

BANKING · RETAIL, BUSINESS & INSTITUTIONAL

A bank runs on documents it **cannot verify.**

Cheque images, invoices, payslips, dispute evidence, collateral photos, onboarding selfies - a bank accepts more customer-supplied evidence than any other institution, across more channels, and generative AI now fabricates all of it in minutes. This brief maps six places document fraud enters a bank, and shows the dollar impact of sealing evidence at submission. Every figure is drawn from published industry research, cited at the end.

WHAT CAPSEAL IS

Trust for evidence, decided at the moment of capture.

Generative AI has made it trivial to fake the photos and documents that decisions rely on - a payslip, a bank statement or a damage photo can be fabricated in minutes, with no skill, and it passes inspection. Detecting the fake after the fact is a losing arms race.

CapSeal seals evidence on the device, the instant it is captured - cryptographically binding each photo or document to a real device, time and place, and proving it has not been altered since.

Genuine evidence flows straight through to fast decisions; fabricated evidence cannot produce a valid seal, so it is stopped before any money moves. Each decision carries a proof that can be independently verified. CapSeal integrates into the app and workflow already in use - it is not a rip-and-replace.

THE PROBLEM, IN THE INDUSTRY'S NUMBERS

Every channel that accepts a document is an attack surface

The pattern is identical across products: the bank's systems extract the numbers cleanly, the checks pass, and the fraud surfaces months later - as a credit loss, a covered cheque, or an unrecoverable advance.



The high end of the risk is now criminal-indictment scale: in early 2026, US prosecutors alleged one corporate group secured billions in bank financing on falsified financial statements and inflated receivables. At the retail end, remote-deposit-capture fraud - the same cheque presented twice, or an altered image deposited from a phone - accounted for an estimated \$400 million in a single year. And at onboarding, deepfake and injected-camera attacks now defeat the liveness checks KYC was built on. Different products, one root cause: the evidence cannot prove where it came from.

SIX USE CASES, ONE MECHANISM

Where document fraud enters a bank



THE SHIFT

From inspecting evidence to proving its origin

TODAY

- ✗ Fabricated documents clear OCR, serviceability and payment checks
- ✗ Synthetic files are generated, not edited - forensics find nothing
- ✗ Fraud surfaces as credit losses and covered cheques, months later
- ✗ Manual verification slows every genuine customer and advance
- ✗ Whole products avoided because the documents cannot be trusted

WITH CAPSEAL

- ✓ Fabricated evidence caught at submission, before money moves
- ✓ Evidence must prove its origin - generated documents cannot
- ✓ Attested files fast-track; losses stopped at the gate
- ✓ Verification effort concentrates on genuinely doubtful files
- ✓ Products like invoice finance become writable at scale

HOW IT WORKS IN A BANK

Four steps, across every channel that accepts evidence

01

Capture

Customer or business submits documents, photos or cheque images through your app or portal, sealed at source.

02

Seal

On-device signing for captured evidence; provenance and template-lineage checks for uploaded files.

03

Verify

Tamper, duplicate and generation-artefact checks run; a proof object attaches to the file.

04

Decide

Attested evidence fast-tracks; unverifiable evidence routes to your existing controls - never auto-declined.

