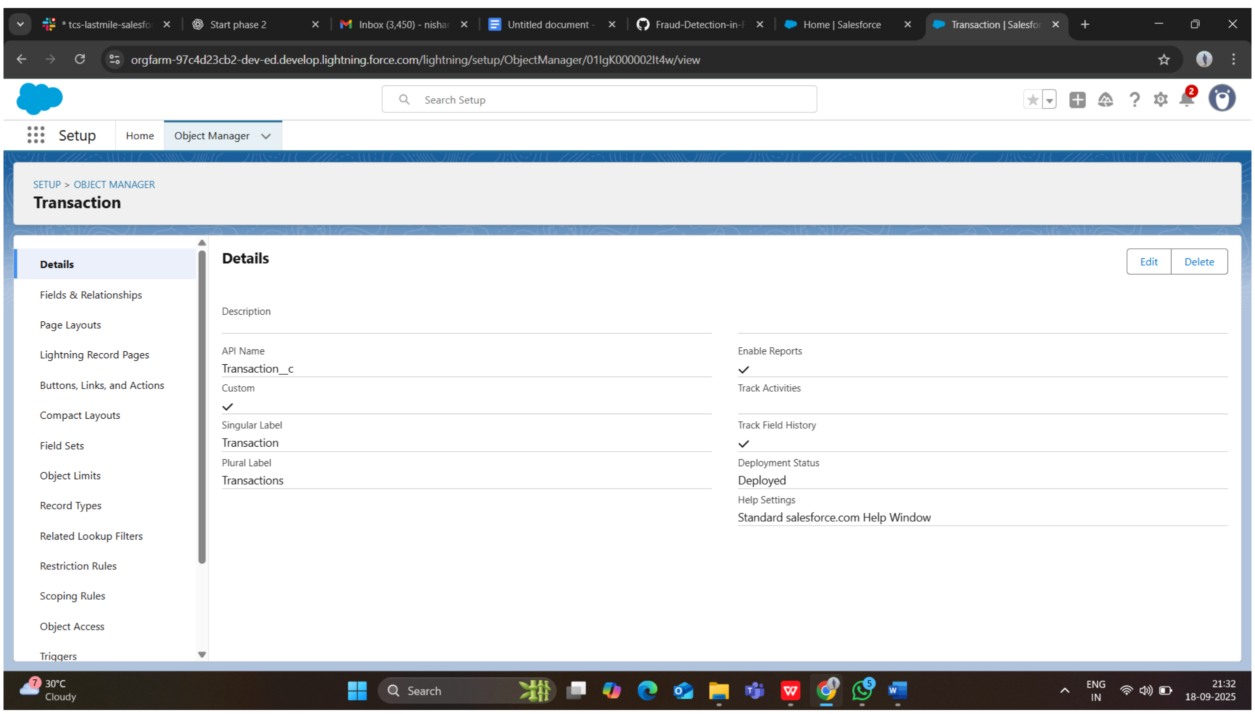
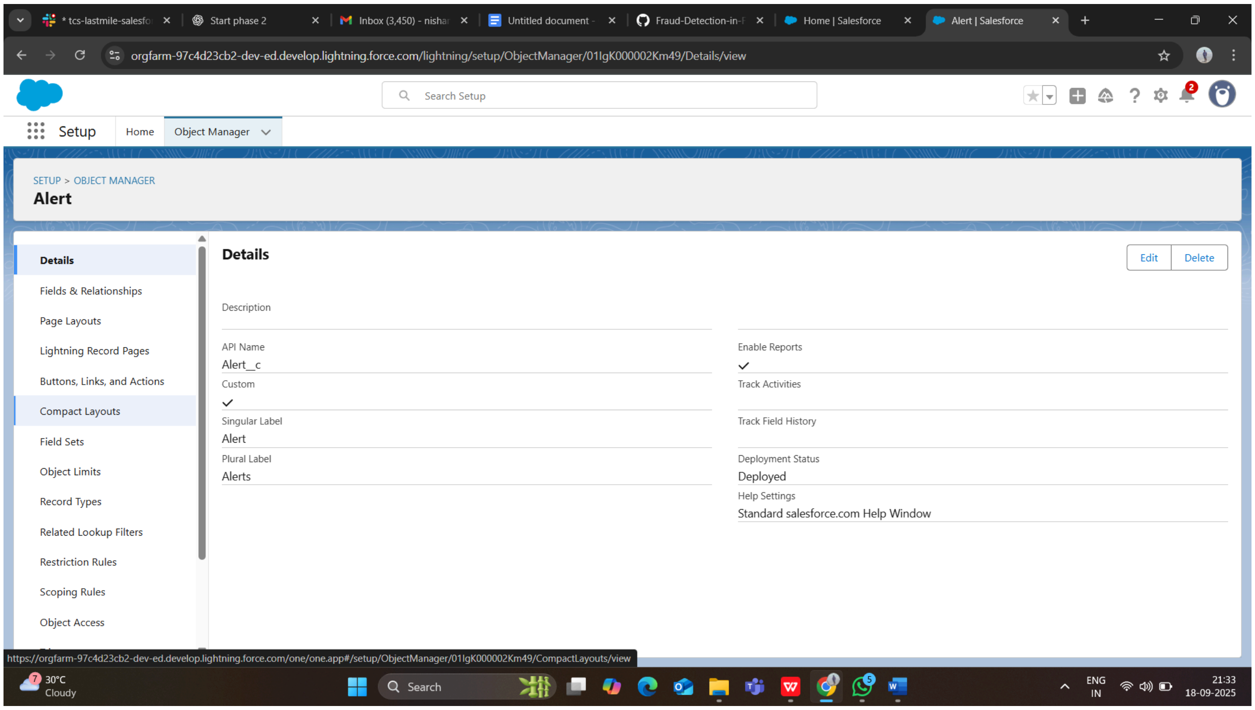
Phase 3: Data Modeling & Relationships

