COBRA KAI DAY · MAY 11, 2026 · BREAKOUT SESSION

Fraud Detection Case Study

From Manual Investigation to AI-Augmented Workflows

CPE CODE : WAXOFF

Session Description

This interactive breakout session presents participants with a realistic fraud scenario and invites them to design an end-to-end investigation workflow using the methods and tools they currently rely on. Through guided discussion, attendees will identify the data sources they would review, the steps they would take to validate concerns, and the challenges they commonly face in manual investigations.

The session then explores how artificial intelligence and data-driven tools can be applied to accelerate evidence gathering, improve consistency, and support clearer documentation, while preserving professional judgment and governance requirements. Participants will leave with a practical understanding of where AI can enhance existing workflows rather than replace them.

Learning Objectives

Participants will learn how to:

- Outline a structured, end-to-end fraud investigation workflow using current practices
- Identify common bottlenecks and risks in manual review and documentation processes
- Recognize practical opportunities where AI and data tools can augment speed, consistency, and decision support while maintaining human oversight and accountability

Participant Name: ______________________

Organization / Team: ______________________

How to use this workbook

Work through each section individually first, then share with your group. There are no right answers — the goal is to surface how your team actually works and where friction exists. The facilitator will debrief each exercise as a full group.

This is a participant workbook — write directly in it, or on the blank lines provided.

The Scenario: The ABC Company Vendor Concern

READ THIS CAREFULLY — the scenario is the basis for all exercises.

Background

ABC Company is a mid-size organization with approximately 1,200 employees across three locations. The Accounts Payable function processes around 4,000 invoices per month with an auto-approval threshold of $10,000. Invoices below $10,000 are auto-approved by the AP system once the AP Manager confirms the vendor and invoice are valid. Invoices at or above $10,000 require Director-level sign-off with documented review.

The Alert

An internal controls analyst running a quarterly exception report notices an unusual concentration of invoices from a vendor referred to here as Vendor X. The report flags the vendor because:

- Vendor X was registered in the vendor management system 7 weeks ago
- 13 invoices totaling $127,400 have been approved over the past 90 days
- All 13 invoices fall between $9,500 and $9,950 — just under the $10,000 auto-approval threshold
- All 13 were approved by the same Accounts Payable Manager: John Doe
- Invoice descriptions are vague: "operational supplies," "facility materials," "maintenance items"

Additional Context Uncovered During Initial Triage

A brief look at the vendor registry reveals the following:

- Vendor X was incorporated 9 weeks ago — 2 weeks before being registered as a vendor
- The registered business address for Vendor X is "Suite 3B" at a small commercial building
- A second recently-registered vendor, Vendor Y, is registered at "Suite 3A" of the same building — the adjacent unit
- Vendor Y has received $34,200 in invoices over the same 90-day window, also approved by John Doe
- A conflict-of-interest disclosure search shows that John Doe disclosed a relative relationship with "J. Doe" — the listed owner of Vendor X — four years ago, but no annual refresh has been completed since
- No purchase orders, contracts, statements of work, or delivery receipts are on file for either vendor

At-a-Glance Summary

	Vendor X	Vendor Y
Vendor registered	7 weeks ago	9 weeks ago
Total invoices	13 invoices, 90 days	8 invoices, 90 days
Total spend	$127,400	$34,200
Invoice range	$9,500 – $9,950	$3,200 – $9,800
Approver	John Doe (AP Mgr)	John Doe (AP Mgr)
Documentation	None on file	None on file
Address	Suite 3B, same building	Suite 3A, same building
Conflict of interest	John Doe disclosed relative as owner	Unknown

Important framing for this session

This scenario intentionally combines multiple fraud signals: threshold splitting, related-entity vendors, a potential conflict of interest, and missing documentation. In the real world, these signals are rarely this concentrated — but they are often this subtle individually. Your job in each exercise is to think about what you would do, not what the right answer is.

Remember: the scenario presents concerns, not conclusions. No verdict has been reached.

EX 01

Map Your Current Investigation Workflow

Individual exercise | 10 minutes, then group share

You've just received the alert described in the scenario. Using your current tools, processes, and team structure, map out how you would investigate this from start to finish.

#	Investigation Step	Data Source / Tool You'd Use	Estimated Time
Ex.	*Review the flagged transaction report*	*ERP export / AP module*	*30 min*
1			
2			
3			
4			
5			
6			
7			
8			

Total estimated time for this investigation:
From alert to documented findings: ________________ hours / days

Reflection questions — answer individually, then discuss:

1. What is the first thing you would do — and why that first?

2. Which step in your workflow would take the longest, and why?

3. At what point (if any) would you escalate before completing the full investigation?

EX 02

Where Does Your Process Break Down?

Group exercise | 10 minutes

For each bottleneck category below, rate how significant this challenge is in your current environment, then note the specific friction you experience.

