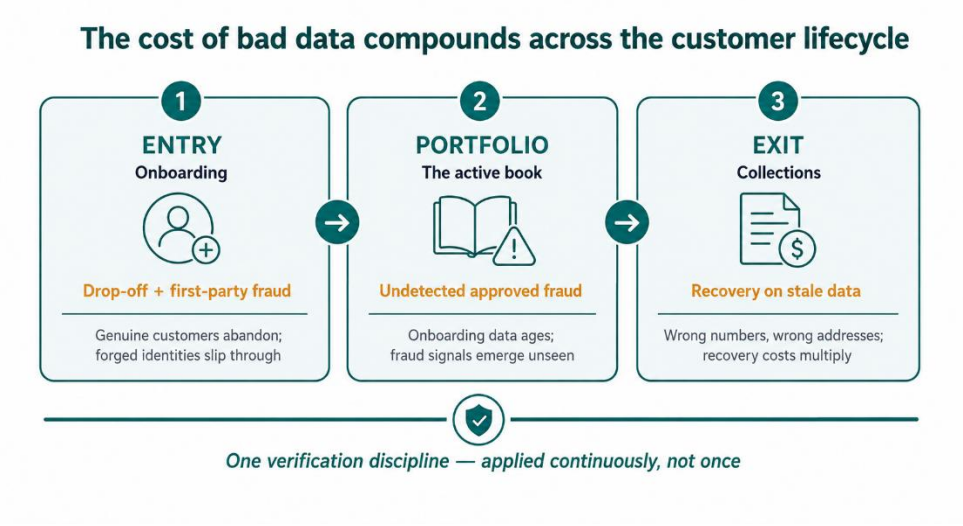
KYCKART®

INDUSTRY WHITE PAPER

# Verification That Doesn't Expire

## Why one-time KYC is quietly costing Indian BFSI at the front door, inside the book, and at the exit




*A study of the verification gap across the customer lifecycle in Indian banking, lending, and insurance.*

**July 2026**

## Purpose & goal of this paper

This paper exists to reframe how Indian BFSI leaders think about verification. The industry treats KYC as a one-time gate at onboarding; this paper makes the case that verification is a **lifecycle discipline**. The identity, contact, and financial data captured at the front door decays continuously, and that decay quietly costs the business at three stages - onboarding (drop-off and first-party fraud), the active portfolio (undetected approved fraud), and collections (recovery on stale data). Using independent market and regulatory data, the paper quantifies that cost and establishes the problem as both real and urgent.

Its goal is to move the reader from seeing three separate problems - solved by three separate tools - to seeing one problem, data that expires, solved by one continuous verification layer. In doing so it aims to:

- **Build credibility** by leading with third-party evidence rather than product claims, so a business leader trusts the argument on its merits.
- **Create urgency** around the economic and regulatory exposure of the status quo - fraud losses, lost conversion, failed recovery, and DPDP/RBI compliance.
- **Open a conversation** by converting interest into a low-friction next step - a verification gap assessment - rather than a hard sell.

In short, it educates the market on the lifecycle-verification thesis, positions KYCKART as the category authority for it, and grounds the next discussion in the reader's own exposure.

### Intended audience

This paper is written for **business leaders in Indian BFSI** who carry the commercial consequences of the verification gap - chief executives, business and lending heads, and risk, fraud, and collections leaders across banks, NBFCs, fintechs, and insurers. It assumes a strategic rather than technical reader: the argument is built on economics, exposure, and regulation rather than integration detail. Heads of technology, product, and compliance will also find it a useful framing for aligning verification strategy across the customer lifecycle.

# Contents

## Executive summary

India is digitising financial services faster than any market on earth. Fintech lenders now originate close to nine in ten personal loans under ₹1 lakh; the digital lending platform market is compounding at more than 30% a year; and the country's real-time payments rail clears upwards of 18 billion transactions every month. Growth on this scale is the headline story of Indian BFSI - and it is genuine.

