

GenA.I. Sandbox Cohort 2 Use Case – Livi Bank

Turning Facial Recognition Images into Investigative Intelligence

For faster, more dynamic financial crime investigations

THE OPPORTUNITY

Move beyond manual review and fixed-pattern detection.

A.I. can search and compare onboarding and authentication images, helping investigators surface relationships that traditional account review may miss.

SANDBOX AT A GLANCE

- ~30,000 synthetic images
- 2,000+ masked production images
- 3 models benchmarked
- Quantitative + Financial Crime Compliance (FCC) investigator review

WHAT WE SET OUT TO SOLVE

ADAPT FASTER

Introduce new suspicious scenarios through image search, reducing reliance on repeated model retraining.

FIND HIDDEN LINKS

Connect images through shared backgrounds, objects, and environments, even when photos are captured from different angles or lighting.

SCALE INVESTIGATIONS

Search large image repositories more efficiently and prioritize potentially related cases for investigator review.

WHY IT MATTERS FOR FINANCIAL CRIME INVESTIGATIONS

- Reveal potential relationships across seemingly unrelated customer accounts.
- Reduce manual review across large facial-recognition image repositories.
- Support faster response to emerging fraud typologies without extensive labeled-data preparation.
- Detect suspicions from images.
- Create a foundation for dynamic AML and fraud risk assessment.
- Extend investigation beyond transaction data into contextual visual signals.

THREE MODELS, COMPLEMENTARY STRENGTHS

LIGHTWEIGHT

Enables efficient and reliable image-based risk assessment with lower computing requirements.

BALANCED

Strong retrieval performance with a favorable balance of accuracy and efficiency.

LARGE SIZE BUT MORE CAPABLE

Strongest contextual understanding, semantic retrieval and text-to-image search in the sandbox.

RESULTS & ROADMAP

From Strong Sandbox Results to Pragmatic Adoption

Balancing investigative value, privacy controls, and infrastructure readiness

TOP PERFORMER

Large Size But More Capable Model

Led the benchmark on image retrieval and ranking, including Recall@K, MRR@10 and nDCG@10.

FCC QUALITATIVE TESTING

100% within Top 30

Correct match located within the top 30 results in the reported investigator tests, versus 85% average accuracy for the lightweight model.

RESPONSIBLE TESTING BY DESIGN

PRIVACY

Production data were masked before sandbox use.

SECURITY

Data transfer to the Cyberport sandbox was conducted through an encrypted channel.

VALIDATION

MMEB-V2-style quantitative evaluation was complemented by manual FCC investigator assessment.

RECOMMENDED PATH TO PRODUCTION

NOW

Deploy Lightweight model first

Use the lightweight model to establish practical image-similarity capability in the Bank's current CPU-based environment.

BUILD

Strengthen A.I. platform

Develop scalable compute, model hosting, and A.I. service capability to support more advanced multimodal models.

SCALE

Advance to richer intelligence

Evaluate migration to higher-performing models and expand into dynamic risk assessment and deepfake detection.

THE TAKEAWAY The sandbox validated image intelligence as a viable new capability for FCC. A larger, more capable model showed the strongest investigative potential, while the lightweight model offers the most practical entry point today. A phased approach enables Livi Bank to capture near-term value while building toward a more advanced enterprise A.I. capability.