1. Standard & Custom Objects

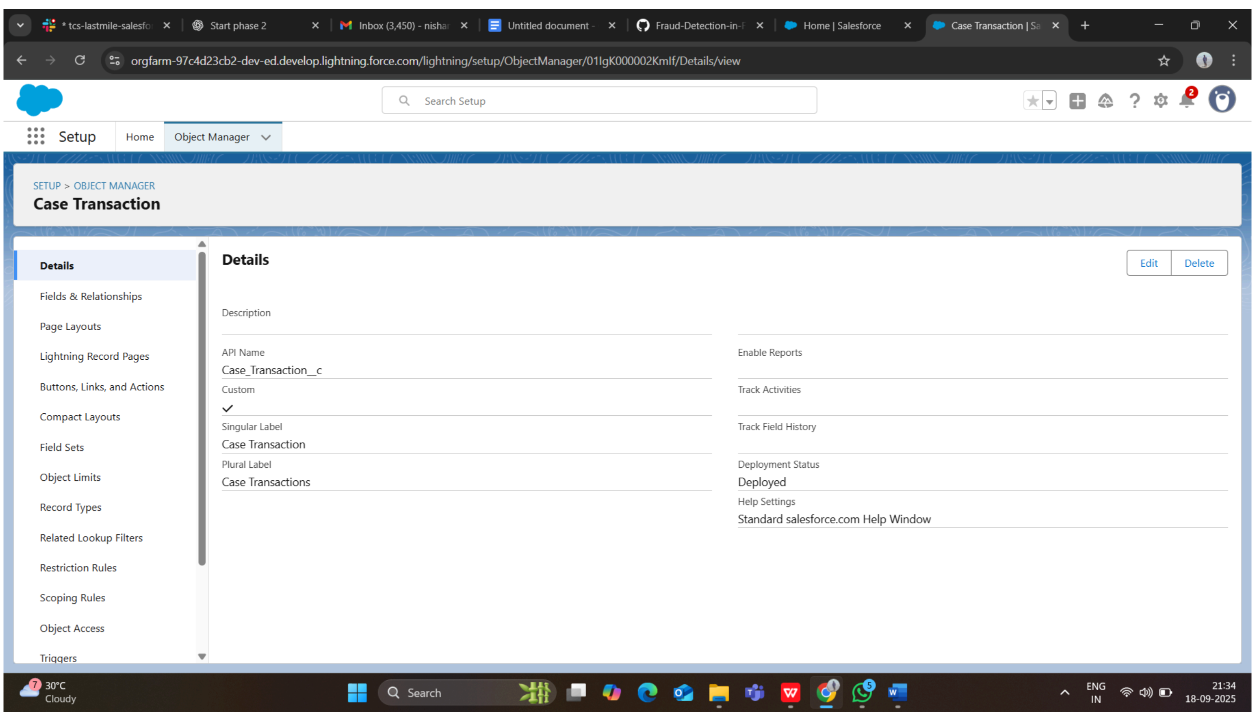
- **Standard:**
    - **Account** (represents customer or business)
    - **Contact** (customer representatives).
- **Custom:**
    - **Transaction** (each financial activity).



