

Letter of Confirmation

Issued to Oz Forensics Software Trading L.L.C
for the test report issued on the 19th of August 2025 for
Injection Attack Detection (IAD) evaluation of,

OzLiveness Demo (Android SDK v8.17, iOS SDK v8.17) and OzWebLiveness Demo SDK v1.7.14

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 and does not yield an NVLAP-accredited outcome.

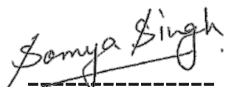
Between May–August 2025, BixeLab independently evaluated the IAD posture of OzForensics' liveness solutions listed above. The objective was to exercise representative injection attack methods (IAMS) and injection attack instruments (IAIs) and record outcomes under controlled conditions in a test environment.

Testing parameters

- **Platforms:** Web SDK (Windows/macOS), Android 13/14 (v8.17), iOS 18.5 (v8.17).
- **Injection Attack Methods (IAMS):** virtual-sensor injection (virtual camera) and platform-integrity checks (emulator/rooted device), network/API observation.
- **Injection Attack Instruments (IAIs):** six species including static selfie image, passport-style image, prerecorded video, deepfake video, live video stream (e.g., Teams), and live face-morph output.
- **Bona fide runs:** Web (15), Android (5), iOS (5) with 0% BPCER.
- **Injection attempts:** 100 virtual-camera attacks across 6 IAI species and 4 subjects. All attacks were declined by back-end PAD classification (APCER 0%). The SUT exposes no explicit "IAD detected" flag, therefore IAD verdicts were inferred from PAD outcomes.
- **Integrity & environment controls:** Native apps blocked emulator/simulator use and detected rooted devices, concealment attempts were unsuccessful.

Conclusion

Within the executed scope, no injection bypass was achieved. All six IAI species delivered via a virtual camera were declined, and native apps enforced platform-integrity checks. Web transport/session handling would benefit from clearer auth semantics, anti-replay binding, and an explicit IAD flag in logs and results to distinguish IAD from PAD outcomes. See full details in test report 25_BXLO46_TR_01.v2.0.



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.