But the same velocity that wins customers has industrialised the risk that travels with them. Reported bank-fraud value surged **194% to ₹36,014 crore in FY25**. India lost an estimated **US$2.5 billion to digital payment fraud** in a single year. Stress in the microfinance book climbed to **15.3% by March 2025** from 5.9% a year earlier. These are not isolated numbers from unrelated corners of the industry. They share a single, rarely-named root cause.

| +194% | $2.5bn | 15.3% |
|---|---|---|
| Bank fraud value, FY25 | Digital fraud loss, one year | NBFC-MFI stress, Mar 2025 |

That root cause is structural: **the industry treats verification as a one-time event at onboarding.** The identity, contact, address, and financial data captured at the front door is assumed to remain true for the life of the relationship. It does not. It begins to decay the moment it is captured - and the cost of that decay surfaces at three distinct stages of the customer lifecycle:

- **At the front door,** where slow or manual verification drives genuine customers to abandon, and forged or borrowed identities pass visual inspection.
- **Inside the portfolio,** where fraud that cleared onboarding sits undetected and grows more expensive to unwind with every month.
- **At the exit,** where collections teams chase delinquent borrowers using contact data that aged out long before the account turned.

This paper makes the case that verification must be reframed - from a one-time gate into a **lifecycle discipline.** It quantifies the cost of the present model at each of the three stages using independent market and regulatory data, and sets out what a continuous, source-authenticated verification posture would change. It is written for business leaders who carry the P&L consequences of these gaps, not only the teams who operate the checks.

*A worked example of what this is worth in practice, modelled on a single large bank's personal-loan book, appears in Appendix B: The Value of Verifying Continuously.*

# 1. The paradox: record growth, record leakage

Indian BFSI is living a paradox. By almost every growth measure, it is thriving. The digital lending platform market is projected to grow from roughly **US$487 million in 2024 to US$2.45 billion by 2030 - a 31.5% compound annual growth rate.** Fintech personal-loan volumes rose to 6.4 million accounts worth ₹97,381 crore in the first half of FY26, up from ₹78,084 crore a year earlier. The country's digital payments rail crossed 18,000 crore transactions in FY25.

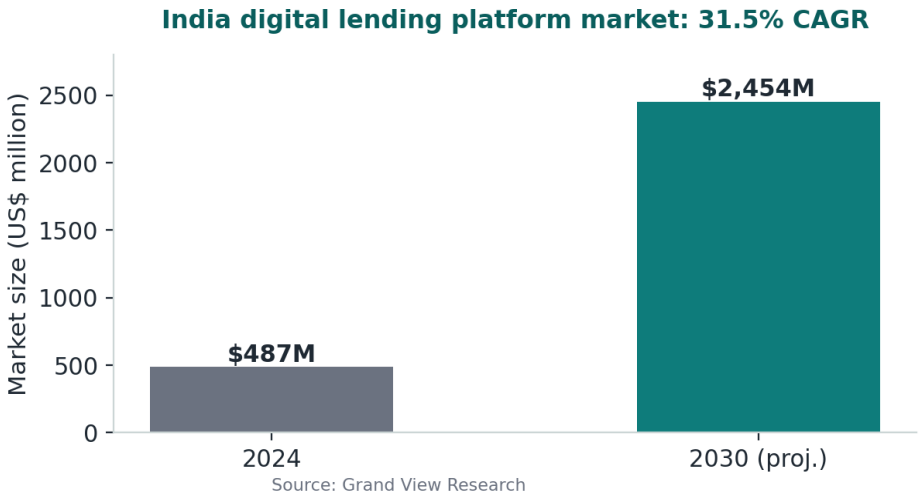



*Figure 1. India's digital lending market is set to grow more than fivefold by 2030.*

And yet the leakage is growing faster than the book. The Reserve Bank of India's FY25 Annual Report put total reported fraud value at **₹36,014 crore - a 194% jump** from ₹12,230 crore the year before, with frauds tied to loan advances alone surging to ₹33,148 crore. Separately, digital payment fraud losses have risen roughly 41-fold over five years to nearly ₹23,000 crore.

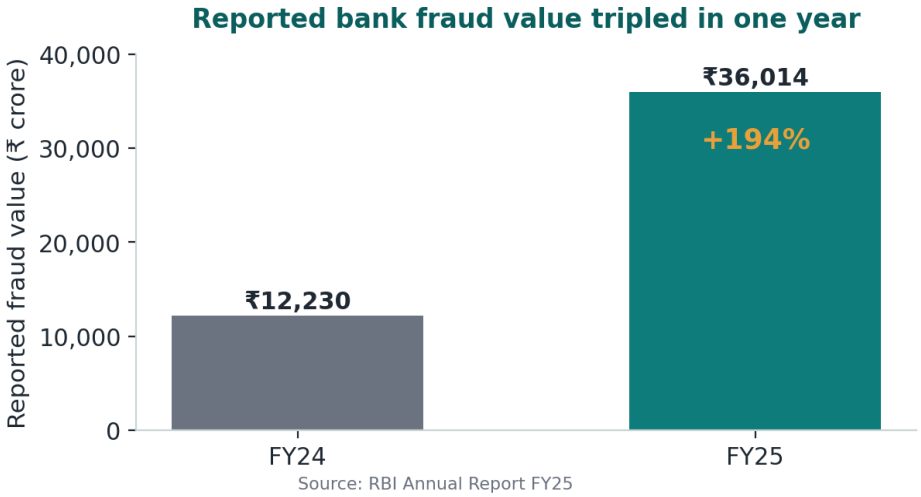



*Figure 2. Reported bank-fraud value nearly tripled year-on-year, even as case volumes fell.*

