Docusign Envelope ID: E894307D-FF64-4728-90C7-3102CD20CD8A

BixeLab

Biometrics Identity Experience & Evaluation Laboratory

Letter of Confirmation

Issued to FaceTec, Inc.
for the test report issued on the 27th of October 2025 for
Injection Attack Detection (IAD) evaluation of,
FaceTec SDK (Mobile v9.7.83, Web v9.7.76)

To whom it may concern,

BixeLab (NVLAP Lab Code: 600301-0) is accredited by the NIST-administered National Voluntary Laboratory Accreditation Program (NVLAP) to ISO/IEC 17025:2017 for services listed on its published scope. NVLAP does not currently accredit IAD to CEN/TS 18099: this evaluation was conducted in close alignment with CEN/TS 18099, but does not yield an NVLAP-accredited outcome.

Between September and October 2025, BixeLab conducted an independent Injection Attack Detection (IAD) evaluation of FaceTec's Mobile and Web SDKs (v9.7.83 and v9.7.76 respectively). The evaluation exercised a range of representative injection attack methods (IAMs) and injection attack instruments (IAIs) across mobile and web environments to assess the system's resilience under controlled test conditions.

Testing parameters

- **Platforms:** Android 13, iOS 18.5, and Web SDK on Windows/macOS.
- **Injection Attack Methods (IAMs):** Virtual-sensor injection (OBS and USB capture card), rooted-device manipulation, emulator-based execution, API injection, and code review.
- **Injection Attack Instruments (IAIs):** Four representative species – selfie images, passport-style images, face morphs, and deepfake videos.
- **Bona fide runs:** 1 classification error across 50 bona fide presentations. Note: The single BPCER occurred when the IUT prompted the user to retry. The user was not blocked and ultimately passed the liveness check within allowed retries. This resulted in 0% user level BPCER.
- **Injection Attempts:** All 48 IAI transactions via USB capture or other vectors resulted in "Retry Required" or equivalent rejections. Attempts to bypass protections through virtual cameras, rooted devices, emulators, API payloads, and JavaScript tampering were unsuccessful.
- **Integrity & Environment Controls:** All tests executed under controlled lab conditions at BixeLab's Canberra facility using predefined test devices and toolchains. Root detection, encryption protocols, code obfuscation, and tamper-detection mechanisms were confirmed to be active and effective

Conclusion

Within the scope of executed testing, no successful injection exploit was observed. The system consistently responded to all injection attempts with appropriate defences, such as blocking, retry prompts, or session cancellation. See full details in test report (*[Final] 25_BXL051_TR_01 Injection v1.1*).

Ms. Somya Singh
Operations Manager
BixeLab Pty Ltd
info@bixelab.com

Dr. Ted Dunstone
Senior Responsible Officer
BixeLab Pty Ltd
info@bixelab.com

NOTE: This letter is a validation summary only i.e., this was not a certification, benchmark, or endorsement by NIST, NVLAP, or any government agency. The results apply only to the stated versions, configurations, datasets, and conditions; coverage is limited to the tested IAMs/IAIs, it may be reproduced only in full, and BixeLab accepts no liability for use beyond the stated purpose.