Fraud Alert and Case Management:

Here's a practical example of a Fraud Alert and Case Management System using the Traffic Light Indicator Approach. This simulates a real-world scenario where fraud alerts are generated, categorized, and managed as cases.



Fraud Alert and Case Management – Example

Scenario:

You're managing fraud detection for an e-commerce platform. Alerts are triggered when suspicious activities are detected—like large transactions, mismatched IPs, or too many failed logins.

Fraud Alerts Table (with Traffic Light Status)

Alert ID	User ID	Alert Type	Risk Score	Risk Level	Status	Action Needed	Assigned To
A101	U001	Login from new device	20	Low	Closed	None	System
A102	U002	Multiple failed logins	55	O Medium	Under Review	Analyst Investigation	Alice
A103	U003	\$5000 Transaction	88	High	Escalated	Lock account + Review	Bob
A104	U004	IP mismatch	35	Medium	New Alert	Needs Assignment	-
A105	U005	Fake ID document	95	High	Investigating	Escalate to Legal	Rahul

Case Management Lifecycle (for Alert A103)

Case Field	Details
Case ID	C-A103
User ID	U003
Alert Triggered	High-value transaction
Risk Score	88
Risk Level	High
Assigned Analyst	Bob
Actions Taken	Account locked, user notified
Investigation Notes	Previous chargebacks found
Current Status	Escalated to Fraud Team
Date Opened	2025-04-12
Date Closed	_

Color-Coded Actions Overview

Color	Action By Analyst	System Action
Green	No action, monitor	Auto-close
Yellow	Review required, verify info	Alert analyst
Red	Immediate response needed	Lock account, notify fraud team