It would be comforting to read growth and leakage as two separate stories - one a triumph, the other a cost of doing business. They are not separate. They are the same story. Scale has outrun the

verification model beneath it. Each new million accounts opened on a one-time check is another million data points that begin decaying on day one, and another million places where fraud can enter undetected or recovery can later fail.

> **The growth and the losses are not two stories. They are the same story: scale has outrun the verification model underneath it.**

## 2. The root cause: data that dies the moment you capture it

Most BFSI verification architecture rests on a single assumption - that verifying a customer thoroughly once, at onboarding, provides lasting cover. That assumption fails in three structural ways.

1. **It treats a moving target as static.** A borrower's mobile number, address, employer, and financial relationships change continuously. Onboarding data is a photograph of a moment that has already passed; the gap between that photograph and reality widens every month.
2. **It optimises for the wrong failure.** A one-time gate is tuned to reject obvious fraud at entry. It has nothing to say about fraud that passed the gate - which the RBI data shows is exactly where the largest losses concentrate, in advances rather than at the point of sale.
3. **It offers nothing at the exit.** When an account turns delinquent twelve or eighteen months later, the onboarding file is the only intelligence the recovery team holds - and by then a significant share of it is wrong.

The cost of bad data, in other words, is not paid once. It **compounds across the lifecycle.** The chart below illustrates the dynamic that quietly drives losses in a digital book: as the accuracy of onboarding-era data falls, the proportion of the portfolio entering delinquency rises. The two curves move in opposite directions - and the widening gap between them is unmanaged risk.

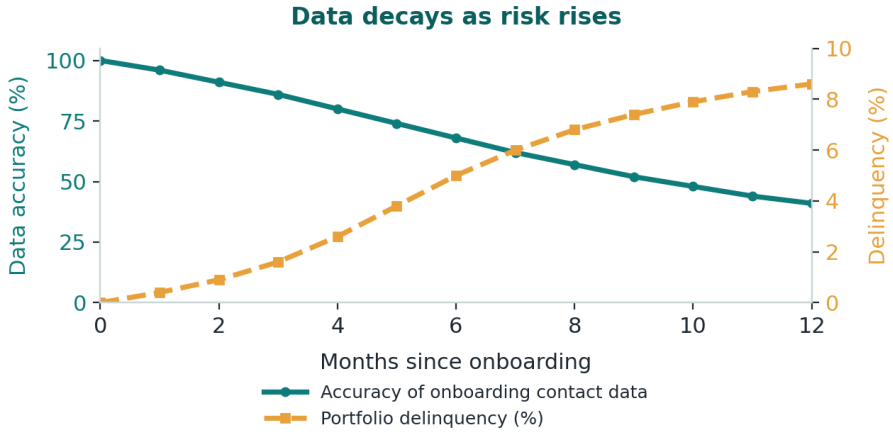



*Figure 3. As onboarding data loses accuracy, the share of the book in distress climbs. The gap is unmanaged risk.*

The remainder of this paper follows that cost through its three stages - the front door, the portfolio, and the exit - and quantifies what the present model leaves on the table at each.

# 3. Stage one – the front door

## The cost of friction and first-party fraud

Onboarding is where two costs collide. The first is **drop-off.** Industry research consistently finds abandonment of 40–60% on manual or poorly designed digital KYC flows, with roughly 70% of users abandoning a verification journey that runs longer than three minutes. Every one of those is a genuine, already-acquired customer - fully marketed to, fully intent-qualified - lost at the final step. For a business leader, that is acquisition spend converted directly into nothing.

The second cost is **fraud at entry.** Sophisticated applicants now present authentic-looking forged documents, borrowed identities, and fabricated financial histories that pass visual inspection. The RBI's FY25 data is blunt about where this lands: advance-related fraud reached ₹33,148 crore. The most expensive fraud is not the attack that was blocked - it is the application that was approved. Once credit is extended, insurance is bound, or an account is opened, the loss is already on the books, and recovery costs multiples of what a real-time check would have cost.

