📋 **Incidents Table & Schema Design - Questionnaire for Foodlobbyin**

Based on your fraud prevention and privacy-first B2B platform

---

1. Incident Data Structure & Core Fields

1.1 Incident Identification & Classification

Already defined in your docs, but let's confirm:

Incident Types (from your DATA_PRIVACY_POLICY.md):

- Payment Default (unpaid invoices, delayed payments) - Yes

- Fraud (fake companies, identity theft, advance payment scams) - Yes

- Quality Issues (substandard goods, wrong products, short delivery) - Yes

- Breach of Contract (unilateral changes, broken promises) – Can be mentioned but I not a major issue. It's a new normal in the industry. But can be allowed to build insights

- Other (custom category)

Question: Are these 5 types sufficient, or do you need additional categories like:

- Delivery/logistics issues? – Not concern

- Communication/responsiveness issues? – Not a concern

- Document fraud (fake invoices, certificates)? – Yes ca be used, but not a major concern.

1.2 Company Identification (Critical for your gated search)

Question: How will you handle companies that have:

- Only GSTN (15-digit)

- Only mobile number (10-digit)

- Both GSTN and mobile

- Neither (e.g., unregistered vendors) - should this be allowed?

Answer: 1. Companies without GSTN can be allowed but will have to create an option to select(Eg. Registered under GST or Unregistered under GST. If Registered then GSTN should be Mandatory to submit. If unregistered, then nt required)

2. Mobile number is not required in Company Data. There will be three database linked to a company. 1. Contact person and 2. Invoices unpaid 3. Other incidents. And then Notes to discuss abut the company(where users can comment and provide insights)

Validation:

- Should the system **require at least one identifier** (GSTN or mobile)?

Ans: Identifier for the registered company should be GSTN by default. But while attempting gated search. Mobile number will lead to contact person which then will lead to company details.

- Should GSTN be validated against a known format (e.g., ^[0-9]{2}[A-Z]{5}[0-9]{4}[A-Z]{1}[1-9A-Z]{1}Z[0-9A-Z]{1}$)?

    Ans: Yes. (In future when projects turn profitable we will valudate with API as well, but create a basic validation for now that do not require API)

1.3 Financial Impact

Question: What financial details should be captured?

- Amount involved (in INR) - Yes

- Currency (if international transactions) - Yes

- Payment terms that were violated - Yes

- Outstanding amount vs. original amount - Yes

- Interest/penalties accrued – Yes (provide a description box to mention why the penelaty was charged and by which department)

2. Evidence & Documentation

2.1 Evidence Table Structure

From your docs, you mentioned evidence upload. **Confirm structure**:

SQL

```
CREATE TABLE incident_evidence (
  id SERIAL PRIMARY KEY,
  incident_id INTEGER REFERENCES incidents(id) ON DELETE CASCADE,
```

```
  file_name VARCHAR(255),

  file_path TEXT,  -- or S3 URL

  file_type VARCHAR(50), -- 'invoice', 'contract', 'email', 'photo', 'video', 'pdf'

  file_size_bytes INTEGER,

  mime_type VARCHAR(100),

  uploaded_at TIMESTAMP DEFAULT NOW(),

  uploaded_by INTEGER REFERENCES users(id),

  is_encrypted BOOLEAN DEFAULT FALSE,

  encryption_key TEXT,

  watermark_applied BOOLEAN DEFAULT FALSE,

  metadata JSONB -- store additional info like date, parties, amounts

);
```

Questions:

- Should evidence files be **encrypted at rest**? (You mentioned this in BUSINESS_VISION.md)

  Will work on encryption later as would require professional help.

- Should evidence have **watermarks** for authenticity?

  No

- Maximum file size per evidence? (e.g., 10MB per file, 50MB total per incident)

  1 MB

- Maximum number of evidence files per incident?

  3

2.2 Evidence Types

Which evidence types should be supported?

