LOQR

• LOQR Case Study

Perpetual KYC in Banking: Eliminating Operational Backlogs and Achieving Continuous Compliance

Updating customer information is not only necessary but mandatory. Financial institutions are constantly being subjected to strict regulatory requirements, such as KYC (Know Your Customer) and AML (Anti-Money Laundering) regulations. Therefore, it is crucial that customer databases remain up to date to comply with applicable regulations, avoiding unnecessary fines and increasing efficiency.

With V3 of LOQR’s Platform, financial institutions can benefit from an innovative and fully automated perpetual KYC solution that will transform their customer data update process by simplifying data collection, reducing manual intervention and minimising errors in customer data.

1. The Emerging pKYC Challenge for Banks

Customer due diligence obligations do not end at onboarding. Under European AML regulation and Portuguese legislation - including Lei n.º 83/2017 and Aviso n.º 1/2022 do Banco de Portugal - financial institutions must ensure that customer information remains accurate and up to date throughout the entire business relationship.

This requirement has led regulators and the financial industry to adopt the concept of Perpetual KYC (pKYC).

Instead of relying solely on periodic remediation campaigns, banks are expected to maintain continuous mechanisms for customer data verification.

The challenge is no longer whether banks must perform KYC updates, but how to do so at scale.

Risk-Based Review Cycles

Under the risk-based approach defined by AML regulation**, financial institutions must periodically review and update customer information depending on the** risk profile assigned to each customer**.**

Although the exact review policies may vary between institutions, banks typically apply review cycles similar to the following:

Customer Risk Level	Typical Review Frequency
High Risk	Every 1 year
Medium Risk	Every 3 years
Low Risk	Every 5 years

Structural Volume of pKYC Updates

Example retail bank with 500,000 customers:

Risk Level	Customers	Review Cycle	Annual Reviews
High Risk	5%	1 year	25,000
Medium Risk	25%	3 years	41,667
Low Risk	70%	5 years	70,000

Total ≈ 136,667 pKYC/year.

Even without regulatory remediation programs, risk-based review cycles alone generate more than **130,000 pKYC processes per year** in a mid-sized retail bank.

For institutions with 700,000 to 1 million customers, the annual pKYC workload can easily exceed **200,000 updates per year**, even without remediation campaigns.

These reviews require institutions to verify that customer information remains accurate and up to date, including:

- Identification documents.
- Proof of address.
- Professional and financial information.
- Additional supporting documentation when required.

As a result, banks must process **large volumes of KYC updates every year**.

However, many institutions still rely on:

- Manual document collection.
- Branch-based updates.
- Email-based document submission.
- Operational remediation campaigns.

These approaches create significant operational pressure and compliance risks.

2. Why Many pKYC Programs Struggle

In practice, many banks encounter structural obstacles when implementing pKYC programs.

Lack of Document Standardisation

Customers submit documents in many different formats and from different issuers. Operations teams must manually review each case, increasing processing time and operational costs.

Large Operational Backlogs

The volume of pending KYC updates often exceeds the processing capacity of operations teams.

Typical consequences include:

- Large remediation backlogs.
- Delayed data updates.
- Increased regulatory exposure.
- Operational pressure on compliance and operations teams.

Compliance Gaps in Notification Campaigns

Many institutions attempt to comply with pKYC requirements by sending notifications requesting customers to update their information.

However, in many cases:

- Customers ignore the request.
- The update process is complex.
- The bank does not enforce completion.

As a result, although the institution has requested the update, customer data often remains outdated.

From a regulatory perspective, simply requesting updated information is not sufficient. Financial institutions must ensure that customer information is effectively updated when required under risk-based review obligations.

3. Limitations of Single-Channel pKYC Approaches

Some institutions have implemented simplified pKYC processes relying primarily on Chave Móvel Digital (CMD) authentication.

While CMD is a secure authentication mechanism, relying on it exclusively has limitations.

Adoption Does Not Equal Effective Usage

Although many citizens have activated CMD, effective usage in banking processes is significantly lower.