> **The costliest fraud is not the fraud you stopped. It is the fraud you approved.**

These two costs are usually traded off against each other. Tighten verification and you stop more fraud but lose more genuine customers to friction; loosen it and you convert better but admit more fraud. Most institutions manage this as a dial, accepting a worse outcome on one axis to protect the other.

The trade-off only collapses when verification becomes **fast enough to be invisible and accurate enough to be trusted** - when a check returns in well under a second, drawn from an authoritative source rather than a manual review queue. At that point friction and fraud stop being opposed: the genuine customer never feels the check, and the fraudulent applicant cannot satisfy it. That design point - synchronous, source-authenticated verification at the moment of application - is the standard the front door now demands.

# 4. Stage two – inside the book

## The fraud you have already approved

The dangerous assumption at the portfolio stage is that onboarding fraud and portfolio fraud are different problems requiring different tools. They are not. They are the same identities, surfacing later. An account that cleared onboarding can develop fraud signals over time - contact details go dark, declared addresses disconnect, financial relationships shift in ways that no longer match the original file. An institution with no ongoing monitoring is, in effect, holding undiscovered losses on its balance sheet and calling them performing assets.

The numbers explain why this stage matters more with every quarter. **Over half of new retail NPAs are now emerging from unsecured loans** - the precise segment in which fintech and digital lenders concentrate. NBFC-MFI portfolio stress reached 15.3% by March 2025, and loans overdue by 31–180 days rose from 2% to 6.2% of the book. Fraud detection that stops at the onboarding timestamp is blind to all of it.

Reframing fraud as a lifecycle problem changes what "detection" means. It is no longer a single decision at entry but a standing capability: periodic re-verification of the active portfolio, cross-referenced against authoritative sources, that surfaces accounts whose underlying details have shifted in ways that indicate elevated risk. This turns fraud control from a gate into an early-warning system - and it produces something the present model rarely can: source-attributed, timestamped, structured evidence, ready to support recovery action, regulatory reporting, and insurance claims.

# 5. Stage three – the exit

## Recovering on data that has already expired

By the time an account is delinquent, the cost of stale data is no longer theoretical - it is the difference between recovering and writing off. Contact details captured at onboarding degrade every month, so collections teams routinely begin a recovery cycle dialling numbers that no longer reach the borrower and dispatching field agents to addresses the borrower has left. The economics are unforgiving.

Post-NPA - once an account crosses 90 days past due - **average recovery in unsecured lending falls below 25%,** and even secured recovery rarely exceeds 50% on a present-value basis once legal costs and timelines are counted. By the time an account reaches SARFAESI or DRT proceedings, the all-in recovery cost - legal fees, field investigation, court expense, and management time - can exceed ₹50,000–1,00,000 per account.

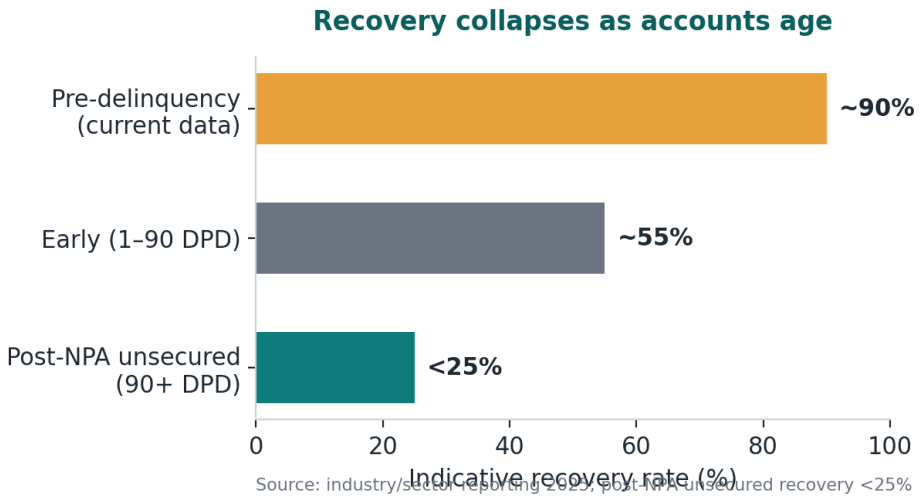



*Figure 4. Every month an account ages on stale data, the recoverable value falls.*

Against that backdrop, every wasted call and every field visit to an outdated address is margin destroyed before a rupee is recovered. The usual answer - manual skip-tracing - is labour-intensive, inconsistent between agents, rarely documented, and impossible to scale to the size of a modern delinquent portfolio.