- **Alert** (potential fraud case).

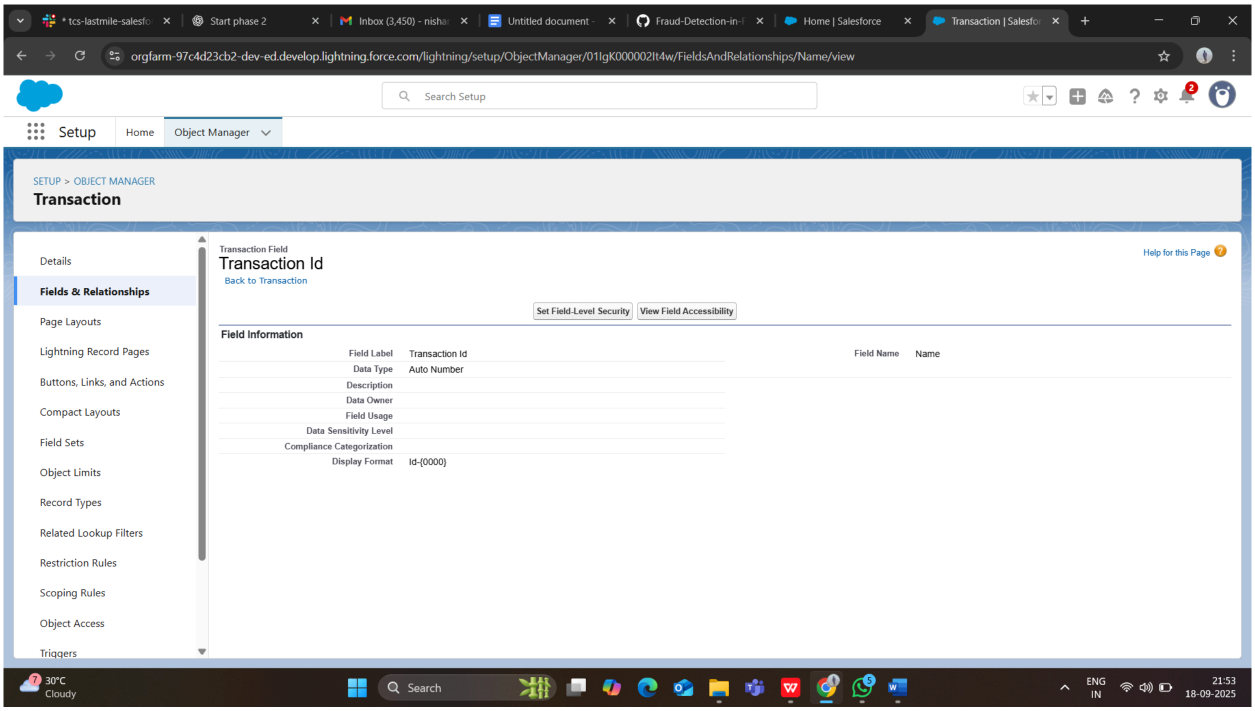


- **Case Transaction** (junction between Case & Transaction if needed).