- Images (JPEG, PNG, WEBP) - Yes

- PDFs (invoices, contracts) - Yes

- Videos (evidence recordings) - No

- Documents (Word, Excel) No

- Audio recordings - Yes

- Email screenshots - Yes

- WhatsApp chat screenshots - Yes

---

3. Moderation & Workflow

3.1 Moderation Status (from your DAILY_IMPLEMENTATION_PLAN.md)

You mentioned a moderation queue. **Confirm workflow**:

Incident Status Values:

- draft - Reporter is still editing

- submitted - Awaiting moderation

- under_review - Moderator is reviewing

- approved - Published and visible in searches

- rejected - Did not pass moderation

- disputed - Company disputed the claim

- resolved - Issue resolved between parties

- withdrawn - Reporter withdrew the complaint

- archived - Old incident archived

Questions:

- Who moderates? (Platform admin, community, AI-assisted?)

  Will Need to appoint admins from users.

- What's the target moderation time? (24-48 hours per your docs)

  No Time limit.

- Should rejected incidents be visible to the reporter with reason?

  Yes

3.2 Approval/Rejection Workflow

SQL

ALTER TABLE incidents ADD COLUMN moderation_status VARCHAR(20) DEFAULT 'submitted';

ALTER TABLE incidents ADD COLUMN moderation_notes TEXT; -- Admin notes

ALTER TABLE incidents ADD COLUMN moderated_by INTEGER REFERENCES users(id);

ALTER TABLE incidents ADD COLUMN moderated_at TIMESTAMP;

Questions:

- Should there be **multiple moderation levels** (L1 review, L2 review)?

  Can be helpful at the time of peak engagement. But will be confusing at start

- Should **auto-approval** be enabled for trusted users (e.g., after 100+ verified reports)?

  Yes. Admins can tag users as trusted for better functioning

---

4. Company Response Mechanism

4.1 Company Responses Table

From your docs, accused companies can respond. **Confirm structure**:

SQL

```
CREATE TABLE incident_responses (
  id SERIAL PRIMARY KEY,
  incident_id INTEGER REFERENCES incidents(id) ON DELETE CASCADE,
  responding_company_id INTEGER REFERENCES company_profiles(id),
  responding_user_id INTEGER REFERENCES users(id),
  response_text TEXT NOT NULL,
  response_type VARCHAR(20) CHECK (response_type IN ('denial', 'partial_admission', 'full_admission', 'clarification', 'counter_evidence')),
  resolution_offered BOOLEAN DEFAULT FALSE,
  resolution_details TEXT,
  created_at TIMESTAMP DEFAULT NOW(),
```

updated_at TIMESTAMP DEFAULT NOW(),

is_public BOOLEAN DEFAULT TRUE

);

Questions:

- How many responses can a company submit? (One final, or multiple updates?)

  This has to be dealt with consciously. Cannot make the forum a place of mocery. Company can mark the Incident with some predefined tags and can also apply for Hiding of the incident to Moderator so that issue can be solved through other channels. Moderator can undo hidden incident whenever he thinks fit.

  (Please note all the users Identity will be concealed on forum as well in Incident details. Even appointed moderator wont be able to identify the user for complete user privacy)

- Should responses also go through moderation?

  Yes

- Can reporters **reply to company responses**? (threaded discussion?)

  Yes

4.2 Notification to Company

Ans: These function will be added later if required

Questions:

- How should companies be notified?
  - Email to registered email
  - SMS to mobile number
  - In-app notification (if they have an account)
  - All of the above
- What if the company **doesn't have an account** on Foodlobbyin?
- **Ans: These function will be added later if required**

- Should there be a **grace period** before incident goes public? (7 days per your docs)

---

5. Privacy & Audit Trail

5.1 Search Audit Log (from DAILY_IMPLEMENTATION_PLAN.md Day 3)

You need to log all searches for compliance:

