

ONE PAGER

5 Things Your CFO Should Know About the Cost of OTP

Your OTP solution costs more than you realize. As volume grows, so do delivery fees, failed attempts, support costs, customer abandonment, and fraud losses.

A more unified authentication approach can help you flip the model: recognizing trusted customers passively and reserving stronger controls for real risk. The payoff for your company is higher conversions, lower fraud, reduced operating costs, and growth without authentication spend growing alongside it.

1

OTP is a variable cost that scales with volume, not a fixed line item

Every message, retry, and step-up adds marginal cost. As transaction volume grows, so does spend with no ceiling and no efficiency of scale.

2

Failed authentication is unbudgeted revenue leakage

Delayed or failed OTPs drive abandonment at login, onboarding, servicing, and payment, which turns an authentication cost into a direct hit on top-line conversion.

3

Fraud exposure is funding your own cost center

Bots, SMS pumping, phishing, and repeat requests convert authentication infrastructure into an attack surface. CFOs end up underwriting the fraud through inflated messaging spend.

4

Hidden opex is distributed across multiple P&Ls

Retries, lockouts, support calls, investigations, and vendor management push costs into service, fraud, and engineering budgets. That makes the true cost of OTP harder to see and harder to control.

5

Unified authentication is actually a cost-reduction lever

Passively recognizing trusted customers reduces routine OTP volume while preserving step-up controls where risk actually warrants it, which improves unit economics without compromising fraud posture.

See how unified authentication can reduce costs and improve ROI.

Book a consultation →