
* Once selected, the system should generate the report with relevant data and **export options** (PDF, CSV, Excel).
* SMRs should have a section for **comments or notes** from the investigator before final submission.

**8.2 Report Reason Breakdown**

This section provides a breakdown of the most common reasons for generating SMRs and other regulatory reports.

**Design Requirements:**

* **Bar charts** showing the breakdown of SMRs generated by reason:
  + **Advanced Fee/Scam**
  + **Suspicious Behavior**
  + **Tax Evasion**
  + **Proceeds of Crime**
  + **Structuring of Funds**
  + **Unusual Gambling Activity**
* Filters should allow users to view this data by region, customer type, and risk profile.
* Clicking on a specific reason should take the user to a **detailed report** showing which entities and transactions triggered the report.

**8.3 Advanced Reporting**

This section enables advanced customization of reports, allowing users to apply complex filters for better data analysis.

**Design Requirements:**

* Allow the generation of **Customer Due Diligence (CDD)** reports with options to include specific fields such as:
  + **Customer Information** (Name, DOB, Address, etc.)
  + **Transaction History**
  + **Risk Rating**
* Users can generate **Transaction Threshold Reports (TTR)** by selecting:
  + Specific thresholds (e.g., transactions above $10,000).
  + Time periods (e.g., monthly, quarterly).
* The system must also allow for **International Funds Transfer Instructions (IFTI)** reports that track cross-border transfers.
* All reports should have an **export function** that supports formats like CSV, PDF, and Excel.

**9. Data Ingestion and Resolution (Page 30)**

The **Data Ingestion and Resolution** dashboard provides real-time status on the ingestion of customer data and the resolution of ongoing financial crime investigations. It is crucial for ensuring data completeness and prompt resolution of alerts and cases.

**9.1 Data Ingestion Progress**

This section tracks the real-time progress of incoming customer data and transactional data ingestion.

**Design Requirements:**

* **Progress bars** indicating the percentage of completed data ingestion tasks.
* **Tables** showing:
  + Number of new customers processed.
  + Pending KYC documents.
  + Data entry errors or discrepancies.
* The system should send **alerts** if there are any ingestion issues, such as missing fields or failed data imports.
* Users should have access to a **log** of previous ingestions, showing timestamps and any errors.

**9.2 Resolution Progress**

This section monitors the status of case and alert resolutions, ensuring that flagged items are addressed in a timely manner.

**Design Requirements:**

* **Pie chart** showing resolved vs. unresolved cases and alerts.
* **Bar chart** showing the aging of unresolved alerts by severity (critical, high, medium, low).
* Users should be able to click into unresolved cases to take immediate action, such as escalating the issue or adding notes.
* Resolution timelines should be color-coded based on urgency:
  + **Red** for critical items exceeding the deadline.
  + **Yellow** for items nearing the deadline.
  + **Green** for resolved cases.

**10. Settings (Page 31-32)**

The **Settings** section allows administrators and system managers to configure user roles, set alert thresholds, and manage system-level settings for the FinCrime Case Management platform.

**10.1 User Roles & Permissions**

This section allows administrators to assign different roles and access levels to users, ensuring that data access and system functionality are appropriately restricted based on user roles.

**Design Requirements:**

* Provide a **user management dashboard** where admin users can:
  + Assign roles such as:
    - **Administrator**
    - **Investigator**
    - **Compliance Officer**
    - **Read-Only User**
* Each role should have specific permissions to access different areas of the platform (e.g., full access to case management, restricted access to reporting).
* Admins should be able to create **custom roles** with specific permissions.

**10.2 Alert Thresholds**

This section allows the configuration of thresholds for triggering alerts, ensuring that compliance teams are not overwhelmed by false positives or insignificant alerts.

**Design Requirements:**

* **Slider controls** for setting thresholds for alerts based on:
  + Transaction amount (e.g., trigger alerts for transactions above $10,000).
  + Velocity (e.g., multiple transactions within a short time period).
* Provide **preset alert levels** (Low, Medium, High) for quicker configuration.
* Include a **test function** to simulate how the alert threshold will affect transaction screening, allowing users to fine-tune settings.

**10.3 System Alerts**

This section provides system administrators with the tools to monitor the health of the platform, including data ingestion status, system performance, and any error messages.

**Design Requirements:**

* Include a **dashboard** that shows real-time system performance, including server health, data processing status, and error logs.
* Admins should be able to configure **system alerts** for issues like:
  + Failed data ingestion.
  + Delayed transaction screening.
* **Email notifications** should be sent automatically to admins when critical system issues arise.