SQL

```
CREATE TABLE search_audit_log (

 id SERIAL PRIMARY KEY,

 user_id INTEGER REFERENCES users(id),

 search_type VARCHAR(10) CHECK (search_type IN ('gstn', 'mobile')),

 search_value VARCHAR(50), -- GSTN or mobile searched

 search_timestamp TIMESTAMP DEFAULT NOW(),

 ip_address INET,

 user_agent TEXT,

 results_found INTEGER, -- how many incidents returned

 rate_limit_check BOOLEAN DEFAULT TRUE, -- was rate limit passed

 legitimate_interest_declared BOOLEAN DEFAULT FALSE -- did user declare reason?

);
```

Questions:

- Should **legitimate interest declaration** be mandatory? (text field: "I am considering business with this company")

- How long should search logs be retained? (1 year, 3 years, indefinitely?)

  3 Years

- Should there be **alerts for suspicious search patterns**? (e.g., 100 searches in 1 hour)

  - Yes, 100 Search in one day should be the limit

5.2 Reporter Privacy

Questions:

- Should reporters be **anonymous by default** or identified?

  Only the Admin has the right to seek identification of a user. Rest any other user including Moderator should no be allowed to seek identity. Users should be Anonymous by default.

  Only in one case user can choose to disclose his/her identity is while engaging in forums or commenting on news or Updates.

  In Forums there will be options to create a topic where users should be allowed to comment **anonymously or not. To maintain the decorum.**

- Can reporters choose: [ ] Public (name visible) [ ] Pseudonymous (username visible) [ ] Anonymous - Yes

- Should **verified reporters** get a badge/score boost?

  Will think on it later

---

6. Reputation & Scoring

6.1 Company Reputation Table (from Day 4 of your plan)

SQL

```
CREATE TABLE company_reputation (

  id SERIAL PRIMARY KEY,

  company_gstn VARCHAR(15) UNIQUE,

  company_mobile VARCHAR(15),

  total_incidents INTEGER DEFAULT 0,

  resolved_incidents INTEGER DEFAULT 0,

  disputed_incidents INTEGER DEFAULT 0,

  pending_incidents INTEGER DEFAULT 0,

  total_amount_involved DECIMAL(18,2) DEFAULT 0,

  avg_resolution_days DECIMAL(10,2),
```

reputation_score DECIMAL(5,2) DEFAULT 50.00, -- 0-100 scale

risk_level VARCHAR(20) DEFAULT 'unknown' CHECK (risk_level IN ('low', 'medium', 'high', 'critical', 'unknown')),

last_incident_date DATE,

created_at TIMESTAMP DEFAULT NOW(),

updated_at TIMESTAMP DEFAULT NOW()

);

Questions:

- **Reputation algorithm**: How should incidents be weighted?

    o   All incidents count equally - No

    o   Recent incidents weighted more (decay over time)- Yes

    o   Severity-based weighting (fraud = 10x, quality issue = 2x) - Yes

    o   Amount-based weighting (larger amounts = bigger impact) - Yes

- **Risk level thresholds**:

    o   Low: 0-2 incidents, or all resolved -

    o   Medium: 3-5 incidents, mixed resolution

    o   High: 6-10 incidents, <50% resolution rate

    o   Critical: 10+ incidents, <30% resolution rate, or active fraud reports

Ans: Did not understand this question will required to be discussed furhter

- **Score decay**: Should old, resolved incidents reduce impact over time? (e.g., 50% weight after 2 years) - Yes

---

7. Incident Relationships & Dependencies

7.1 Related Incidents

Questions:

- Should incidents be **linkable**? (e.g., "This is a duplicate of Incident #123") No incident can not be duplicate

- Should incidents support **parent/child relationships**? (e.g., one major fraud with multiple victims) – Yes, Incident can be link to an events (Eg. Liquidation, Bankrupcy and other similar events) Moderator can create an event and link all the incidents to that even. But these are rare cases.