The lifecycle view points to a different intervention: attack the **input,** not the effort. If the delinquent portfolio is refreshed with current, source-authenticated contact and asset intelligence before the collections cycle begins, every downstream action improves at once - higher right-party contact rates, fewer call attempts per resolved account, and lower cost per recovery, because agents spend their time talking to the right person rather than searching for them. Stale onboarding data becomes a live collections advantage.

> **Collections does not have a productivity problem. It has a data problem wearing a productivity costume.**

## 6. The case for continuous verification

Read together, the three stages tell one story. The front door, the portfolio, and the exit are not three separate risk domains with three separate budgets and three separate vendors. They are three points on a single timeline along which one asset - verified customer data - silently loses its value. The losses look different at each stage (abandoned conversions, approved fraud, failed recovery), but the mechanism is identical: data captured once and never re-verified.

That reframing has a direct operational consequence. The remedy is not more point tools bolted onto each stage. It is a **single verification discipline applied continuously** - the same authoritative sources queried at onboarding, queried again across the live portfolio, and queried once more before recovery. Continuity is the product. The institutions that will pull ahead are those that stop treating verification as a cost incurred once at acquisition and start treating it as infrastructure that runs for the life of the relationship.

Three properties define verification fit for that role:

- **Source-authenticated, not inferred.** Data verified against primary government and regulatory sources - not aggregated data lakes or bureau proxies that themselves age.
- **Real-time, not review-queue.** Results in seconds, so verification can sit inside the customer flow without creating friction or backlog.
- **Multi-source and auditable.** Cross-referenced across independent sources, with every check timestamped and structured into an examination-ready record.

## 7. The compliance dividend

For a business leader, compliance has shifted from a back-office cost to a board-level exposure. The **DPDP Rules 2025, notified in November 2025,** layer a comprehensive data-protection regime on top of existing RBI Master Directions, with most BFSI organisations likely to be classified as Significant Data Fiduciaries and a compliance horizon around May 2027. At the same time, the RBI's KYC Master Direction continues to mandate record retention and source-level diligence.

Continuous, source-authenticated verification is not only operationally superior - it is the posture this regulatory environment now expects. Verification conducted against authorised sources, with a timestamped, audit-ready record for every check, satisfies the examiner and the data-protection regime at the same time. In that light, "compliant by design" is a dividend rather than a constraint: the same discipline that closes the economic gaps also closes the regulatory ones.

## 8. Conclusion

India's BFSI growth story is real, and so is the leakage running alongside it. The leakage has a single root - verification treated as a one-time event in a world where identity, contact, and financial data decay continuously. The losses surface in three places: drop-off and fraud at the front door,

undetected fraud inside the book, and failed recovery at the exit. But they are one problem wearing three costumes, and they yield to one answer: verification that does not expire.

The institutions that internalise this will not buy three more tools. They will adopt a single verification intelligence layer that stays live across the lifecycle - source-authenticated, real-time, multi-source, and audit-ready by design.

**Where KYCKART fits.** KYCKART is built to occupy exactly this position: a unified verification layer for Indian BFSI that authenticates identity, financial credentials, and entity legitimacy in real time against primary government and regulatory sources - at onboarding, across the active portfolio, and ahead of collections. One integration, applied continuously, spanning the same three stages this paper describes.

The first step is not a purchase - it is a diagnosis. We invite BFSI leaders to map their current verification workflow against the three-stage model in this paper and identify where data is decaying unseen. KYCKART's specialists will run that gap assessment with you, and show - stage by stage - where verification that doesn't expire changes the economics.

**Click to book a verification gap assessment**

*For a worked numerical illustration of what this looks like inside a single large-bank personal-loan book, see Appendix B - The Value of Verifying Continuously.*

