PASSKEY VS. MFA BREAKDOWN

FEATURE/FACTOR	PASSKEY	MULTI-FACTOR AUTHENTICATION
Authentication Method	Passwordless — uses cryptographic key pairs and device biometrics or PIN	Requires password plus an additional factor like a code from an app, SMS, hardware token, or biometrics
Security Strength	**Very high:** resistant to phishing, replay attacks, and credential stuffing	**High:** significantly improves security over password alone but can be vulnerable to SIM swapping and social engineering
User Experience	**Seamless and fast:** no passwords to remember or enter, uses device-native biometric/PIN	**Slightly slower:** involves entering codes or approving prompts, which can add friction
Phishing Risk	**Near zero:** no shared secret sent over network to intercept	**Moderate:** attackers may trick users into sharing MFA codes or approving fraudulent requests
Device Dependency	Strongly tied to specific devices that store passkeys securely	Can be more flexible — codes can be received on multiple devices, depending on method
Setup Complexity	Requires compatible hardware/software and initial enrollment	Generally easy to set up, widely supported across platforms
Recovery Options	Recovery can be complex if device is lost — requires backup devices or recovery processes	Often easier — backup codes or alternative methods can be used for account recovery
Potential Risks	Device loss or theft can pose risk if biometrics/PIN are compromised	SIM swapping attacks can intercept SMS codes; users may approve fraudulent MFA prompts