Beacon

FTDH AND FRAUD OPERATIONS FOR BANKS

Every fraud case, handled with evidence

Beacon is a case-driven fraud operations desk for digital banks. It brings fraud cases, FTDH handling, restoration and reporting together, with AI that drafts cited reports for people to approve.

CASE HANDLING
FTDH

APPROVAL
4-eyes

IDENTIFIER ENCRYPTION
AES-256

ON-PREM OR CLOUD
AI

Evidence-led cases
Fraud Desk and FTDH



Controlled review
Four-eyes approval

Protect sensitive identifiers
Masking, audited reveal and restoration

Fraud Desk
One workspace for case handling.

FTDH
Manage disputed transfers end to end.

Restoration
Track restoration to completion.

OPERATIONAL CONTEXT

A clearer way to work

Beacon is a case-driven fraud operations desk for digital banks. It brings fraud cases, FTDH handling, restoration and reporting together, with AI that drafts cited reports for people to approve.

01

Too many portals

Analysts move between systems for one case.

02

Regulatory clocks

Dispute and reporting timelines are tight.

03

Manual reports

Case reports take time to write and check.

THE CHANGE IN DAILY OPERATIONS

Before	With Beacon
— Portal hopping	✓ One fraud desk
— Manual evidence capture	✓ Agent evidence gathering
— Hand-written reports	✓ Cited AI drafts
— Clear-text identifiers	✓ Encrypted, masked data
— Spreadsheet tracking	✓ Tracked case clocks

AN OPERATIONAL SCENARIO

Keep fraud case handling accountable

A bank analyst needs to gather evidence, handle disputed funds and track restoration while protecting sensitive customer identifiers.

One
Case desk

Cited
AI report drafts

4-eyes
Control

Audited
Every reveal

CAPABILITIES 1

The capabilities that do the work

Explore the core functions of Beacon and the operational tasks they support.

01

Fraud Desk

One workspace for case handling.

02

FTDH

Manage disputed transfers end to end.

03

Restoration

Track restoration to completion.

04

Reporting

Case, customer reply and regulatory drafts.

05

Automation

Software agents gather evidence from bank portals.

06

Policy control

Versioned policies and configuration.

DESIGNED AROUND THE USERS

Fraud teams A single case desk.

Risk Controlled policies.

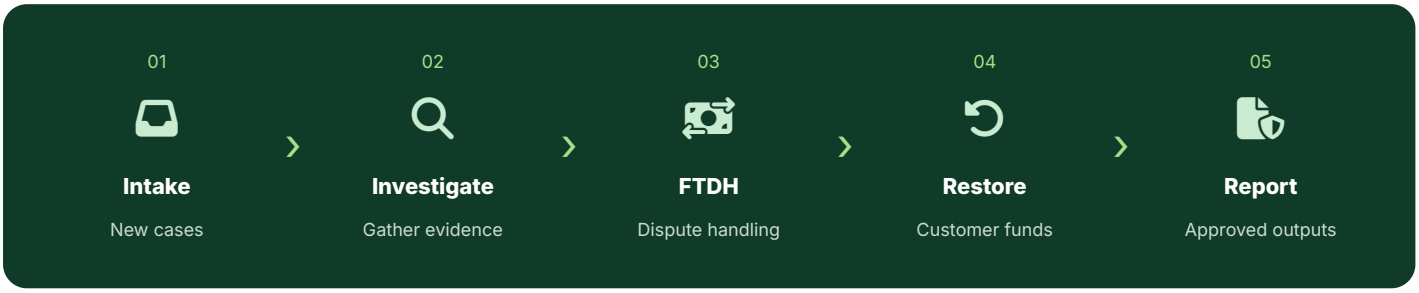
Compliance Audit-ready records.

Digital banks On-prem deployment.

WORKFLOW

From the first step to the outcome

A connected sequence makes the handoffs and responsibilities easier to follow.