# Appendix A – Data sources

*All market and regulatory figures cited in this paper are drawn from independent third-party sources, listed below. Figures are FY25 unless otherwise noted.*

| Indicator | Figure | Source |
|---|---|---|
| Bank fraud value, FY25 | ₹36,014 cr (+194%) | RBI Annual Report FY25 |
| Advance-related fraud, FY25 | ₹33,148 cr | RBI Annual Report FY25 |
| Digital payment fraud loss | ~$2.5bn / ~₹23,000 cr (5-yr) | RBI / industry reporting 2025 |
| Digital lending market | $487M (2024) → $2.45B (2030) | Grand View Research |
| Fintech loan volumes, H1 FY26 | 6.4M accounts / ₹97,381 cr | Fintech sector data |
| NBFC-MFI portfolio stress | 15.3% (Mar 2025) vs 5.9% | CRISIL / sector reporting |
| Retail NPAs from unsecured | Over 50% of new retail NPAs | Sector reporting 2025 |
| Post-NPA unsecured recovery | Below 25%; ₹50k–1L per account | Industry / sector reporting |
| KYC onboarding drop-off | 40–60%; ~70% abandon >3 min | UserTesting / industry benchmarks |
| DPDP Rules 2025 | Notified Nov 2025; ~May 2027 horizon | DPDP Rules 2025 / legal advisories |

*Note: a frequently-cited "video-KYC spoofing" figure was found only in vendor commentary and has been deliberately excluded pending independent corroboration.*

## APPENDIX B

# The Value of Verifying Continuously

A continuous-verification business case for a large private bank's personal-loan division

| ₹178 cr | 7.7× | <2 mo |
|---|---|---|
| Annual benefit | Return on investment | Payback period |

*A companion analysis to the KYCKART white paper, "Verification That Doesn't Expire."*

June 2026

> **This is an illustrative, hypothetical model. "Meridian Bank" is fictional; every figure is derived from the stated base assumptions and is intended to demonstrate the economic logic of continuous verification, not to represent any specific institution's results.**

## 1. The scenario

**Meridian Bank** is a hypothetical large private-sector bank in India with a personal-loan (PL) division comparable to the upper tier of the market. Its book and origination engine are sized as follows:

| Parameter | Value |
|---|---|
| Personal-loan book outstanding | ₹40,000 crore |
| Active PL accounts | 25,00,000 (~25 lakh) |
| Average outstanding ticket | ₹1.6 lakh |
| Loan applications received / year | 14,40,000 (1.2 lakh/month) |
| Approval rate | 42% |
| New loans booked / year | 6,04,800 |
| Average disbursal on a new loan | ₹1.8 lakh |
| Annual new disbursal | **₹10,886 crore** |

Today Meridian verifies customers ***once***, at onboarding. After that, the identity, contact, and financial data it captured is assumed to hold for the life of the loan. The sections that follow quantify what that one-time model costs Meridian across three stages of the customer lifecycle - and what a continuous, source-authenticated verification layer recovers.

> **Meridian does not have three problems. It has one problem - data that expires - surfacing at three points on the loan lifecycle.**

## 2. Where one-time verification leaks money

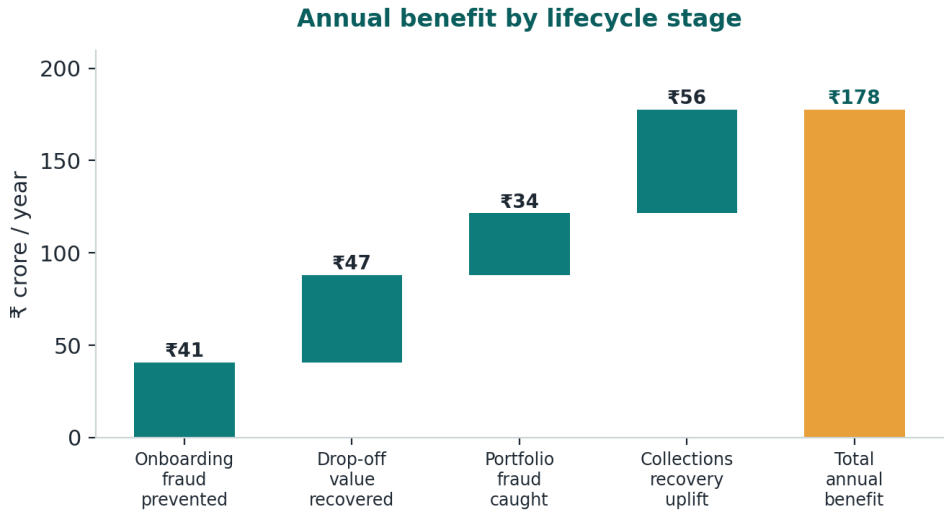



*Figure 1. Annual benefit of continuous verification at Meridian Bank, by lifecycle stage (₹ crore).*

