

Anti-Fraud Face Watch List (FWL)

livi offers a comprehensive **Face Watch List ("FWL")** solution, which leverages a machine learning model to compare facial images against the customer database. This enhances the Bank's capability to detect digital fraud activities and assist in identifying controllers of mule accounts within the Bank.

How does it work?

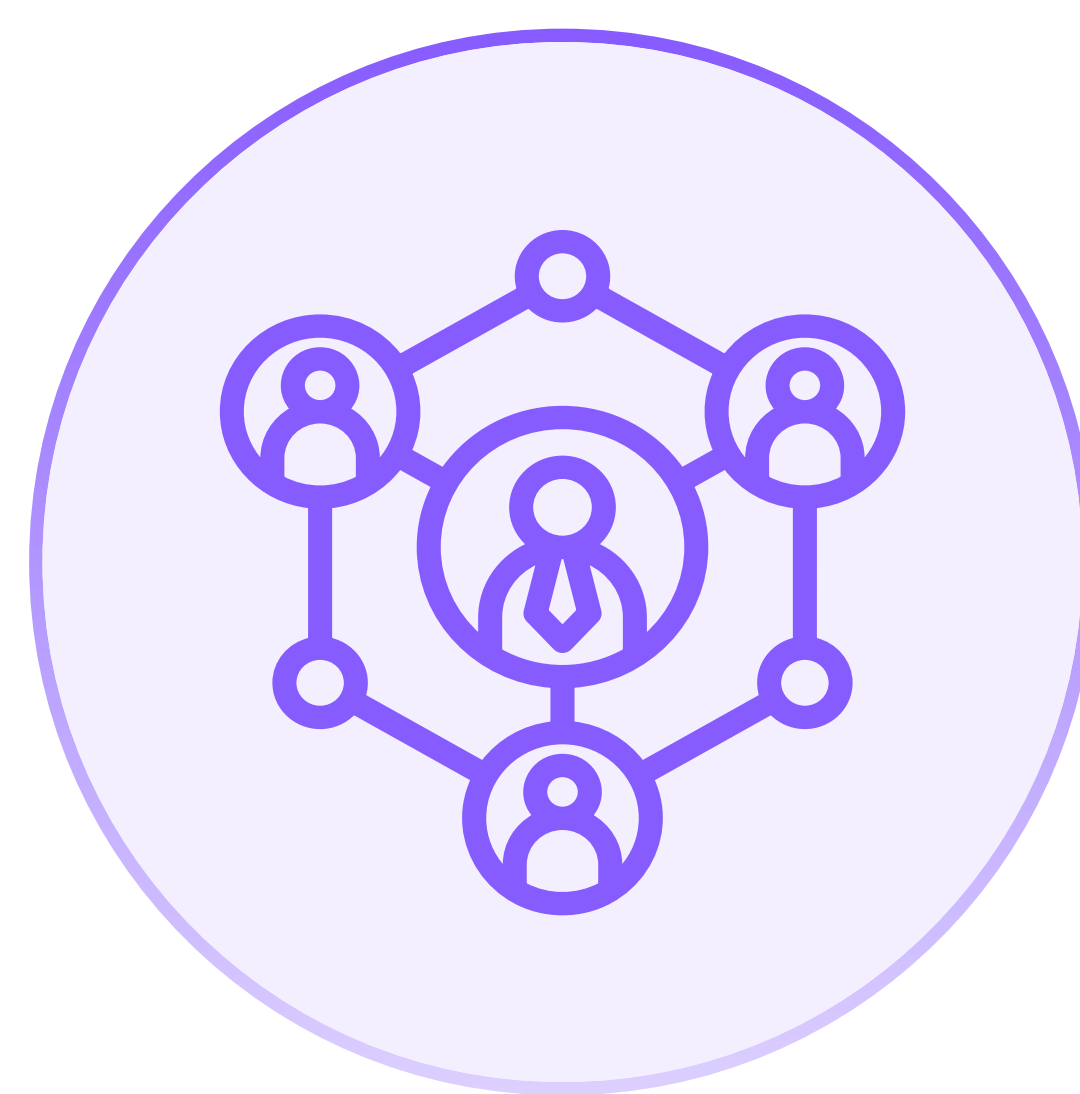
The FWL solution extracts facial tract features from any image and compares them to the selfie images in the Bank's database. This comparison process can be completed in seconds.



Current use cases in livi



**1:N comparison in
money laundering
and fraud
investigation**



**N:N comparison in
detecting multiple
account opening
attempts**



**Blacklisting
suspicious selfie
image**

In response to the evolving digital fraud trend and market pain points, livi has optimised the FWL Solution through the **GenAI Sandbox**, enabling it to detect potential mule accounts or fraud accounts from suspicious backgrounds in the facial recognition images.

