PT EN

STRATEGIC EBOOK · EXECUTIVE LEVEL

FOR CEOS, CIOS, CROS, CISOS, HEADS OF RISK, HEADS OF AML AND BOARD MEMBERS OF THE LARGEST BRAZILIAN AND GLOBAL BANKS, FINTECHS AND ASSET MANAGERS

# The Account That Stays *Sealed*.

*How Fully Homomorphic Encryption enables banks to perform scoring, AML, fraud detection and M&A — without ever decrypting what belongs to the client. And how to survive the post-quantum transition that has already begun.*

VOLUME I · EDITION 2026 · CONFIDENTIAL

TABLE OF CONTENTS

PT EN

# What you will *read*.

## Appendices

PT EN

# The argument in *one* page.

*If you read only one thing from this eBook, read this.*

The financial industry has been, for five centuries, the industry of trust. More than product, more than technology, more than innovation — banks sell the promise that the client's money is safe, and that information about that money will not fall into the wrong hands. Everything else is operational detail. This promise has survived crises, wars, panics, hyperinflations. It endured because it was — and largely still is — true.

But the technology that sustains this promise is changing rapidly and silently. For two reasons:

1

CRQC

Cryptographically relevant quantum computer estimated for 2029. Breaks ECDSA, RSA, ECDH. All current banking cryptography.

2

HNDL

"Harvest Now, Decrypt Later" — adversaries are storing encrypted data today to decrypt in 2029.

3

COLLABORATIVE AML

Money laundering costs USD 2 trillion/year. Fighting it requires cooperation between banks — today impossible.

4

FAIR SCORING

Credit models under regulatory scrutiny for bias. Audits must inspect the model without exposing the client.

FHE — Fully Homomorphic Encryption — is the central technology to solve the four problems simultaneously. It enables collaborative AML among competing banks. It enables scoring over encrypted

data. It enables M&A due diligence under encryption. And it enables a structured migration to post-quantum cryptography that protects **present and future** data.

PT EN

> *"The next decade of the financial system will be defined by which institutions first learn to collaborate mathematically — and to survive the post-quantum transition without losing data that is encrypted today."*

**THE DECISION**

The question for the board is not "whether" to invest in next-generation cryptographic architecture. It is "how much it costs to wait until you discover that the adversary was already waiting".

CHAPTER I

PT EN

# The *Trust* Industry.

*The modern bank is a data operation disguised as a financial institution. And most of its competitive advantage lives precisely in the data it has the hardest time using.*

In 1990, a bank competed through branches, managers, rates and products. In 2025, it competes through risk models, digital infrastructure, real-time transaction processing capability, AI quality, and — invisible to most — cryptographic capability to protect data and transactions. The old dimensions remain relevant; the new ones have become decisive.

This transition has created a structural contradiction. Banks accumulate client data at unprecedented volume — transactions, behavior, scores, collateral, risk. This data is the central asset for any predictive model, any fraud detection, any scoring, any onboarding of a new client. But it is also the most regulated, most sensitive asset, most contested by regulators and most coveted by adversaries.

# The Invisible Assets of a Bank

PT EN

| ASSET | WHAT IT IS | WHY IT IS UNIQUE |
|---|---|---|
| **Transactional history** | Every client movement over the years | Only actor with complete temporal view |
| **Real credit score** | Observed vs. predicted default | Each bank has its own, nobody shares |
| **AML patterns** | Detected suspicious movements | Visible in isolation; more valuable in consortium |
| **Client knowledge** | KYC, profile, behavior | Replicating is expensive; sharing is taboo |
| **Collateral and guarantees** | Valuation of real estate, vehicles, equipment | Fragmented market, cooperation opportunity |

## The paradox of financial data

Banks hold the most valuable, most sensitive and most regulated data in the economy. And most of the most important business decisions — onboarding, scoring, AML, fraud — require cross-referencing this data in ways that regulation makes difficult and that the competitive culture among banks makes politically impossible.

The result is an industry that knows a great deal about the individual client of each bank and almost nothing about the client of the market as a whole. Each bank knows its own history and looks at the competitor's client through a credit bureau that provides a partial and delayed view.

PT EN

THE SILENT PROBLEM

All current banking cryptography — TLS, AES, ECDSA, RSA — is vulnerable to a quantum computer. CRQC is estimated for 2029. Sophisticated adversaries are collecting banking ciphertext today, waiting to decrypt tomorrow. Every transaction encrypted with classical cryptography generated today is potentially vulnerable retroactively.