### *Stage 1a – Onboarding: fraud stopped at the gate*

First-party and identity fraud runs at an estimated **1.1% of approved loans** - roughly **6,653 fraudulent loans a year**. At an average disbursal of ₹1.8 lakh and 85% loss-given-fraud, that is ₹102 crore of annual fraud loss reaching the books. Continuous, multi-source verification at application is modelled to catch 40% of it before disbursal:

| Onboarding fraud | Amount |
|---|---|
| Fraudulent loans / year | 6,653 |
| Fraud exposure (disbursed) | ₹120 cr |
| Loss reaching the book (today) | ₹102 cr |
| Catch rate at gate | 40% |
| Annual fraud prevented | **₹41 cr** |

### *Stage 1b – Onboarding: genuine customers retained*

Around 30% of approvable, genuine applicants abandon onboarding at the KYC step - about 2,59,200 lost customers a year. Faster, silent verification is modelled to recover 15% of them (38,880 customers), worth ₹700 crore of incremental disbursal. Valued conservatively at 4.5% net interest margin over 1.5 years, that is:

| Drop-off recovered | Amount |
|---|---|
| Genuine applicants lost today / year | 2,59,200 |
| Customers recovered (15% of drop-off) | 38,880 |
| Incremental disbursal | ₹700 cr |
| Margin value (NIM × tenor) | **₹47 cr** |

### *Stage 2 – Portfolio: emerging fraud caught early*

An estimated 0.4% of the book per year - ₹160 crore - develops fraud signals after onboarding (contact details go dark, addresses disconnect). Left unmonitored, 70% of that exposure is lost. Quarterly portfolio scrubs catch 30% of it early:

| Portfolio fraud | Amount |
|---|---|
| Emergent fraud exposure / year | ₹160 cr |
| Loss if missed (70% severity) | ₹112 cr |
| Caught early (30%) | **₹34 cr** |

### *Stage 3 – Collections: recovering more on fresh data*

Meridian slips ₹1,400 crore to NPA a year (3.5% of the book). On stale onboarding contact data, post-NPA recovery sits at 22%. Refreshing contact and asset data before each collections cycle lifts recovery by 4.0 percentage points:

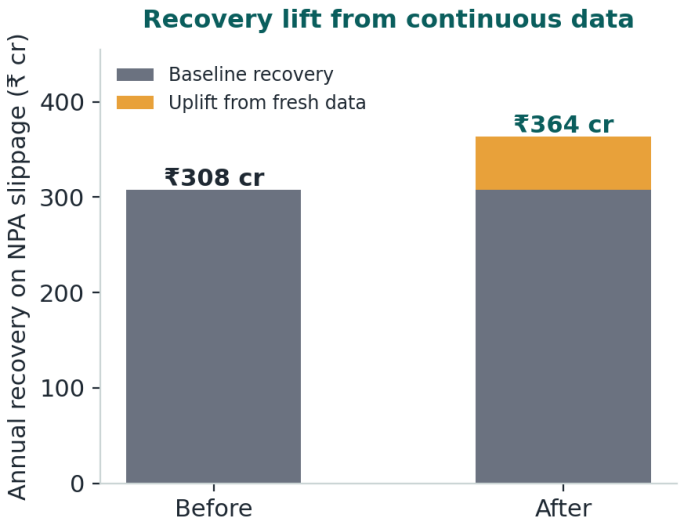
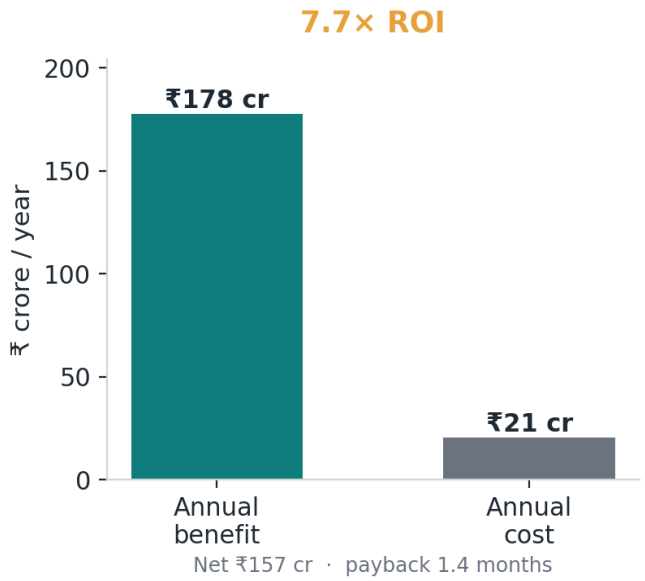



