Hani Yacoub

Fraud Prevention • AI Abuse • Enforcement Operations @AWS

Berlin, Germany · hani_yacoub@hotmail.com · https://linkedin.com/in/hani1995 · https://haniyacoub.com

PROFESSIONAL SUMMARY

Fraud prevention analyst at AWS. 6+ years in data, risk, and abuse analytics. I build LLM-powered investigation agents, design detection rules across the full account population, and identify how AI services are exploited by fraud actors. I manage precision/recall tradeoffs, build enforcement processes from scratch, and coordinate across engineering, policy, and data science.

CORE SKILLS

Large Language Models & AI Agents · Adversarial Detection & Threat Modeling · Machine Learning (XGBoost, Classifiers) · Enforcement Systems & Policy Design · Python • SQL • Data Pipelines · Cross-Team Coordination & Process Building · Precision/Recall & False-Positive Analysis · Dashboards & Operational Reporting

PROFESSIONAL EXPERIENCE

Fraud Prevention Analyst – AWS Payments & Fraud Prevention

Amazon Web Services (AWS) · Mar 2026 – Present · Berlin, Germany

AI Abuse Detection & Tooling

- First to characterize a novel AI-abuse pattern on an enterprise code-generation service: one payer enrolling thousands of seats on stolen cards to burn model credits, invisible to standard spend controls. Proposed an org-level credit-velocity tripwire.
- Built Claude-based investigation agents that evaluate account signals, automate evidence gathering, and generate enforcement reports. Reduced investigation time from ~1 week to 1 day. Defined output evaluation criteria and operational framework from scratch.
- Built an agent to surface sleeper-account fraud patterns, backed by an XGBoost model (billing spikes, linked accounts, IP-country, payment instruments, risk-score history) with a Streamlit investigation queue.

Enforcement Rules & Systems

- Designed a fraud detection rule using domain age and email-authentication signals. Recall: hundreds of abusive accounts caught. Collateral: near-zero impacts to legitimate customers.
- Added device fingerprint as an ensemble feature to the Fraud Relations model. Result: 34% more disputed dollars caught. Quantified false-positive tradeoffs per signal.
- Traced a $1.17M SageMaker abuse case (1,966 jobs, 740K instances) to a regex gap in enforcement code. Identified the root cause and specified the fix for engineering. Deployed an hourly alert to detect recurrence.

Large-Scale Investigations

- Led analysis of a regional fraud-reporting threshold breach. Proved a coordinated ring (not general population fraud) was the driver. Isolated chargebacks to a handful of accounts. Overturned prior assumptions; enabled targeted enforcement.
- Built a fraud-ring detection framework scoring accounts across 13 signals (fingerprint, BIN, ASN, IP, bank, email domain, time zone). 91% of ring members shared 5+ signals. Dispositioned hundreds of accounts with per-account safety carve-outs.
- Built the first fraud-and-revenue dashboard for AWS new EU region. Surfaced fraud-to-revenue ratio and reversal rates for enforcement prioritization.

False-Positive Prevention

- Reversed fraud calls on legitimate accounts. Example: proved a $4.29M flagged-OPEX account was reserved-but-unused GPU capacity (VC-backed startup). Proved a shutdown was a billing soft-decline, not fraud.
- Built verification workflows and enforcement SOPs with carve-out gates for bulk shutdowns. Protected legitimate accounts from false enforcement. Quantified exposure for stakeholder sign-off.

Senior Product Analyst – Risk & Abuse

Zalando · Apr 2024 – Mar 2026 · Berlin, Germany

- Investigated bot networks, account takeovers, and refund abuse across European markets. Translated findings into enforcement policy recommendations and product decisions.
- Developed a "remaining fraud damage" metric comparing refund rates across segments. Quantified unmitigated fraud; informed defensive investment priorities.
- Measured financial impact of refund and account abuse (Databricks, Azure). Built dashboards consumed by Risk, Product, and Finance leadership.

Data Analyst – Customer Acquisition

AUTO1 Group · Oct 2021 – Apr 2024 · Berlin, Germany

- Built scoring systems to identify high-value B2B customers and churn risk. Enabled the commercial team to prioritize outreach.
- Identified highest-impact retention opportunities from customer drop-off patterns. Quantified revenue upside.

Quantitative Analyst Intern – Energy Markets

Statkraft · Jul 2020 – Feb 2021 · Düsseldorf, Germany

- Built quantitative models for market access analytics across wind, solar, and hydropower assets.

PROJECTS

- **Renitor** — Built and published Renitor, a VS Code extension (v1.75) for multi-agent AI coding: repo-aware handoffs that carry an unfinished task across 11 coding agents (Claude Code, Codex, Cursor, and more), a multi-model chat with automatic failover when a provider hits its usage cap, and a deterministic safety layer that reviews risky commands before they run. Local-first, zero telemetry. (renitor.com)
- **Preflights** — Built Preflights, a pre-import QA tool for Shopify and Google Shopping: a deterministic validation engine that inspects supplier CSVs against live store exports and flags irreversible import risks — variant deletion, handle collisions, price and stock conflicts — in a safe / review / blocked report. AI is used only to explain findings and suggest fixes, never to decide.

EDUCATION

- **Self-directed ML-engineering curriculum — fraud-ML focus (ongoing)** — Structured 12-month program: hand-built implementations before libraries, verified against independent implementations at full data scale, 2026 –
- **Data Engineering with AWS — Nanodegree** — Udacity, 2024 – 2025
- **Master's Degree, Business Management** — SRH Berlin University of Applied Sciences, 2018 – 2021