- Should there be a **pattern detection** system? (e.g., "10 companies reported similar fraud from this GSTN") - Yes

7.2 User Reporting History

Questions:

- Should there be a **trust score for reporters**? - Yes

    o   Based on: verified reports, resolution rate, evidence quality - Yes

- Should **serial false reporters** be flagged/banned? - Yes

- Should there be **corroboration** (multiple users report same incident)? – No Incidents are unique to every users. It can so happen that the incident may have happen at the same time. But every incident is a unique incident. Let them submit seperately

---

8. Temporal & Resolution Tracking

8.1 Incident Timeline

Key Timestamps to Capture:

- incident_date - When the incident actually occurred

- reported_at - When it was submitted to platform

- published_at - When it went live after moderation

- company_notified_at - When company was notified

- first_response_at - When company first responded

- resolved_at - When incident marked resolved

- archived_at - When incident archived

Questions:

- How far back can incidents be reported? (1 year, 5 years, unlimited?)

    Unlimited. Incidents can be presented in timelines going back as much as possible.

- Should there be **statute of limitations**? (e.g., incidents >5 years old auto-archived)

  No, we only learn from our past

8.2 Resolution Process

Questions:

- Who can mark an incident as "resolved"?

  - o Only the reporter

  - o Both parties (mutual agreement)

  - o Mediator/admin

  - o Automatic (e.g., after payment proof uploaded)

Reporter and moderator can mark it as resolved. Company can submit a request to moderator and Reporter to do the same.

- Should resolved incidents remain visible? (Yes, per your docs - shows company improved)

---

9. Data Retention & Compliance

9.1 GDPR/Data Protection Compliance

From your DATA_PRIVACY_POLICY.md:

Questions:

- Should incidents have **soft delete**? (hidden but not removed from DB) - Yes in case a reporter is a fraudster himself and using a forum to mislead other. If a reporter is found doing such things Banning reporter should allow moderator to soft delete his submitted reports. To clean database.

- How should **right to erasure** work for incidents?

  - o ~~Anonymize reporter (remove personal info, keep incident)~~

  - o ~~Full deletion (not recommended for fraud records)~~

  - o Mark as "deleted by user request" but keep for legal compliance - Yes

- Retention period:

  - o 7 years (GDPR recommendation for financial records)

  - o 10 years (Indian Companies Act requirement)

- o Indefinitely (fraud prevention justification) - Yes

9.2 Legal Compliance

Questions:

- Should incidents be **exportable for legal proceedings**? (PDF with digital signature) – Yes, but only by a professional. (User can be marked as Legal professional. And can be appointed to certain cases. Will discuss this separately later in detail)

- Should there be a **litigation hold** flag to prevent deletion during legal disputes? - Yes

---

10. Technical Implementation

10.1 Database Choices

From your current setup: **PostgreSQL**

Questions:

- Should incident descriptions support **full-text search**? – No (PostgreSQL tsvector, tsquery)

- Should evidence metadata be stored as **JSONB** for flexibility? – No idea, choose whats better

- Should there be **partitioning** for old incidents? (e.g., by year) Just tag a client with Month and year of signup

10.2 Performance & Scale

Expected Volume (estimate from your goals):

- 100+ verified vendors at launch - Yes

- 50+ incidents in first 6 months - More my be 100 to 500

- 500+ searches per day - Possible

Questions:

- Should there be **caching** for popular searches? (Redis) No (no other user, don't even create a search log)

- Should reputation scores be **precomputed** or calculated on-demand? (Reputation score should be kept under hood and only be launch once perfected) Not to visible to users a t present

- Should there be **read replicas** for search queries? No

10.3 Indexes (Critical for Performance)

SQL

```
-- From your DAILY_IMPLEMENTATION_PLAN.md Day 1

CREATE INDEX idx_incidents_company_gstn ON incidents(company_gstn) WHERE company_gstn IS NOT NULL;

CREATE INDEX idx_incidents_company_mobile ON incidents(company_mobile) WHERE company_mobile IS NOT NULL;

CREATE INDEX idx_incidents_reporter_id ON incidents(reporter_id);

CREATE INDEX idx_incidents_status ON incidents(status);

CREATE INDEX idx_incidents_moderation_status ON incidents(moderation_status);

CREATE INDEX idx_incidents_incident_date ON incidents(incident_date DESC);

CREATE INDEX idx_incidents_created_at ON incidents(created_at DESC);
```

