Summary: DSCI's Submission on RBI's Draft Framework on Alternative Authentication Mechanisms for Digital Payments

The Data Security Council of India (DSCI) submitted its inputs on the Reserve Bank of India's draft framework for alternative authentication mechanisms in digital payment transactions. Welcoming the RBI's move to enable innovation beyond OTP-based systems, DSCI emphasized the need for a forward-looking approach to secure and seamless authentication.

Key Recommendations:

1. **Broader Recognition of Authentication Factors:**

The draft limits authentication to three traditional factors—something the user knows, has, or is. DSCI recommended including newer methods like behavioral biometrics and contextual authentication, already recognized under RBI's Master Directions on Digital Payment Security Controls.

2. **Revisiting the Definition of 'Dynamic' Factors.**

DSCI noted that widely used and secure methods like passkeys (public-private key cryptography) and biometric-based authentication may not qualify as "dynamic" under the current definition. It urged the RBI to clarify or expand this definition to include modern, secure approaches used by industry players.

3. **Balanced Approach to Customer Consent**

While acknowledging the importance of user consent, DSCI raised concerns about shifting the burden of security decisions to users. It recommended a risk-based approach to consent, highlighting the complexity of digital transactions and the risk of "security fatigue" among consumers.

Conclusion

DSCI's submission underlines the importance of supporting innovation while preserving user trust, privacy, and a frictionless digital experience. It urges the RBI to encourage diverse, risk-aware authentication solutions that reflect global best practices and contemporary technological realities.