Market Pain Points

- **Loan applications with fake identity**
- **Mule accounts**
- **Account takeover**
- **Deepfake/injection attack**

Outcomes



Assist in identifying the controllers of mule accounts



Protect victim account from being taken over



Establish early risk alert mechanism using unstructured data

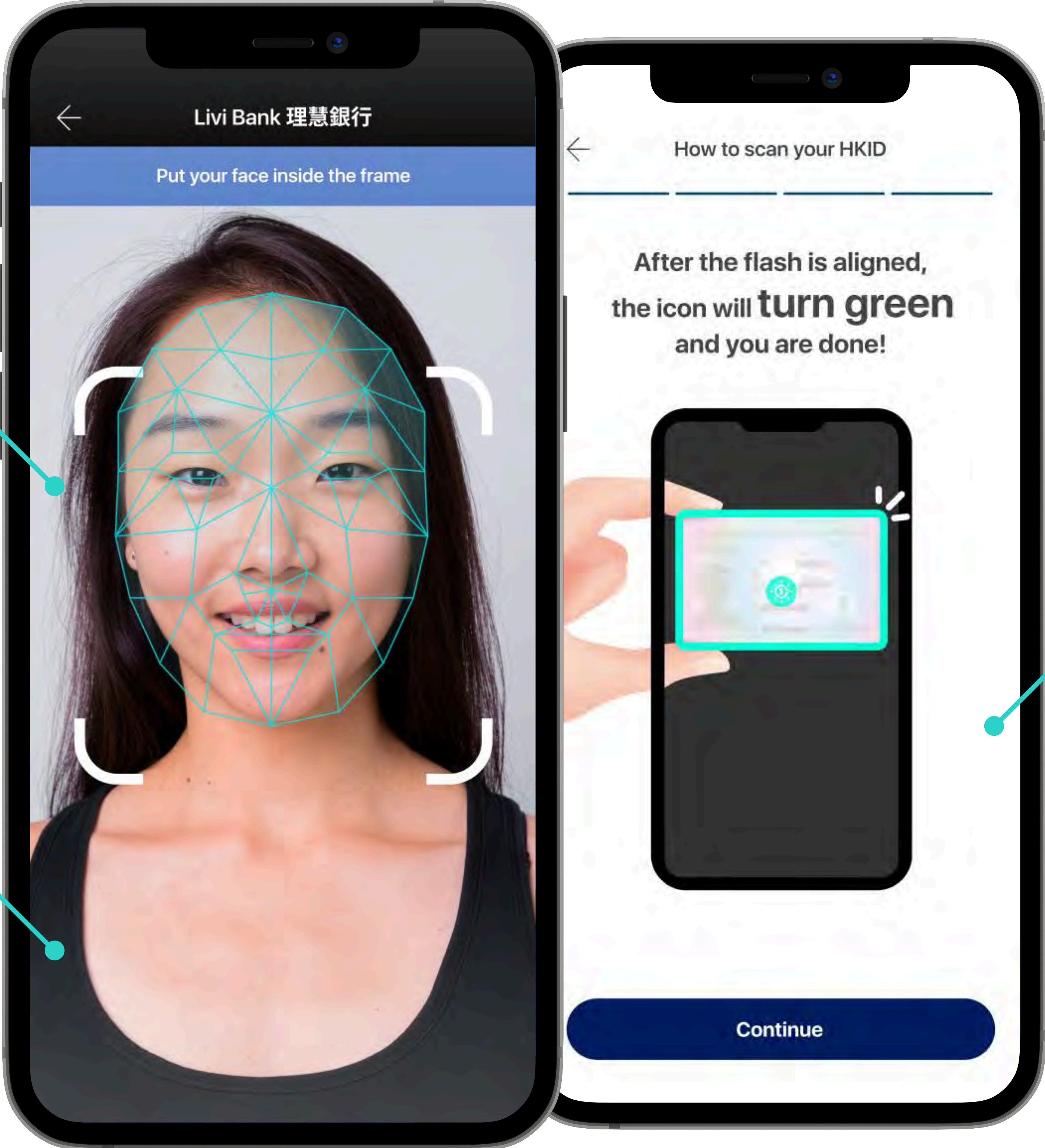
New use cases enabled via GenAI Sandbox

01

Anti DeepFake

03

Distribution Detection



02

Differential Detection

Contact our team to learn more

Mark Mo

mark.wc.mo@livibank.com

(852) 3893 3023

(852) 6767 6185