8x8

Beyond OTPs:

Why BFSI needs bulletproof authentication (and how Descope delivers it)

Rethinking Trust: Moving Beyond OTPs for Stronger BFSI Protection

The BFSI sector is under relentless attack, and OTPs (one-time passwords) have gone from being a stopgap security measure to a glaring weak point. In the BFSI sector, what was once considered a simple and convenient option – OTPs sent via SMS or email – has increasingly become a prime target for exploitation. Banks and financial institutions are particularly vulnerable, as phishing kits, SIM-swap schemes, and malware routinely bypass these methods. The result is steep: escalating fraud losses, frustrated customers, and mounting support overhead.

Regulators are closing in. PCI DSS 4.0, SOC 2, and ISO 27001 emphasize phishing-resistant authentication. Governments mandated change: Singapore's MAS mandated a phase-out of OTPs for customers using mobile digital tokens, while Bank Negara Malaysia instructed institutions to move away from SMS OTPs altogether. The Philippines enacted RA 12010 (AFASA) to combat financial account scamming and require stronger risk controls. OTPs are no longer enough to meet compliance.

This is where **Descope** makes a difference. By delivering passkeys, adaptive MFA, and risk-based authentication through a no-code CIAM platform, Descope allows BFSI institutions to move beyond OTPs without disrupting operations. The payoff is clear: reduced fraud, higher customer trust, lower costs, and full regulatory alignment.

In an industry where trust is currency, moving beyond OTPs is not optional – it's survival.

OTPs: A Growing Risk in BFSI Security

For BFSI organizations, the weaknesses of OTPs are no longer theoretical – they are daily realities. OTPs are:

- **Phishable:** Attackers trick users into entering codes on fraudulent sites.
- **Interceptable:** SIM-swap fraud lets criminals hijack text messages.
- **Automatable:** Bots and malware scale credential stuffing and account takeover campaigns.

These flaws don't just compromise security – they erode business performance. Customers drop out of transactions when OTPs fail to arrive, call centers get flooded with "I didn't get my code" complaints, and fraud costs keep climbing.

Compliance compounds the issue. OTPs fail to satisfy the latest MFA requirements under PCI DSS 4.0 and FIDO2, which demand phishing-resistant, device-bound authentication. Banks and insurers clinging to OTPs face not just fraud risk but regulatory exposure.

In short, OTPs have reached their expiration date. Everyone – from regulators to customers to attackers – knows it. The question for BFSI isn't whether to replace them, but how quickly.

The Authentication Revolution – Passkeys & Risk-Based MFA

The industry is entering a post-OTP, post-password era. At the center of this shift are passkeys, built on public-private key cryptography and tied directly to user devices. Instead of relying on codes that can be intercepted, passkeys authenticate through biometrics or local device PINs, ensuring the private key never leaves the device.

For BFSI, the benefits are clear:

- **Phishing resistance:** Passkeys cannot be stolen through fake sites or SIM swaps.
- **Better customer experience:** One-tap logins and fewer failures mean higher conversions.
- **Lower costs:** Support calls tied to OTP delivery disappear.
- **Compliance alignment:** Passkeys meet FIDO2 and PCI DSS 4.0 requirements.

Layered on top is risk-based MFA. Instead of asking customers for codes at every step, BFSI institutions can use contextual signals – like device reputation, geolocation, or behavioral anomalies – to trigger step-up authentication only when needed. This balances security and convenience, protecting sensitive actions without burdening everyday transactions.

Together, passkeys and adaptive MFA mark a true revolution: strong protection that customers actually welcome.

Why BFSI Needs to Lead, Not Follow

Few industries carry more responsibility for trust than banking and financial services. When a breach happens, it's not just data at risk – it's money, livelihoods, and reputations. OTPs, once tolerated, now undermine that trust.

Unique BFSI pressures:

- **High-value targets:** Fraudsters prioritize banks and insurers because the payoff is direct.
- **Strict regulators:** Compliance frameworks are tighter here than almost anywhere else.
- **Insider risks:** Privileged access in BFSI demands stronger, context-aware controls.