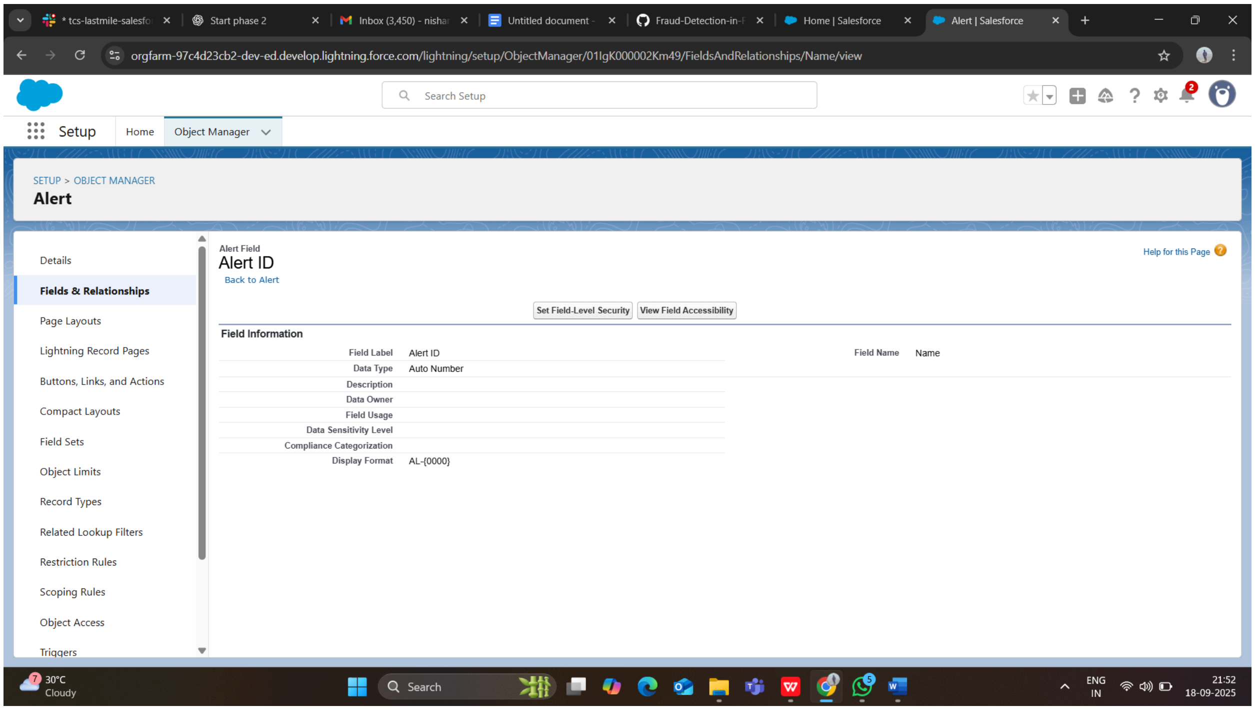


2. Fields

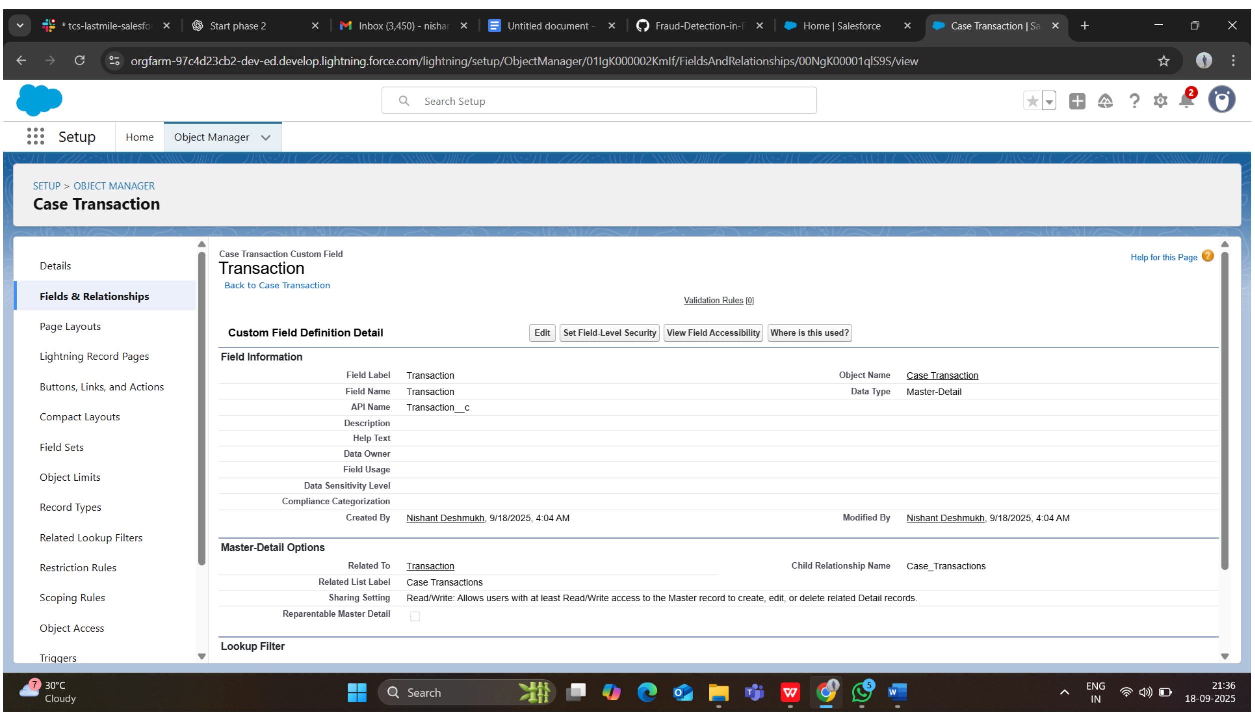
- **Transaction:** Amount, Date, Location, Channel (ATM, Online, POS), Status (Approved/Declined).