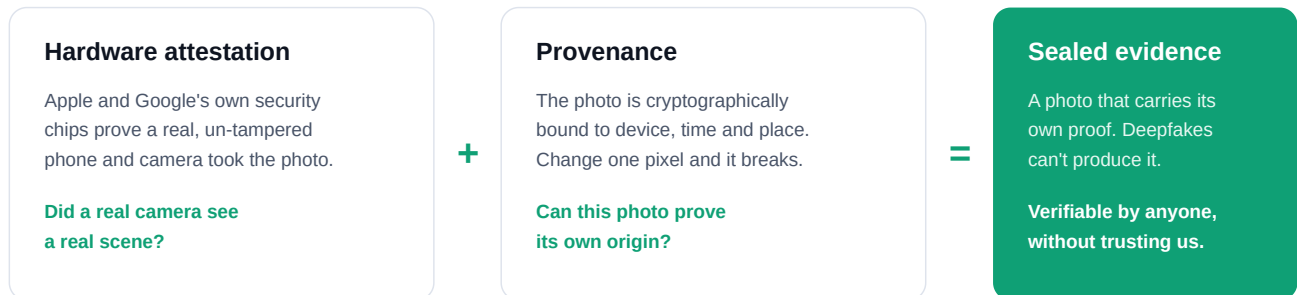
THE MECHANISM, IN ONE PICTURE

How the seal is made - and why it can be trusted

Two things at the moment of capture - **hardware attestation** and a **provenance seal** - make evidence impossible to fabricate after the fact. A generated invoice, an altered cheque image, an injected onboarding selfie: none of them has an origin to prove.



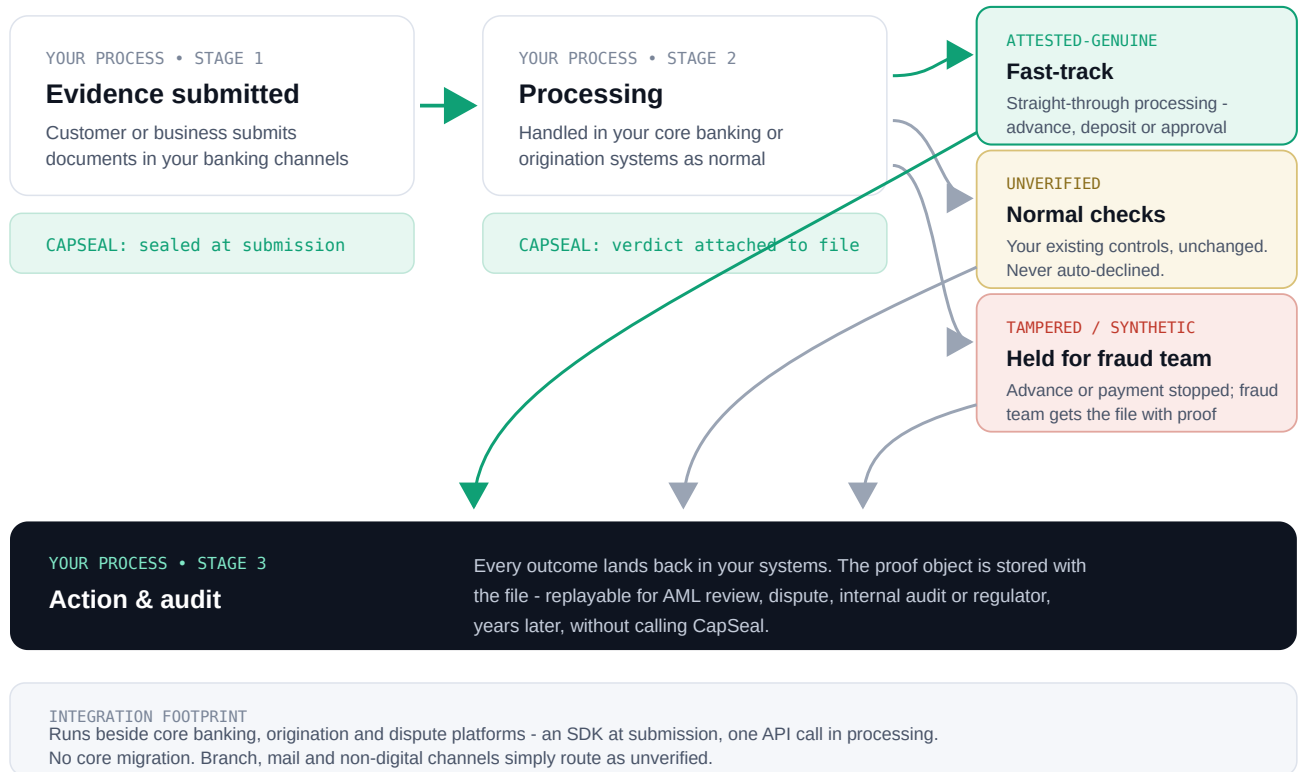
INSIDE THE SEAL



Genuine claims pass and pay instantly. Fabricated evidence never gets a seal.