CHAPTER II

PT EN

# The Regulatory *Siege*.

*Banks live under more regulation than any other industry. What has changed is that regulation has begun to demand mathematical proof.*

## LGPD, Central Bank of Brazil and the double standard

Brazilian banks live under LGPD (Brazilian data protection law) and the Central Bank of Brazil (financial regulation). The two sometimes demand opposite things: LGPD wants minimization, the Central Bank of Brazil wants traceability. The traditional answer is "robust documentary compliance". The modern answer is "technical architecture that satisfies both" — exactly what FHE enables.

## Basel III, IV and the requirement for auditable models

Basel regulations require risk models to be auditable by the regulator. Traditional auditing requires access to plaintext data. Under FHE, it is possible to audit the model without exposing individual data — preserving data sovereignty and compliance simultaneously.

## FATF and AML

The Financial Action Task Force pushes globally for cooperation between banks in the fight against money laundering. Banks resist because sharing nominally is legally complex. FHE combined with PSI solves this: banks discover common patterns without disclosing their databases.

## CRQC and the post-quantum transition

This is the most underestimated and the most urgent regulatory pressure. In August 2024, NIST standardized the first post-quantum algorithms (ML-KEM, ML-DSA, SLH-DSA). In 2025, cybersecurity

authorities (CISA, NSA, ENISA, BSI) began publishing guidelines that essentially require migration by 2030. **Any bank without a PQC migration plan by 2027 will be the subject of specific**



Here FHE and PQC connect: modern FHE schemes (CKKS, BFV, BGV, TFHE) are all based on RLWE — the same mathematical problem on which ML-KEM and ML-DSA are built. **Adopting FHE is simultaneously adopting the mathematical foundation of the next generation of banking cryptography.** The two investments are one investment.

## The cost of inaction

| RISK | PROBABILITY 5 YEARS | IMPACT |
|---|---|---|
| LGPD fine for secondary use without legal basis | High | USD 50M+ |
| Central Bank of Brazil sanction for poorly documented risk model | Medium | Operational restriction |
| FATF / Financial Intelligence Unit sanction for AML failure | Medium | Reputation + international contracts |
| Retroactive post-CRQC leak | High after 2029 | Catastrophic — all classical cryptography |
| Reputational crisis after scoring breach | Low-medium | Loss of premium portfolio |

CHAPTER III

PT EN

# FHE in Executive *Language*.

*No mathematics. What the board needs to understand.*

A transparent vault. You see that something is inside, you do not see what it is. You manipulate the contents from outside — add, multiply, compare, run entire risk models — without ever opening it. You return it sealed. This is FHE.

## The conceptual leap

All current cryptography protects data in transit (TLS) and at rest (AES). The third state — in use — has always required plaintext. That is the instant in which the scoring engine accesses the history in plaintext. It is where the AML system processes the transaction. **FHE eliminates the third state.**

## FHE and PQC — the same mathematics

Modern FHE schemes are built on the RLWE (Ring Learning With Errors) problem. It is exactly the same problem on which NIST standardized ML-KEM (FIPS 203) and ML-DSA (FIPS 204) — the next generation of post-quantum cryptography. **Adopting FHE is adopting PQC implicitly.** The team that learns FHE learns PQC. The infrastructure that supports FHE supports PQC.

# How it works

PT EN

> **ANALOGY FOR THE BANK**
>
> Client data remains permanently encrypted. The scoring engine runs over ciphertexts. The AML algorithm processes encrypted transactions. Risk analysis computes exposure over ciphertexts. At no point does the central server see individual data in plaintext. The regulator's audit inspects the model, not the data.

## FHE vs alternatives

| TECHNOLOGY | PROMISES | FAILS |
|---|---|---|
| De-identification | "We removed identifiers" | Trivial re-identification |
| TEE (SGX, SEV) | "The chip isolates" | Trusts the manufacturer; documented side-channel attacks |
| Federated Learning | "Data stays at the bank" | Gradients leak individual data |
| Differential Privacy | "We added noise" | Inadequate for individual credit decisions |
| **FHE** | **"Server never sees in plaintext"** | **High computational cost — but decreasing** |

CHAPTER IV

PT EN

# Use Cases by *Line of Business*.

## Collaborative AML between banks

Money laundering costs the global financial system USD 2 trillion/year. The fight is structurally ineffective because it requires cooperation between competing banks. Today impossible.