- **Alert:** Risk Score, Alert Type (Suspicious Login, Unusual Transaction), Alert Status (Open, Investigating, Closed).



- **Case Transaction (junction):** Links Case with one or more Transactions.



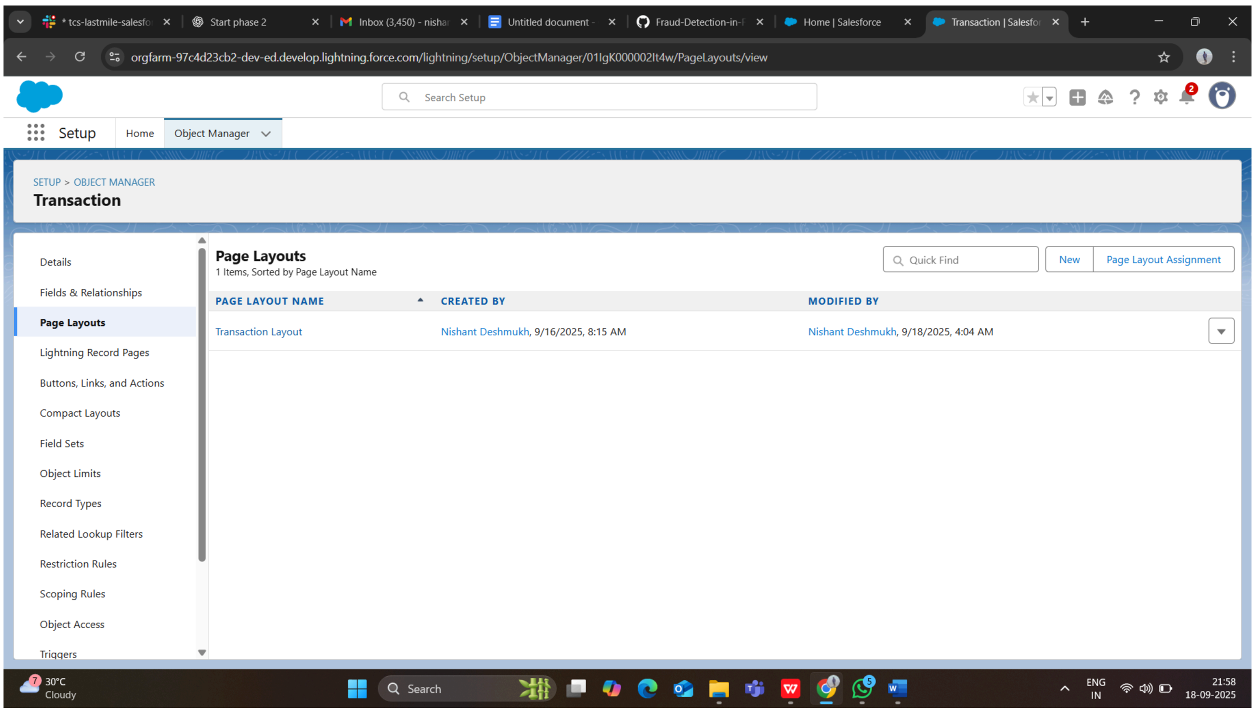
3. Record Types

- **Transaction** → “Domestic Transaction” vs “International Transaction.”
- **Alert** → “High Risk” vs “Medium Risk” vs “Low Risk.”