Where CapSeal sits, whatever the product

The same two touchpoints serve every use case: evidence is sealed at submission, a verdict attaches in processing, and each file routes down one of three paths inside the workflow you already run. No core migration; branch and mail channels simply route as unverified.



THE DOLLAR MODEL

Sizing one use case: invoice & trade finance

A transparent, bottom-up build for a bank financing 60,000 invoices a year at typical 80-90% advance rates - the product where a single fake document converts to a near-total loss, and the one most banks avoid for exactly that reason. Lending origination, deposits and disputes add further impact not counted here.

INVOICES FINANCED / YR	SEALED AT SUBMISSION	FRAUDULENT OR FABRICATED	CAUGHT BEFORE ADVANCE
60,000	75%	1.5%	85%
AVG ADVANCE LOST PER FAKE			
\$36,000			

CALCULATION	STEP	VALUE
Invoices financed per year		60,000
Sealed at submission 60,000 x 75%	x 75%	45,000
Fraudulent or fabricated invoices 45,000 x 1.5% - conservative vs published loss rates	x 1.5%	675
Caught before advance x 85% prevention effectiveness	x 85%	574

Advance losses avoided

574 x \$36,000 avg advance on a fake invoice

\$20.7M / yr

RECOVERABLE ANNUAL IMPACT · INVOICE FINANCE LINE ALONE

\$20.7M

in advance losses avoided per year on one product line - before counting lending origination, deposit fraud, dispute evidence and onboarding. The strategic upside is larger still: a book you can grow because the documents finally prove themselves.

CONSERVATIVE

\$10M

BASE CASE

\$20.7M

AGGRESSIVE

\$32M

Why we lead with dollars, not a ratio: because CapSeal's cost is small next to the losses it prevents, the return multiple is inherently very large. We report the absolute dollar impact instead - a headline ROI of that size invites disbelief more than it earns trust.

HOW IT SCALES

The same model across book sizes

INVOICES FINANCED / YR	SEALED	FAKES STOPPED	LOSSES AVOIDED	CAPSEAL COST	NET IMPACT
60,000 single line	45,000	574	\$20.7M	\$0.13M	\$20.6M
150,000 multi-product	112,500	1,434	\$51.6M	\$0.18M	\$51.4M
400,000 institutional	300,000	3,825	\$137.7M	\$0.33M	\$137.4M

The honest boundary: CapSeal proves a document or image is genuine, current and unaltered - it does not verify that the underlying transaction is sound, and it does not replace credit assessment, AML screening or dispute adjudication. It removes fabricated evidence from every funnel and hands your controls a file they can finally trust. For fraud where the documents are real but the story is not, CapSeal is the intake layer that feeds deeper investigation.

SOURCES

Every input is cited

Nasdaq Global Financial Crime Report (2023) - global cheque fraud losses of \$26.6B, ~80% in the Americas. **American Bankers Association** - cheque fraud up roughly 385% since 2020.

Industry analyses (2023-25) - remote-deposit-capture fraud estimated at \$400M in a single year; cheque fraud accounts for ~20% of all suspicious-activity reports.

Industry survey (2025) - 88% of banks avoid invoice financing due to distrust of document authenticity; the average finance team suffers ~9 successful invoice frauds a year at ~\$133,000 per case (CFO.com); 71% of organisations faced payment fraud, ~45% invoice-related.

US federal indictment (Jan 2026) - corporate group alleged to have secured billions in bank financing on falsified financial statements and inflated receivables.

Reported 2026 - a major Australian bank uncovered over \$1B in suspected loan fraud involving AI-generated documents. AI-generated document fraud grew ~5x in 2025.

Illustrative model built on published industry ranges, not results from a named bank. Where sources give ranges, conservative values are used. Independent analysis by Syptime; not endorsed by the organisations cited. Figures USD.

Size this on your own book

We will model the impact on your portfolio and scope a pilot that runs beside your current process.

Request a pilot pilots@capseal.ai · Contact sales sales@capseal.ai