Under FHE with PSI: banks encrypt lists of tax IDs, IPs and suspicious accounts. They discover **only the intersection** — those who appear in three or more banks with anomalous movement patterns. Without revealing the databases. The Financial Intelligence Unit and FATF are signaling explicit regulatory support for this approach. **It is the largest unexplored collaborative opportunity in the financial sector.**

## Credit scoring under encryption

The credit score is the bank's most valuable and most regulated asset. Regulatory auditing of the model requires access to training data, creating tension between supervision and privacy. Under FHE, it is possible to audit the model (check fairness, bias, accuracy) without the auditor ever seeing individual client data.

## Open Banking under verifiable privacy

Open Banking depends on the client authorizing the sharing of data between institutions. Trust is fragile — clients hesitate, receiving banks distrust. Under FHE, aggregate analyses (consolidation, cash flow analysis, risk scoring) happen over encrypted data. **Open Banking gains a technical trust foundation that it currently lacks.**

## M&A due diligence under encryption

M&A requires one party to show sensitive data to the other before the deal is closed. Leakage or withdrawal of the buyer is a constant risk. Under FHE, the buyer can perform due diligence over encrypted data, validating hypotheses without the counterparty exposing its database. **Reduces the risk of leaking confidential information in deals that do not close.**

## Real-time fraud detection

Fraud models must analyze patterns in real time. Today they require plaintext data in complex pipelines. Under FHE, fraud models can run over encrypted transactions — useful especially to scale fraud detection to partners (payment gateways, marketplaces) without handing over client data.

## Actuarial analysis with clinical data

A bank with an insurance product needs to price risk using clinical data. Under LGPD, health data is a special category. FHE enables actuarial pricing over encrypted clinical data (from insurers or hospitals), preserving the insured person's privacy.

## Structured post-quantum migration

Adopting FHE brings, as a by-product, the technical maturity for PQC migration. The team that learns FHE learns RLWE, lattices, ML-KEM. The infrastructure that runs FHE in production is the infrastructure that must be ready for PQC. **Investing in FHE is investing in surviving CRQC.**

## HNDL — fighting "Harvest Now, Decrypt Later"

Adversaries (nation-states, sophisticated organized crime) are collecting banking ciphertext today to decrypt when the quantum computer is ready. A bank that migrates to PQC **now** also protects data encrypted *retroactively*. A bank that waits until 2029 loses everything encrypted in the last five years.

## Encrypted portfolio analysis

PT EN

Asset managers analyze client portfolios under privacy constraints. Clients want advice without exposing their full wealth. Under FHE, the manager can analyze the encrypted portfolio and return recommendations without ever seeing individual positions.

## Compliance under private audit

Internal and external audits need to examine sensitive data. Under FHE, an auditor can validate regulatory compliance over encrypted data, without needing access to individual data.

CHAPTER V

PT EN

# The Economics of the *Bank That Does Not See*.

## Initial capex

| COMPONENT | INVESTMENT |
|---|---|
| Founding team (crypto + ML + risk + legal + PQC advisor) | USD 6M – 10M / year |
| Licenses and tooling | USD 400k – 1.5M |
| Compute infrastructure + HSMs | USD 3M – 6M |
| Strategic consulting | USD 1.5M – 3M |
| Regulatory study (Central Bank of Brazil, DPA, FATF) | USD 600k – 1.5M |
| Integration with core banking | USD 3M – 8M |
| **Total year 1** | **USD 14M – 30M** |

## Annual opex

PT EN

| ITEM | ESTIMATE |
|---|---|
| Compute | USD 3M – 8M |
| Maintenance team | USD 5M – 9M |
| Audit | USD 800k – 2M |
| **Stabilized annual opex** | **USD 8.8M – 19M** |

For a Brazilian top-10 bank with revenue above USD 30B, this represents **less than 0.1% of revenue**. It is budget rounding.

## The return — seven vectors

### 1. Collaborative AML

Each bank loses annually in Financial Intelligence Unit fines, remediation costs and investigations between USD 30M–150M. Collaborative AML reduces this drastically: **USD 50–200M per year**.

### 2. More accurate scoring

Access to data from other banks via an FHE consortium improves credit models by 5–15%. For a top-10 bank: **USD 100–500M annually in default reduction**.

### 3. Open Banking as an asset

A bank that offers Open Banking with verifiable privacy captures share. **USD 50–200M per year**.