*Figure 2. Collections recovery on NPA slippage, before and after continuous data refresh.*

| Collections recovery | Amount |
|---|---|
| NPA slippage / year | ₹1,400 cr |
| Recovery today (22%) | ₹308 cr |
| Recovery with fresh data (26.5%) | ₹364 cr |
| Incremental recovery | **₹56 cr** |

## 3. The economics

Stacking the four effects gives the total annual benefit. Against it sits the all-in cost of running continuous verification - onboarding checks on every application, quarterly portfolio scrubs across all 25,00,000 accounts, contact enrichment on the delinquent and pre-delinquent pool, and the platform fee.



| Annual benefit | ₹ crore |
|---|---|
| Stage 1a - onboarding fraud prevented | ₹41 |
| Stage 1b - drop-off value recovered | ₹47 |
| Stage 2 - portfolio fraud caught early | ₹34 |
| Stage 3 - collections recovery uplift | ₹56 |
| Total annual benefit | **₹178** |

| Annual cost | ₹ crore |
|---|---|
| Onboarding verification (14,40,000 apps screened) | ₹5.0 |
| Portfolio scrubs (quarterly, full book) | ₹4.0 |
| Collections enrichment (2,18,750 accounts) | ₹0.5 |
| Platform, integration & support | ₹11.0 |
| Total annual cost | **₹20.5** |

| ₹157 cr | 7.7× | 1.4 mo |
|---|---|---|
| Net annual benefit | ROI | Payback |

In this model, continuous verification returns **₹7.7 for every ₹1 spent**, pays for itself in under two months, and adds ₹157 crore to the division's bottom line each year - the great majority of it from fraud genuinely prevented and losses genuinely recovered, not from soft or speculative effects.

## 4. Why the case holds up

The model is deliberately conservative at every lever where optimism would inflate the result:

- **Single-digit catch and uplift rates.** Onboarding fraud catch is set at 40%, portfolio catch at 30%, drop-off recovery at 15%, and the recovery uplift at just 4.5 percentage points - all below what vendors typically claim.
- **Real per-check pricing.** Costs reflect blended market rates for identity, financial, and contact verification at scale, plus a standalone platform fee - not a token line item.
- **Hard-loss weighting.** Over 80% of the benefit comes from fraud prevented and recovery improved - measurable cash effects - rather than from the softer drop-off margin.
- **Every figure traces to an assumption.** No number in this document is free-standing; each derives arithmetically from the base assumptions in Section 1 and the appendix.

> **Halve every benefit assumption and the case still clears 3× ROI. The economics are not sensitive to optimism.**

## 5. What this means beyond Meridian

Meridian is hypothetical, but the structure is general. Any lender running a large unsecured book on one-time verification is carrying the same three leaks - approved fraud, lost genuine customers, and recovery foregone on stale data. The size of the prize scales with book and origination volume, but the ROI ratio is largely scale-independent, because both benefit and cost grow with the same drivers.

The next step is to run this model on real divisional numbers. KYCKART's specialists will populate the same framework with a bank's actual book size, fraud rate, drop-off, and recovery performance - and return a tailored, defensible business case.

**Connect with us to model your own division**

## Base assumptions

*All results in this document are computed from the assumptions below. Figures are annual unless noted.*

| Assumption | Value |
|---|---|
| Book outstanding | ₹40,000 cr |
| Active accounts | 25,00,000 |
| Applications / year | 14,40,000 |
| Approval rate | 42% |
| Avg new disbursal | ₹1.8 lakh |
| First-party fraud rate (of approvals) | 1.1% |
| Loss given fraud | 85% |
| Onboarding fraud catch uplift | 40% |
| Genuine drop-off rate | 30% |
| Drop-off reduction | 15% |
| Net interest margin / tenor | 4.5% × 1.5 yr |
| Emergent portfolio fraud rate | 0.4% |
| Portfolio loss severity / catch | 70% / 30% |
| NPA slippage rate | 3.5% |
| Baseline recovery / uplift | 22% / +4.0pp |
| Verification cost / app / approval | ₹12 / ₹55 |
| Scrub: frequency / cost | 4×/yr / ₹4 per acct |
| Collections enrichment cost | ₹22 per acct |
| Platform fee | **₹11 cr/yr** |

KYCKART

*Verification that doesn't expire.*

## Let's talk.

If the verification gap described in this paper sounds like your institution's, the next step is a conversation, not a purchase. KYCKART's specialists will map your current workflow against the three-stage model in this paper and show you, stage by stage, where continuous verification changes the economics.

**kyckart.com/contact**



KYCKART®