Bottleneck	Severity (1 Low – 5 High)	Describe the specific friction in your environment
Data Access — pulling records from multiple systems takes significant time	___ / 5	
Volume — too many alerts to investigate thoroughly, so some get triaged away	___ / 5	
Documentation — findings are hard to write up consistently and completely	___ / 5	
Policy Knowledge — locating the exact policy clause that applies takes time	___ / 5	
Precedent — no easy way to check how similar cases were handled before	___ / 5	
Escalation — unclear when a finding warrants escalation vs. a note in the file	___ / 5	
Human Factors — investigator fatigue, inconsistent judgment across team members	___ / 5	
Speed — by the time investigation is complete, the fraud window has stayed open longer than ideal	___ / 5	

Group Discussion Questions

Discuss with your table and capture key points below:

A. Which bottleneck from the table above came up most consistently across your group?

B. In the ABC Company scenario specifically, what would your team struggle most to verify — and why?

C. Has your team ever closed or de-prioritized an alert not because it was clean, but because you ran out of time or resources? What happened?

EX 03 Where Could AI Help — and Where Should It Not?

Group exercise | 10 minutes

For each task in the investigation, decide where AI assistance would add the most value. Use the key below, then add your reasoning.

HIGH VALUE — AI clearly faster/better	SOME VALUE — AI assists, human leads	LOW VALUE — Human judgment essential	? UNSURE — depends on your environment

Investigation Task	Rating (?)	Why? What would AI actually do here?
Pull all transactions for both vendors over 90 days		
Flag threshold-proximity pattern across invoice amounts and dates		
Look up vendor registration dates, addresses, and ownership		
Check for shared address or related entity connections between the two vendors		
Search internal compliance policies for split-invoice rules		
Retrieve similar past cases and how they were resolved		
Cross-reference conflict-of-interest disclosures against vendor contacts		
Assess whether the invoice descriptions suggest a single project or scope		
Write up a structured summary of findings for the investigating auditor		
Decide whether to ESCALATE, MONITOR, or CLOSE the case		

Sign off on the final investigation outcome		

Something to watch for in your table's answers

Most groups rate the last two rows (decide the outcome, sign off) as low value — and they're right. The test of a well-designed AI tool is whether it enforces that line, not just in the UI, but in how it frames its output. If the tool says 'this is fraud' rather than 'here is the evidence,' the governance model has failed.

EX 04

Redesign the Workflow With AI in the Loop

Group exercise | 10 minutes

Using what you mapped in Exercises 1–3, sketch a revised investigation workflow that incorporates AI assistance where appropriate. You don't need to name specific tools — focus on the logic of the workflow.

Current Workflow Step	With AI: What Changes?
FINAL DECISION — ESCALATE / MONITOR / CLOSE	**This step stays with the human auditor. Always.**

Full-Group Debrief Discussion

The facilitator will lead a 10-minute group debrief. Use this space to capture key points from the conversation.

What surprised your group most about where AI could — or couldn't — add value?

What governance or oversight concerns came up in your group when discussing AI in this workflow?

If you were presenting a proposal to use AI for fraud investigations at your organization, what would your leadership's top two objections be?

Key Principles: AI in Fraud Investigation

These principles apply regardless of which tool or platform you use.

01

The AI gathers evidence. The human makes the call.

AI is exceptionally good at pulling data, cross-referencing sources, applying rules, and writing structured summaries. It is not appropriate — technically or ethically — to let it render verdicts on complex, contextual cases where accountability matters. Every investigation outcome must carry a human signature.

02

Transparency is a control requirement, not a preference.

Any AI tool used in a fraud investigation context must explain its reasoning: which evidence it found, which policy it applied, which historical case it cited. 'The AI flagged it' is not audit documentation. If you cannot trace the AI's reasoning, you cannot defend the outcome.

03

Consistency is a feature, not a side effect.

The most underrated benefit of AI in auditing isn't speed — it's consistency. The AI applies the same logic to alert #1 and alert #10,000, regardless of who is on shift, how many alerts came in this week, or how experienced the analyst is. That consistency is itself a control.

04

Your judgment is more valuable now, not less.

When AI handles the mechanical work of an investigation — pulling records, finding policy clauses, drafting summaries — you are freed to spend your time on the cases that require genuine professional judgment: the ones with ambiguous context, competing explanations, or significant stakes. That is the highest use of an auditor's expertise.

My Personal Takeaways

What are the two or three things you want to take back to your team from today's session?

Continue the conversation

The scenario, data, and tools demonstrated in the main session are built on publicly available open-source frameworks for AI agents and document retrieval. If you want to explore building a similar capability for your organization, the architecture is approachable and the core stack is free.

Cobra Kai Day 2026 · Fraud Detection Case Study · 3:45–4:35 PM