### 4. Real-time fraud detection

Transactional fraud reduced by 20–40%. **USD 30–150M per year**.

## 5. PQC migration without rework

A bank that adopts FHE migrates to PQC almost for free. A bank that does not adopt spend **500M in emergency migration** in 2028–2029.

## 6. Retroactive data protection (HNDL)

Every year of delay in PQC migration is one more year of ciphertext exposed retroactively. Hard to quantify but potentially catastrophic.

## 7. Partnership advantage

Banks with FHE capability become preferred partners for fintechs, asset managers and marketplaces that need private processing.

# Business case

| | |
|---|---|
| ~USD 22M<br>YEAR 1 INVESTMENT | ~USD 14M<br>STABILIZED ANNUAL OPEX |
| USD 1B+<br>VALUE ENABLED IN 5 YEARS | 40×–80×<br>EXPECTED ROI IN 5 YEARS |

PT EN

*“For any top-10 bank, FHE is the digital transformation investment with the highest return asymmetry available in 2026 — combining AML, scoring, PQC migration and retroactive protection.”*

CHAPTER VI

PT EN

# Competitive Advantage and *Positioning*.

The financial industry is dominated by consolidation, scale and infrastructure. The winners are those who operate more cheaply and process more transactions. But a new layer of competition is emerging — and the banks that position themselves first in it capture an advantage that lasts a decade.

## The three positionings

### 1 — The Post-Quantum Bank

Focus on being the first Brazilian bank publicly prepared for CRQC. Explicit positioning as "the bank that protects your money even against threats that have not yet arrived". Works best for premium banks with a corporate portfolio.

### 2 — The Sector AML Orchestrator

Focus on building an FHE consortium to fight AML. Captures the role of sector organizer, gains visibility at the Central Bank of Brazil and Financial Intelligence Unit. Works for top-5 banks.

### 3 — The Sovereignty Bank

Focus on independence from foreign AI vendors. A proprietary model under FHE as a sovereign capability. Works for public or investment banks.

## The cost of not positioning

The scenario to spell out: what happens if none of the large Brazilian banks structurally adopts FHE in the next 36 months? Answer: **they will arrive in 2029 without the technical capability for an**

**orderly PQC migration**. They will pay high multiples in emergency, will lose retroactive data encrypted with classical cryptography, and will fall behind in global collaborative AML initiatives.

CHAPTER VII

PT EN

# The *24-Month* Roadmap.

01

MONTHS 1–6 · LEARN

### Foundation and capability

Hire a founding crypto engineer. Identify three use cases (recommendation: AML, scoring, PQC migration). Align with the Central Bank of Brazil, legal and compliance.

02

MONTHS 7–14 · BUILD

### Internal pilot

Build one end-to-end case. Recommendation: fraud detection under FHE OR auditable scoring.

03

MONTHS 15–20 · FIRST COLLABORATION

### Joint study with another bank or partner

Launch the first use case with PSI or external collaboration. Marketing directed at the Central Bank of Brazil, the Financial Intelligence Unit and Febraban.

04

MONTHS 21–24 · INSTITUTIONAL CAPABILITY

### Adoption as a pillar

Multiple cases on top of the infrastructure. Public announcement of PQC migration. Possibly the first AML consortium between banks.

CHAPTER VIII

PT EN

# Risks, Mitigations and *Pitfalls*.

## 1 · Inability to hire talent

**Mitigation:** acquisition via specialized consulting or a partnership with a university.

## 2 · Cultural resistance

Banks are averse to technical novelty in the core. **Mitigation:** start with an isolated sandbox.

## 3 · The Central Bank of Brazil does not understand or rejects it

**Mitigation:** engage the Central Bank of Brazil early, in advisory mode.

## 4 · Other banks do not join the AML consortium

**Mitigation:** start with smaller banks. The top 5 will follow afterwards.

## 5 · Computational cost at scale

**Mitigation:** hybrid architecture.

## Pitfall 1 · Treating it as an IT project

FHE must report to the CRO or Chief Risk Officer, not the CIO.

## Pitfall 2 · Forgetting PQC migration

FHE and PQC must be treated as the same project.

## Pitfall 3 · Underestimating HNDL

Every year of delay means more ciphertext vulnerable retroactively.

PT EN

# A letter to the next decade of the *financial system*.

The industry you lead was built on an old promise: that the client's money is safe, and that information about that money will not fall into the wrong hands. Everything else is operational detail. This promise has endured five centuries. It endured because it was — and largely still is — true.