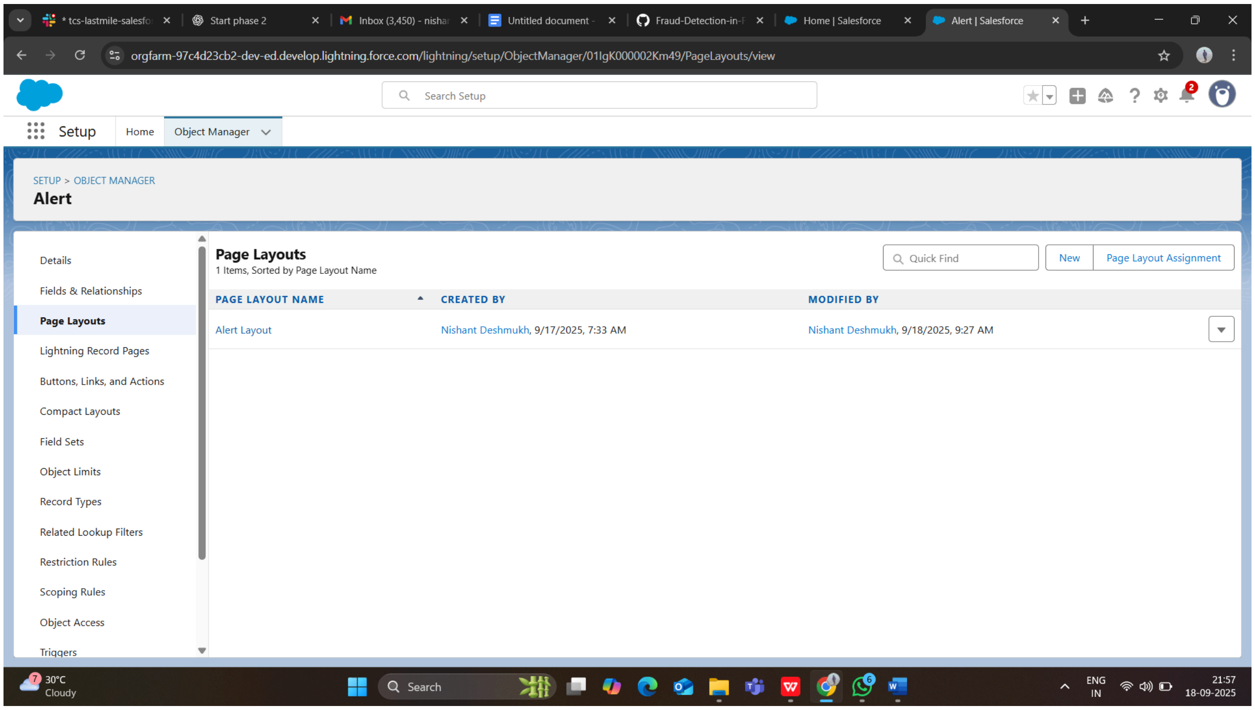
---

4. Page Layouts

- **Transaction page** → shows related customer, alerts, and cases.



- **Alert page** → shows related transactions and assigned fraud analyst.

