1KOSMOS

The hidden profit opportunity

Why digital identity should be a C-suite priority

Improving digital identity processes isn’t seen as a ‘Top 3 Priority’ in a bank’s C-suite, but it should be. According to financial services management consultancy Oliver Wyman, getting it right could boost a bank’s operating profit by up to 35%.

The two most important digital ID processes in a bank are onboarding/account-opening and login authentication — for bank customers as well as bank employees and contractors.

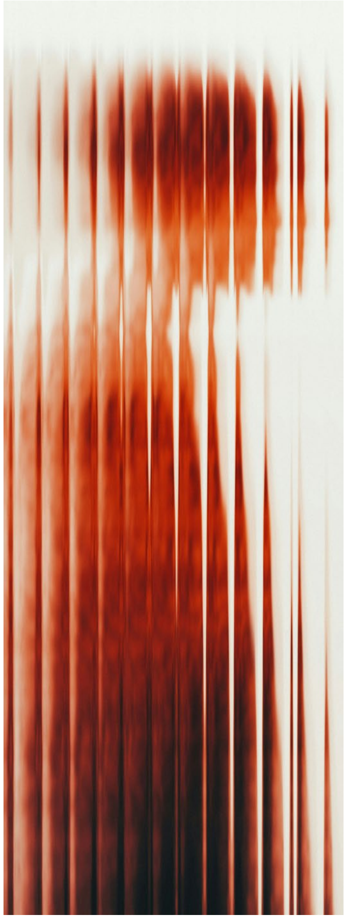
However, weaknesses in onboarding verification and login authentication can bring challenges:

- Synthetic ID fraud
- Account takeover fraud
- Payment scams & fraud
- Data breaches & ransomware
- Frequent, costly password resets
- Multiple vendors, vendor fees

These are all problems that show up in a bank's P&L and otherwise:

- As fraud write-offs
- As legal liability & reimbursements to customers
- As customer anger & reputational damage
- As regulatory fines & remediation costs
- As high call-center OpEx & vendor costs

According to research from Oliver Wyman, the combined annual cost of these problems for US banks is $100-125BN/year.[1] This counts the direct cost of successful fraud attacks plus spending on technology and business processes to keep fraud at current levels. Given the deliberate confusion and obfuscation of some forms of fraud, the true figure could be even higher.



Since U.S. banks report aggregate pre-tax income of about $325B per year, a strong digital ID solution could improve a bank's reported profit by up to 35%.

If that's the potential impact, why is 'Digital Identity' not a C-suite issue?

Because there's no single choke point for these problems.

Peter Carroll, a Senior Partner at Oliver Wyman, puts it this way:

> "The way digital identity verification and authentication works today, the costs of current practices show up in multiple separate places across the bank. This issue simply cuts across too many organizational responsibilities to get the focus it really deserves."

The dollars at stake are significant, and aligning on this should be a CFO, COO, and CEO–level priority.

The two paths forward

We see two ways a bank can get to grips with this problem. One is incremental and cumulative; the other one is to go ‘whole hog’.

The incremental route

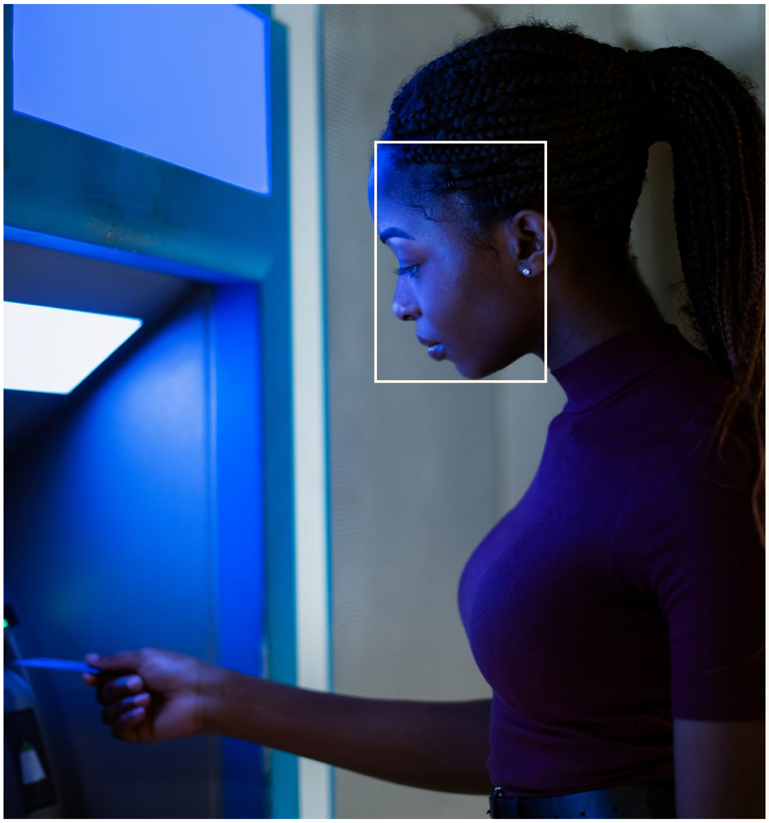
A bite-size approach can make good sense, picking off selected use cases where rapid gains can be made and implementation is easier. This could focus on areas like:

- Employee & contractor onboarding
- Passwordless workstation login
- In-branch customer document scanning and verification
- Upgraded remote-caller verification for password resets

The whole hog approach

The whole hog approach involves assembling a C-suite–level working group to tackle digital identity end-to-end. Done well, it can deliver the largest impact in the shortest time. However, it’s not without risk. Major institutions have been burned before by large-scale IT change, and digital identity touches enough systems, teams, and policies that poor governance can quickly derail momentum.

[1] The estimated total costs were $100-$125B in 2024; this number excludes regulatory fines & customer remediation and excludes any estimate of the monetary value of reputational damage; about 2/3rds of the total runs through banks’ P&Ls and the rest is borne by consumers, at least for now.



Contact us to

- Discuss which approach makes the most sense for your organization
- Review our experience implementing digital identity solutions in similar institutions
- Explore specific use cases where rapid gains can be achieved
- Assess the potential ROI impact on your bank’s bottom line
- Develop a roadmap for addressing digital identity challenges

Contact us