entersekt
The Financial Authentication Company.

Scam prevention solution checklist

The Entersekt difference:

A single, fully integrated solution leveraging the strengths of all available authentication methods on the market. Our solution is driven and augmented by proprietary Entersekt technologies and signals, enabling the right solution for the type of attack, in real-time. Compare our comprehensive scam prevention capabilities to others on the market.

Capability	Entersekt	Vendor #2
Behavioral analytics Analyzes patterns in user actions (typing speed, mouse movements, login habits) to detect anomalies and potential fraud, providing an invisible layer of security that adapts to individual user behavior.	✓	
Risk engine A system that analyzes various data points to assess the likelihood of fraud or unauthorized access, dynamically adjusting security measures to balance protection and user experience.	✓	
Cross-channel risk analysis Ability to detect and correlate fraud signals across multiple customer interaction points – such as digital banking (web browsers, mobile apps, chat banking, call centers) and e-commerce (3-D Secure) transactions – ensuring a unified and consistent fraud prevention approach.	✓	
Identity proofing Verifies that users are who they claim to be, using various methods including document verification and biometric checks, ensuring high-risk events and transactions are protected.	✓	
Push authentication Sends a secure, real-time alert to a user's trusted device, requiring a simple tap or approval to verify their identity or authorize a transaction, adding an extra layer of security and convenience.	✓	
Biometrics and passkeys Uses a customer's unique biological traits (fingerprint, face, voice) to verify their identity, offering a secure and convenient alternative to passwords that is phishing-resistant and user-friendly.	✓	
Trusted device ecosystem Where users explicitly trust their devices for continuous evaluation of trust status based on device behavior, location, and risk signals. This prevents fraudsters from hijacking accounts even if they obtain credentials.	✓	
Cryptographic device binding with persistent device ID Device ID using cryptographic keypairs, silently signing a transaction for passive authentication purposes.	✓	
Device consortium Vital information and signals about originating and authenticating devices to block fraud.	✓	
Proximity proof authentication Blocking remote fraudsters from approving unauthorized actions by scanning a QR code on the originating channel, with the authenticating device.	✓	
Data sharing across systems and channels Risk, authentication, and channel systems that share data seamlessly for more effective protection.	✓	
Context Aware™ Authentication Authentication adapts based on user behavior, transaction type, channel and risk level.	✓	
Regulatory compliance Assists you in meeting PSD2, Open Banking, and other security requirements without adding unnecessary friction to the customer journey.	✓	

Speak to a fraud expert now