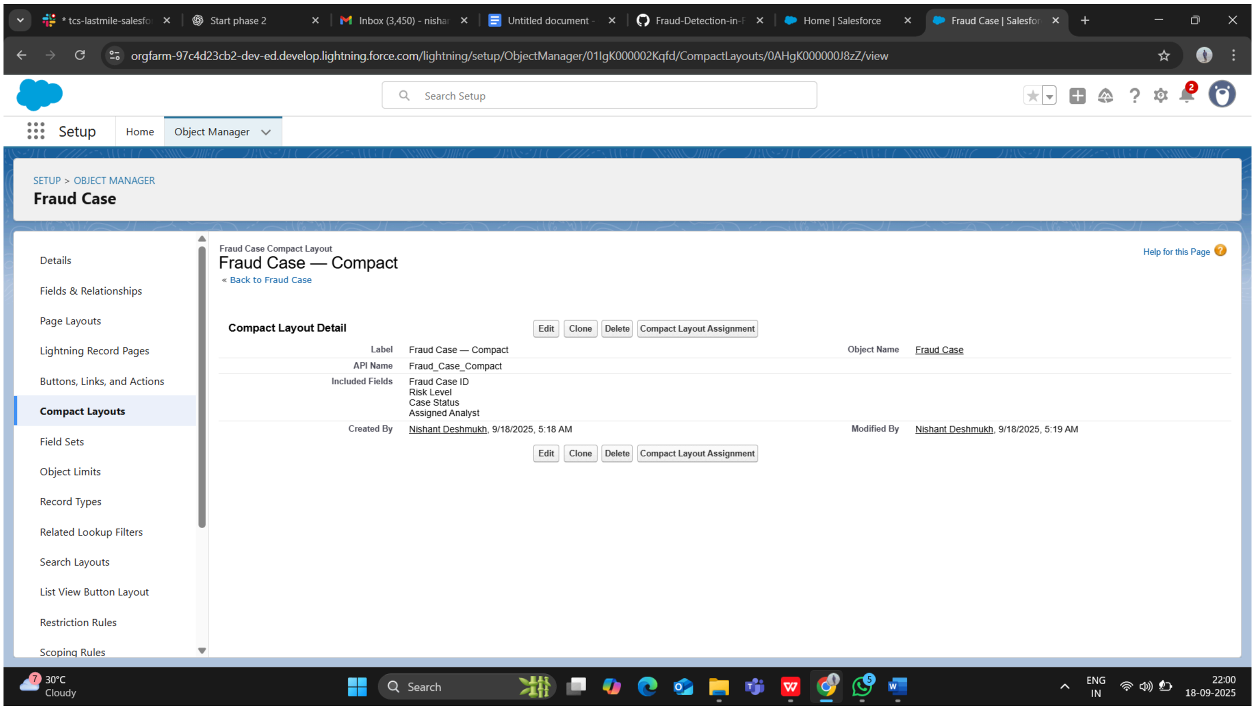


- **Case page** → shows linked alerts and transactions.

---

5. Compact Layouts

- **Mobile (Transaction):** Amount, Date, Status.
- **Mobile (Alert):** Alert Type, Risk Score, Status.

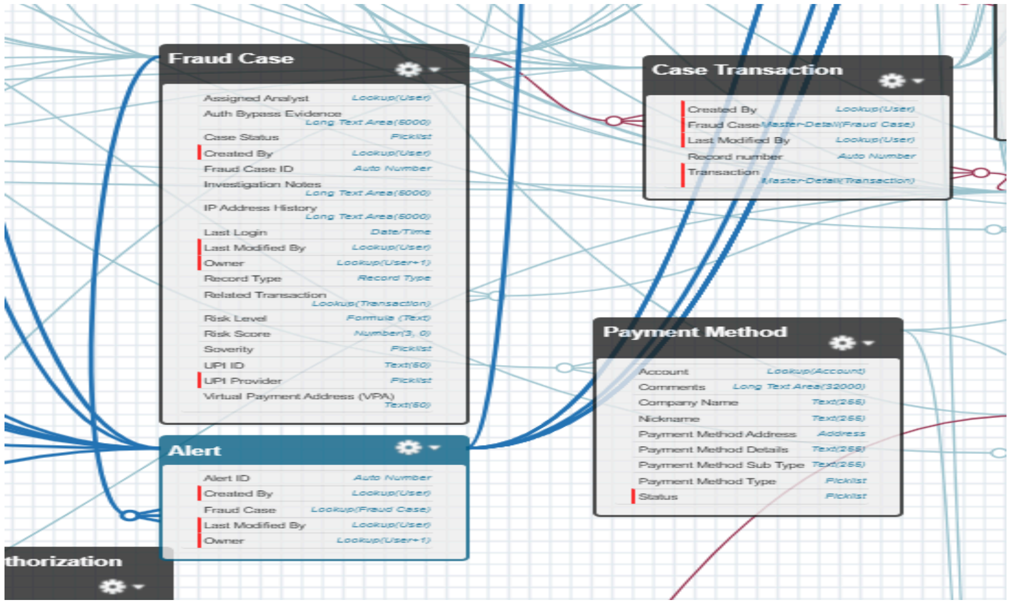


---

6. Schema Builder

- Use **Schema Builder** to visually design:
    - Account → Transaction (Lookup).
    - Transaction → Alert (Lookup).