01 Open
A case enters the Fraud Desk.

02 Gather
Agents collect evidence from connected systems.

03 Decide
Analysts review the evidence under policy.

04 Approve
Four-eyes approval protects sensitive actions.

05 Report
AI drafts cited reports for human sign-off.

A PRACTICAL WALKTHROUGH

Keep fraud case handling accountable

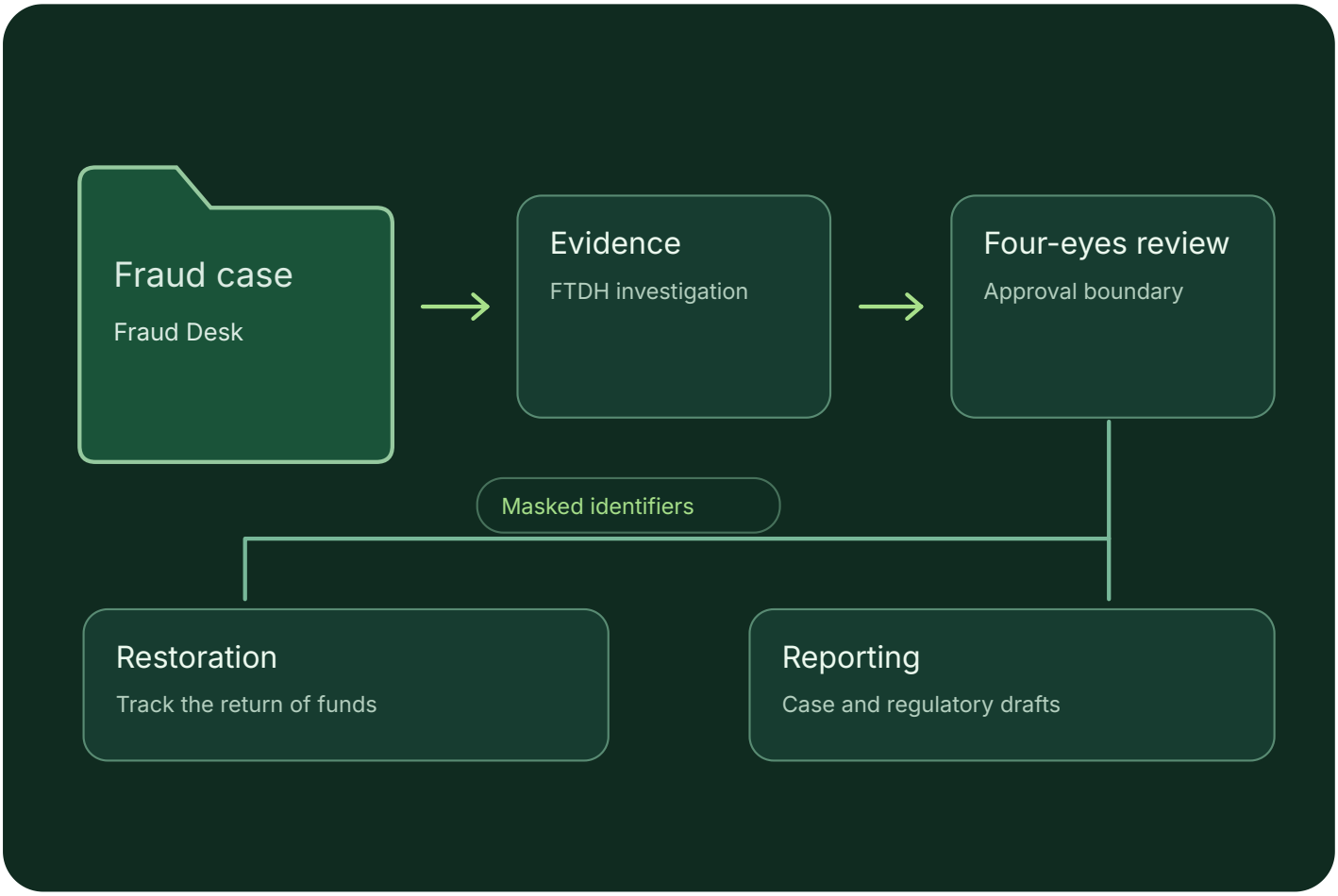
A bank analyst needs to gather evidence, handle disputed funds and track restoration while protecting sensitive customer identifiers.

Follow a case through the Fraud Desk, review masked identifiers and audited reveal, then inspect the four-eyes approval boundary before reporting.

ARCHITECTURE & HANDOFFS

An evidence-led case lifecycle

Fraud handling, disputed transfers and restoration stay connected to a case, with controlled access to customer identifiers.



Conceptual product flow · Beacon

01

Gather the case evidence in the Fraud Desk.

02

Keep identifiers masked and audit their reveal.

03

Apply four-eyes approval and track reporting and restoration.

DISCUSS YOUR ENVIRONMENT

Confirm the source systems, responsibilities and integration boundaries during the walkthrough. The diagram explains the product concept; the deployment scope is agreed for your environment.

TECHNOLOGY 1

Understand the connected pieces

Formats, protocols and tools in the product scope, with plain-language explanations for technical and business readers.

Fraud Desk

The workspace where analysts handle fraud cases.

FTDH

Handling of disputed funds transfers between banks.

Restoration

Tracking the return of funds to affected customers.

Reporting

Case, customer and regulatory report drafting.

Automation

Software agents that carry out repeat evidence gathering.

Masking

Hides sensitive identifiers unless a user has reason to see them.

PDF reports

Finished reports produced as PDF documents.

Bank integrations

Connections to ticketing, core banking and related systems, set up per bank.

THE BEACON OPERATING FLOW



INTEGRATION PLANNING

Agree the source systems, supported versions, data ownership and access requirements during discovery. Validate the relevant interfaces against your environment before production rollout.

ASSURANCE & NEXT STEPS

Prepare for a successful rollout

Match the product scope to your people, systems and operating requirements.

PRODUCT ASSURANCE

- **AES-256 encrypted identifiers**
- **Masked data, audited reveal**
- **Four-eyes approval**
- **On-prem on bank servers**

PLAN THE ENGAGEMENT

01

Discover

Review your current process, source systems, users and constraints. Identify the operational problem the first phase should solve.

02

Demonstrate

Follow a case through the Fraud Desk, review masked identifiers and audited reveal, then inspect the four-eyes approval boundary before reporting.

03

Validate

Agree the applicable product scope, access controls, integration checks and acceptance criteria. Confirm deployment and support responsibilities.

04

Handover

Plan user guidance, operational ownership and support contacts. Confirm the reporting cadence and review process for the agreed scope.

START A CONVERSATION

Explore Beacon with our team.

Bring your operational scenario. We will walk through the relevant workflow and discuss a suitable scope.

info@excelerongroup.com

www.excelerongroup.com · Lahore, Pakistan