Banks frequently encounter customers who:

- Have CMD activated but do not remember the PIN.
- Have never used CMD before.
- Are unfamiliar with the authentication flow.

This creates friction and limits completion rates when CMD is the only available option.

Limited Scope of Data Collection

CMD authentication confirms identity but does not allow institutions to collect additional information often required for KYC updates, such as:

- Updated address proof (if different from fiscal address).
- Professional information.
- Income information.
- Additional supporting documents.

Lack of Customer Choice

Restricting customers to a single authentication mechanism often reduces completion rates.

Providing multiple verification options typically leads to higher success rates and better customer experience.

4. The LOQR Digital pKYC Journey

LOQR provides a fully digital pKYC journey built on the same infrastructure used for digital onboarding.

The journey allows banks to request updates to:

- Identity documents.
- Proof of address.
- Additional supporting documentation.

Customers complete the process remotely through a structured digital flow.

Typical process:

1. Bank triggers pKYC journey.
2. Customer receives a secure notification.
3. Customer submits required information.
4. LOQR performs automated validation.
5. Verified data and evidence are delivered to the bank.

Each completed process generates a Finished Lead containing verified data and audit-ready evidence.

The LOQR Platform also integrates Chave Móvel Digital as one of several available verification methods, allowing institutions to combine CMD authentication with other digital verification mechanisms when necessary.

5. Automated Address Proof Verification

The LOQR Platform supports automated validation of digitally issued address proofs from trusted entities.

Examples include documents issued by:

- Telecommunications
- Energy Providers
- Government Sources

Digitally signed documents can be validated automatically, significantly reducing manual review requirements.

6. Operational Model Comparison

Digital pKYC journeys fundamentally change the operational model for customer data updates.

Metric	Manual KYC Update	Digital pKYC (LOQR)
Customer journey	Branch / email / call center	Fully digital
Document submission	Unstructured	Standardised
Document validation	Manual	Automated
Processing time	Days or weeks	Minutes
Operational workload	High	Low
Cost per case	8€ – 12€	~2€ – 3€
Backlog risk	High	Minimal

7. Operational Impact and ROI

Financial institutions often underestimate the operational cost of manual KYC updates.

Industry studies show that banks commonly allocate 10–15% of their workforce to financial crime compliance activities, including KYC operations.

Operational benchmarking across European retail banks indicates that manual KYC update processes typically cost 8€ to 12€ per case, depending on manual intervention.

Digital pKYC journeys significantly reduce these costs by:

- Standardising document submission.
- Automating validation.
- Allowing customers to self-complete the process.

Example Scenario:

A bank performing 150,000 KYC updates per year may experience the following cost structure.

Potential operational **savings can exceed 1M€ per year.**

In addition to cost reduction, digital pKYC programs allow institutions to eliminate operational backlogs and process customer updates at scale.

Model	Annual Cost
Manual process	~1.5M€
Digital pKYC	~300k€ – 450k€

8. Key Success Factors for pKYC Programs

Successful pKYC programs typically rely on four key factors:

Automation
Automation of document validation significantly reduces operational workload.

Multi-Channel Verification
Allowing multiple verification methods increases completion rates.

Standardised Document Collection
Structured digital journeys ensure consistent and processable documentation.

Operational Scalability
A successful pKYC program must be able to process hundreds of thousands of updates per year without creating operational bottlenecks.

Perpetual KYC is becoming a core operational requirement for financial institutions. Banks that rely on manual or branch-based processes will face increasing operational pressure and regulatory scrutiny.

Digital pKYC journeys allow institutions to transform a regulatory obligation into a scalable, efficient and auditable process capable of handling hundreds of thousands of customer updates per year.

The LOQR Platform enables banks to deploy pKYC quickly using existing infrastructure, ensuring continuous compliance with minimal operational overhead. **This capability is available for institutions operating on LOQR Platform Version 3.**

Want to bring LOQR's solution to your business?

Contact us at SALES@LOQR.COM **or**

request a live demo.