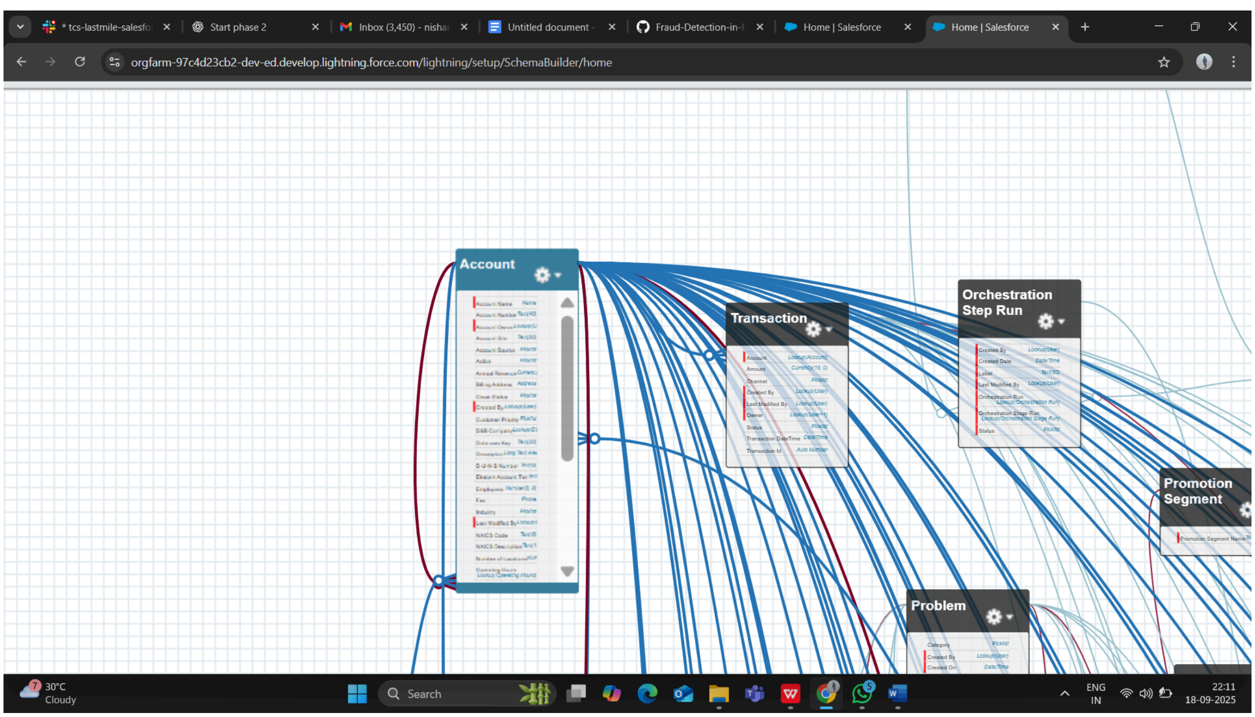
- Case ↔ Transaction (Junction).



---

7. Lookup vs Master-Detail vs Hierarchical

- **Account** ↔ **Transaction** → **Lookup** (transactions don't own accounts, but reference them).



- **Transaction ↔ Alert → Lookup** (one transaction may trigger multiple alerts).

---

8. Junction Objects

- **Case Transaction:**
    - Used when one Case contains multiple suspicious Transactions.
    - Enables many-to-many relationship.

---

9. External Objects

- If fraud detection system integrates with **external banking/credit systems**, use **External Objects** (via Salesforce Connect) to bring in real-time **transaction logs, blacklist databases, or KYC data** without storing them directly in Salesforce.