But the technology that sustains this promise is changing. The quantum computer, which seemed like fiction five years ago, is today an engineering roadmap. The cryptography that sustains all current banking operations will be obsolete in a few years. The sophisticated adversary already knows this and is collecting ciphertext today to decrypt tomorrow. Anyone who does not migrate now will discover, in 2029, that they protect only the present — not the past, nor the future.

FHE offers a dual answer. It solves the current problem of impossible collaboration between banks on AML, scoring and fraud. And it positions the bank for the post-quantum transition, because the mathematical foundation is the same. **Investing in FHE is investing in surviving CRQC.**

What is at stake is not a technical feature. It is the continuity of the old promise in a fundamentally new technological world.

> *"In three years, some banks will be ready for CRQC. The question is whether yours will be one of them, or whether it will be caught off guard alongside the rest."*

APPENDIX A

PT EN

# Executive *Glossary*.

**FHE**

Computation over encrypted data.

**RLWE**

Ring Learning With Errors — mathematical foundation of modern FHE and NIST PQC.

**CRQC**

Cryptographically Relevant Quantum Computer. Current estimate: 2029.

**HNDL**

Harvest Now, Decrypt Later — adversaries collect ciphertext today to decrypt once they have CRQC.

**ML-KEM, ML-DSA**

Post-quantum algorithms standardized by NIST in 2024 (FIPS 203, 204). Based on RLWE.

**PSI**

Private Set Intersection. Central use case for collaborative AML.

**HSM**

Hardware Security Module — where banking keys live today. FHE adds a logical layer above.

**FATF, FINANCIAL INTELLIGENCE UNIT, CENTRAL BANK OF BRAZIL, DPA**

Converging regulators.

**LATTIGO, OPENFHE, CONCRETE**

FHE libraries.

APPENDIX B

PT EN

# Vendors and *Partners*.

| VENDOR | FOCUS |
|---|---|
| **Inpher** | FHE+MPC, historical focus on finance |
| **Duality** | OpenFHE, focus on finance and analytics |
| **Zama** | Concrete, TFHE, fintech use cases |
| **Tune Insight** | Lattigo |
| **Stickybit** | Brazilian technical boutique in FHE/PQC |

## Relevant initiatives

- **NIST PQC** — post-quantum standardization (FIPS 203/204/205)
- **FATF** — global guidelines on collaborative AML
- **BIS Innovation Hub** — privacy-preserving finance projects

APPENDIX C

PT EN

# 30 Questions for the *CRO/CISO/CIO*.

## Strategy

1. Who understands advanced cryptography and PQC in our company?
2. Do we have a formal PQC migration plan?
3. What is our current exposure to HNDL?
4. Inventory of algorithms vulnerable to CRQC?
5. Open dialogue with the Central Bank of Brazil about PQC?

## Priority use cases

6. How much do we lose each year on AML we cannot fight alone?
7. How much would our scoring improve with data from other banks?
8. How many M&A deals have stalled over privacy issues?
9. Is Open Banking reaching its potential?
10. Would other banks join an AML consortium?

## Technical

11. Which FHE scheme for our first use case?
12. Acceptable latency for core banking?
13. How do we integrate with HSMs and the core?
14. How do we manage keys between the bank and partners?
15. Is threshold cryptography compatible?

## Cost

PT EN

16. FHE cost vs plaintext?
17. Build in-house or via vendor?
18. 24-month capex and opex?
19. C-level sponsor confirmed?

## Regulation

20. Demonstrable compliance with LGPD, Central Bank of Brazil, Basel?
21. How will the Central Bank of Brazil audit a model under FHE?
22. Dialogue with the Financial Intelligence Unit on collaborative AML?

## PQC

23. When do we start the migration to ML-KEM/ML-DSA?
24. What is our exposure if CRQC arrives before 2029?
25. How do we protect ciphertext already generated?
26. How are our partners preparing?

## Commercial

27. How do we price the advantage?
28. Which clients would pay for a mathematical guarantee?
29. What is the brand narrative?
30. Worst-case scenario if a competitor leads PQC first?

PT EN

**The Account That Stays Sealed**

Strategic eBook for senior management at banks, fintechs and asset managers.
Volume I · Edition 2026 · Confidential distribution.

Set in Iowan Old Style and SF Pro.

— end —