At the same time, user expectations have changed. Customers now expect seamless, mobile-first, and passwordless experiences. Delays from failed OTPs don't just cause frustration – they drive churn.

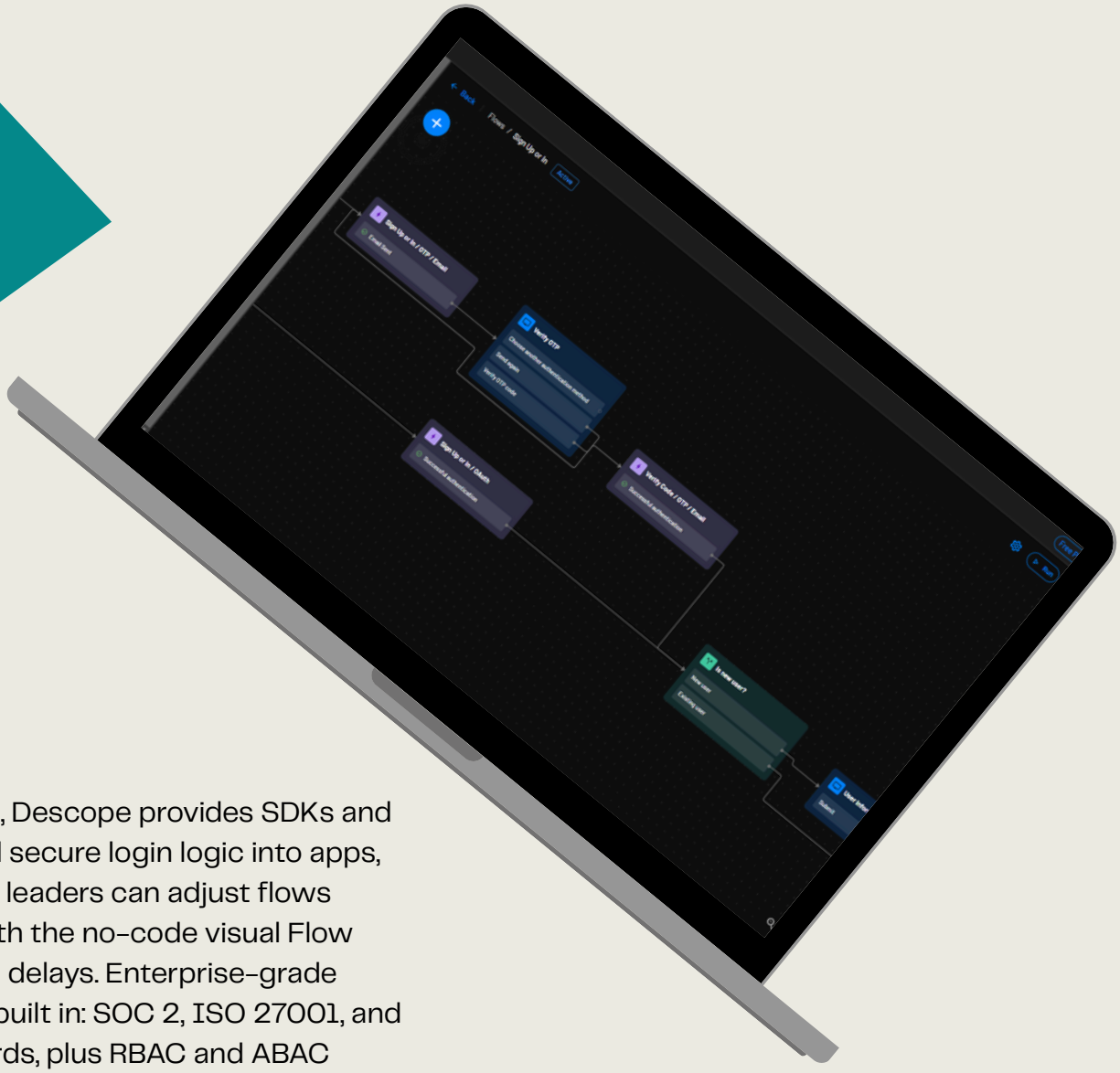
Boards and executives feel the squeeze: cut fraud, meet regulatory demands, and deliver digital experiences that rival fintech challengers. Passive, adaptive authentication isn't just security; it's a competitive edge.

