Fraud Analyst interview questions

careertips.com.au: common questions and what they're really testing

What to expect

Fraud analyst interviews blend technical testing with judgement-based scenarios and regulatory knowledge. Employers want to see how you think through a case, how you use data to support decisions, and how you communicate findings to stakeholders.

- **Technical and data analysis:** Questions on SQL, Python, or R, and how you would query transaction data to surface suspicious patterns.
- **Process and case walkthrough:** Step-by-step scenarios that ask you to take a flagged account from alert to resolution.
- **Behavioural:** Past examples of identifying fraud, working under pressure, or collaborating with compliance and legal teams.
- **Scenario and judgement:** Hypothetical situations that test how you weigh risk, handle ambiguity, and decide when to escalate.
- **Regulatory and compliance:** Questions on AUSTRAC reporting, the AML/CTF Act, and your obligations when you suspect financial crime.
- **Stakeholder communication:** How you explain complex findings to non-technical audiences such as management or internal audit.

Interviews usually start with a short phone screen covering your background and motivation, followed by a technical assessment or case study. The final stage often involves a panel with the hiring manager and a compliance or risk representative, where you walk through a real or hypothetical fraud case and discuss how you would report it.

1. Walk me through how you would investigate a flagged account from alert to resolution.

Why they ask

This tests your process knowledge and whether you understand the end-to-end workflow, including documentation and escalation.

How to structure your answer

Use a chronological walk-through: acknowledge the alert, gather data, assess against known typologies, decide on next steps, escalate or close with clear reasoning, and document everything.

Example answer

“First, I would review the alert details and the transaction history in the case management system. I would check whether the activity matches known fraud typologies, such as structuring, rapid movement of funds, or unusual merchant categories. If it does, I would pull additional data using SQL, looking at the customer's profile, device information, and recent changes to contact details. I would then assess the risk level: if there is a strong indication of fraud, I would escalate to the financial crime team and prepare a suspicious matter report for AUSTRAC. If the activity is explainable, I would document why I closed the alert and update any relevant rules to reduce false positives.”

2. Tell me about a time you identified a fraud pattern that others had missed.

Why they ask

This behavioural question looks for proactivity, analytical thinking, and the ability to spot anomalies in data.

How to structure your answer

Use STAR: Situation, Task, Action, Result. Keep the result focused on what changed because of your action.

Example answer

“At my previous role, we were seeing a rise in account takeover complaints, but the existing rules were not catching them early. I noticed that many of the compromised accounts had a small test transaction from a new device just before the larger fraudulent withdrawal. I built a SQL query to flag accounts with that pattern and worked with the team to add a new detection rule. The rule started alerting us to suspicious devices before the main fraud occurred, and we were able to contact customers to secure their accounts. The pattern was later incorporated into our standard monitoring.”

3. You notice a transaction pattern that looks like money muling but the customer has a long history with the bank. What do you do?

Why they ask

This scenario tests judgement, risk assessment, and how you balance customer relationships with regulatory obligations.

How to structure your answer

Assess, prioritise, action, escalate: outline your immediate assessment, how you weigh the customer history, what steps you take, and when you escalate.

Example answer

“I would start by reviewing the pattern in detail. Money muling often involves multiple small deposits from different sources followed by a large transfer out. Even with a long-standing customer, I cannot ignore the red flags. I would check if there are any legitimate explanations, such as a business account or a known payment schedule. If the pattern remains suspicious, I would escalate to the financial crime team and prepare a suspicious matter report. I would also document my reasoning, including why the customer history did not outweigh the indicators. If it turns out to be a false positive, I would note that for future rule tuning.”

4. How would you write a SQL query to identify accounts with multiple small deposits followed by a large withdrawal?

Why they ask

This technical question checks your SQL skills and your ability to translate a fraud typology into a query.

How to structure your answer

Clarify the data structure, outline the query logic step by step, explain the output, and mention how you would validate results.

Example answer

“I would first confirm the table structure: transactions with account_id, amount, transaction_date, and transaction_type. I would write a query that groups transactions by account_id and a time window, say 24 hours. I would count deposits under a certain threshold, sum them, and then check for a withdrawal that is significantly larger than the sum of those deposits. I would use a subquery or a window function to compare the deposit total to the withdrawal amount. The output would be a list of accounts that meet the pattern. I would validate by checking a sample of accounts manually and sharing the query with the team for review before turning it into a detection rule.”

5. What are your obligations under the AML/CTF Act when you identify suspicious activity?

Why they ask

This tests your regulatory knowledge and understanding of AUSTRAC reporting requirements.

How to structure your answer

Recall the key obligations, apply them to the situation, explain the documentation and escalation process, and note any timelines.

Example answer

“Under the AML/CTF Act, I must report suspicious matters to AUSTRAC as soon as practicable. That means I would document the activity, my reasoning, and the evidence, and then submit a suspicious matter report through the appropriate channel. I would also ensure the customer is not tipped off, as that is a criminal offence. I would follow my organisation's internal escalation process, which usually involves a review by the financial crime team before submission. I would keep a record of the report and any follow-up actions.”

6. Describe a time you had to explain a complex fraud finding to a non-technical stakeholder.

Why they ask

This assesses your written and verbal communication, and whether you can make technical findings accessible.

How to structure your answer

Use STAR, focusing on how you tailored your explanation and what the stakeholder did as a result.

Example answer

“I once identified a complex pattern of merchant collusion that involved multiple accounts and different transaction types. The findings were technical, involving SQL queries and rule logic. I had to present this to a senior manager in internal audit who was not familiar with the data. I created a one-page summary with a simple flowchart showing the flow of funds and a table of key transactions. I avoided jargon and focused on the risk and the recommended action. The manager approved additional monitoring and used my summary to brief the wider team. The report was later used as evidence in a review of our controls.”