Questions:

- Should there be **composite indexes** for common queries?
    - (company_gstn, status, incident_date)
    - (reporter_id, created_at)
- Should there be **partial indexes** for performance?
    - WHERE status = 'approved' (only live incidents)

    I did not understand this query. Explain me I laymens language

---

11. Notifications & Alerts

11.1 Notification Types

Questions:

- Who gets notified when?
    - Reporter: When incident approved/rejected - Yes
    - Company: When incident published – Not t present

- Company: When resolution requested – Not at present

- Admin: When incident submitted - Yes

- Community: When critical fraud detected (broadcast alert) –

  All the submitted reports are only accessible when user passes a gated search. Only moderators received notification for approving the incident.

11.2 Fraud Alert System (will work on this infuture)

From your BUSINESS_VISION.md:

Questions:

- Should there be **automatic fraud alerts**?

  - New critical incident in your industry

  - Company you searched got a new incident

  - Pattern detected (multiple reports of same scam)

- Delivery method:

  - Email (immediate or daily digest)

  - In-app notification

  - SMS (for critical alerts only)

---

12. Success Metrics & Analytics

12.1 What to Track

Questions:

- Should the system track:

  - Average time to resolution

  - Incident resolution rate by type

  - Reporter response rate

  - Company response rate

  - Evidence attachment rate

  - Search-to-report conversion (users who searched, then reported)

These can be track only for analysing by website owner. Not accessible for user or not a part of webapp feature.

12.2 Reporting Dashboard

For admins/founders:

- Total incidents (by type, by status) - Yes

- Incidents over time (trend)- Yes

- Top reported companies – Only when approved by moderator

- Most active reporters - No

- Average moderation time - No

- Geographic distribution (by state/city) - Yes

---

13. MVP vs. Future Features

13.1 Must-Have for MVP (Day 1-10 from your plan)

- Basic incidents table with GSTN/mobile search - Yes

- Evidence upload (single table, basic file storage) – File storage

- Moderation workflow (simple approve/reject) – Yes

- Company reputation calculation – Not now, let users judge

- Search audit logging - No

13.2 Can Be Added Later (Post-MVP)

- Company response system – Will see

- Advanced pattern detection - Yes

- AI-assisted moderation – No

- Corroboration/voting system - No

- Mediation workflow – can be added in future.

- Incident analytics dashboard – For Website owner only.

Question: Do you want to implement the full system from Day 1, or start with MVP and iterate?

---

14. Final Confirmation

14.1 Schema Summary

Based on your docs, here are the tables we'll create:

1. **incidents** - Core incident reports

2. **incident_evidence** - File uploads (invoices, screenshots)

3. **incident_responses** - Company responses to incidents

4. **search_audit_log** - Privacy compliance & search tracking

5. **company_reputation** - Precomputed reputation scores

6. **incident_moderation_log** - Track moderation actions

Question: Does this structure match your vision?

14.2 Next Steps

Once you answer these questions, I'll:

1. **Generate the complete SQL migration** (003_add_incidents_table.sql)

2. **Create sample seed data** for testing

3. **Design the ER diagram** showing relationships

4. **Write the TypeScript models** (for backend)

5. **Create the repository layer** (CRUD operations)

6. **Define the API endpoints** (for incident submission, search, etc.)

✅ **Action Required**

Please review this questionnaire and:

1. **Answer the questions** marked with [ ] checkboxes

2. **Clarify any uncertainties** about incident workflow

3. **Prioritize features** (MVP vs. future)

4. **Confirm the schema structure** matches your vision

Once I have your answers, we'll move to **implementation** with the exact schema tailored to your requirements! 🚀

I have tried to answer the quest with the best of my understanding. Create further questionaries for better clarity and clarification I required. Also create a document describing database architecture for my understanding before we proceed to Develop.