For BFSI, leading on authentication is non-negotiable. Those who cling to OTPs risk being left behind – by attackers, by regulators, and by their own customers.

How Descope Simplifies Secure Authentication

Replacing OTPs doesn't have to mean massive rewrites or costly migrations. Descope offers a no-code visual flow builder and prebuilt authentication templates, allowing BFSI teams to drag-and-drop modern authentication steps without writing extensive code. Capabilities include:

- **Passwordless Authentication:** Deploy passkeys, social logins, one-tap passwordless flows and more.
- **Multi-Factor Authentication (MFA):** Add step-up MFA for sensitive transactions.
- **Device Fingerprinting & Geolocation Monitoring:** Spot unusual login behavior and detect anomalies.
- **Bot & Fraud Detection:** Block credential stuffing, automated attacks, and account takeovers.
- **Biometric & Behavioral Authentication:** Strengthen identity verification with face, fingerprint, or behavioral patterns.
- **Adaptive Authentication:** Adjust security dynamically based on risk context.
- **Full Audit Logging & Reporting:** Ensure compliance with detailed tracking and insights.
- **Omni Shield Integration:** Enhance fraud prevention with a dedicated protection layer.



For developers, Descope provides SDKs and APIs to embed secure login logic into apps, while business leaders can adjust flows themselves with the no-code visual Flow Builder, cutting delays. Enterprise-grade compliance is built in: SOC 2, ISO 27001, and FIDO2 standards, plus RBAC and ABAC controls to match BFSI's complex user hierarchies.

By integrating seamlessly with legacy systems like Auth0 or Cognito, Descope helps BFSI institutions modernize quickly, without ripping out existing infrastructure. The result is a future-proof authentication layer that reduces fraud, satisfies regulators, and keeps customers happy.

BFSI Use Cases – From Login to Transactional Trust

Authentication challenges in BFSI go far beyond login screens. With Descope, institutions can secure the entire trust chain:

- **Privileged users:** enforce step-up MFA for admins and insiders.
- **Fund transfers:** apply risk scoring and contextual MFA only when transactions look suspicious.
- **Retail banking:** replace OTPs with device-bound passkeys for fast, biometric logins.
- **External portals:** protect vendors and partners with MFA and bot detection.

By moving beyond OTPs, BFSI firms cut down on credential stuffing, account takeover, and fraud losses. At the same time, customers enjoy a frictionless, personalized experience – faster logins, fewer interruptions, and authentication tailored to their risk profile. Staff access stays tightly controlled, while regulators gain confidence that phishing-resistant methods are in place.

Descope doesn't just solve for login – it secures every interaction where money, identity, and trust intersect.

Migration Without Disruption – A Fast Track to Modern Auth

Moving away from OTPs can feel risky, but with the right approach, BFSI institutions can modernize quickly and safely. Descope makes migration a phased process: audit where OTPs are used, deploy passkeys in low-risk logins, then layer contextual MFA for sensitive actions like fund transfers or PII access.

Because Descope integrates with existing CIAM systems and banking platforms, changes don't require a full rebuild. Analytics help refine flows as adoption grows, while user education ensures smoother onboarding. The transition happens in weeks, not years, and without major disruptions to business operations.

The result is a practical path forward: BFSI firms replace OTPs step by step, strengthen compliance, and deliver better customer experiences – all while keeping systems running without interruption.

The Last OTP You'll Ever Need

OTPs once gave the illusion of security, but today they are a weak link attackers exploit with ease. Regulators are phasing them out, customers are tired of them, and fraud costs continue to rise. For BFSI, the choice is simple: evolve or fall behind.

Passkeys and adaptive MFA are the new standard – phishing-resistant, frictionless, and regulator-approved. Descope offers the fastest route to get there, combining no-code simplicity with enterprise-grade compliance.

The last OTP you'll ever need is the one you leave behind. By adopting modern authentication now, BFSI institutions secure users, protect reputations, and future-proof trust in a digital era.

Move beyond OTPs – secure your future with **Descope** today.