FaceTec's Third-Party Testing & Security Initiatives

November 21st, 2025

FaceTec's 3D Liveness and Face Matching technology has been rigorously evaluated by independent, NIST/NVLAP- and ISO/IEC 17025-accredited labs and security firms for Presentation Attack Detection (PAD) compliance under ISO/IEC 30107-3, injection attack detection (IAD), face matching accuracy under ISO/IEC 19795-2, biometric subsystem certification, and advanced spoof bypass resistance.

Testing began with foundational matching certifications in 2017, and FaceTec was the first Liveness vendor in the world to pass Level 1 & 2 PAD certification in 2018/19. Since then, FaceTec has progressed to higher PAD/IAD levels (up to Level 5 injection attacks and equivalent high-level IAD), reverse engineering assessments, face matching evaluations, and regular recertifications on updated SDK versions.

All PAD/IAD tests have achieved 0% successful attacks (0% APCER), while matching tests show extremely low error rates, demonstrating unmatched resistance to photos, videos, masks, deepfakes, injection attacks, and other threats, combined with high-accuracy 3D-to-2D/3D-to-3D face matching. Complementing these third-party validations is FaceTec's ongoing $600,000 Spoof Bounty Program, which crowdsources real-world vulnerability discovery as highlighted by ENISA ID Proofing guidelines.

Whitepapers listed on FaceTec's site (Resources) provide context for these results, including:

- **FaceTec 3D Face Matching Whitepaper**: Details the algorithm, false acceptance rates (<0.000008%), and demographic bias testing. Link
- **Intro to UR Codes**: Explains digitally signed biometric barcodes. Link
- **Liveness Detection Security Report**: Summarizes current attack techniques and defenses. Link

The **ISO/IEC 30107-3** standard defines only **three levels** of Presentation Attack Detection (PAD), covering physical spoofs only:

- **Level 1**: Basic 2D attacks - photos, video replays
- **Level 2**: Commercially available 3D masks and dolls
- **Level 3**: Expensive, custom-crafted, realistic masks or heads

These Levels 1-3 do **not** address attacks that bypass the camera. Bypasses and Injections are very scalable using deepfakes, so **FaceTec created Levels 4 & 5 in 2018** (more info on **Liveness.com**):

- **Level 4**: Payload tampering, bypass, decryption, or reverse-engineering of the encrypted data
- **Level 5**: Injection Attack Detection (IAD) – deepfakes, virtual cameras, emulators, rooted-device hooking, API tampering

Passing only ISO Levels 1–3 leaves systems wide open to low-cost Level 4/5 attacks that dominate today's fraud. True security for banking and eKYC therefore requires independently verified resistance across **all five levels** — the benchmark FaceTec alone has consistently met and repeatedly achieved.

Below is a year-by-year breakdown of the third-party testing focused on PAD levels, matching conformance, and security certifications.

Year	Testing Lab	Level & Focus	Date	Key Results	Letter/Report
2017	iBeta Quality Assurance	DEA EPCS Biometric Subsystem Cert (21 CFR Part 1311) – Face Matching	June 23, 2017	False Match Rate (FMR) well below required ≤0.001); 4,295 attempts on 100 subjects; ZoOm SDK v5.1.1.	DEA EPCS Biometric Subsystem Certification Report
2018	iBeta Quality Assurance (NIST/NVLAP Lab: 200962)	PAD Level 1 (Basic spoofs: photos, videos)	Aug 20, 2018	0% Imposter Attack Presentation Match Rate across ~1,500 attacks; 6 species; ZoOm v6.6.0.	Level 1 Pass Letter
2019	iBeta Quality Assurance (NIST/NVLAP Lab: 200962)	PAD Level 2 (Advanced spoofs: 3D masks, dolls)	Feb 7, 2019	0% success rate across 1,800 attacks; 6 high-fidelity artifacts; ZoOm v6.9.11.	Level 2 Pass Letter
2023	BixeLab Pty Ltd (NIST/NVLAP Lab: 600301-0)	3D-to-2D Face Matching (ISO/IEC 19795-2 tech eval)	May 2023	At threshold 6: FMR 0.005%, FNMR 2.21%; 1,005,007 comparisons on 1,002 diverse subjects; FTA 0%.	3D-2D Face Match Report
2023	BixeLab Pty Ltd (NIST/NVLAP Lab: 600301-0)	PAD Level 2 (advanced spoofs)	June 27, 2023	0% APCER across 2,100 Level 1 & 2 attacks; tested on SDK v9.x.	Level 2 Pass Letter
2025	Praetorian Security, Inc.	Level 4 Bypass & Reverse Engineering	Aug 27, 2025	0 vulnerabilities (critical/high/medium); 200 hours pen-testing; resisted all bypass attempts on SDK v9.7.x.	Level 4 Pass Letter
2025	BixeLab Pty Ltd (NIST/NVLAP Lab: 600301-0)	PAD Levels 1–3 & Level 5 Injection Attacks (v9.7.x)	Oct 27, 2025	0% APCER on all PAD; 100% rejection of 48 injection attacks (emulators, API tampering, virtual cams); Android/iOS/Web.	Level 1 Pass Letter Level 2 Pass Letter Level 3 Pass Letter Level 5 Pass Letter
2025	Ingenium Biometric Labs (ISO/IEC 17025 & FIDO accredited)	PAD Level 3 & Injection Attack Detection – L-2 IAD (equivalent to CEN/TS 18099 Level High)	Nov 20, 2025	0% APCER on Level 3 Masks; 100% detection of injection attacks; >40 attack types (emulators, hooking, rooted devices); BPCER met; tested on Android SDK v9.7.92.	Level 3 Pass Letter Level 5 (IAD L-2) Pass Letter

About Ingenium Biometrics Lab

Ingenium Biometric Laboratories operates as an independent, ISO/IEC 17025:2017 and FIDO-accredited test laboratory, with its accreditation granted by a national body that is a full signatory to the International Laboratory Accreditation Cooperation (ILAC) Mutual Recognition Arrangement (MRA). Under the ILAC MRA and its link to the European co-operation for Accreditation (EA), the principle of "Accredited once, accepted everywhere" applies within the European Union: test reports and certificates issued by Ingenium and bearing the ILAC MRA mark from its signatory accreditation body are recognized as equivalent to those issued by any EA-member accreditation body in the EU.

This is explicitly supported by the mutual recognition framework described by European Accreditation, meaning that regulators and public authorities across EU Member States accept Ingenium's results without re-testing or additional certification. Provided the biometric testing falls within the accredited scope (as listed by its accreditation body), its test reports therefore carry full validity and legal recognition throughout Europe, facilitating seamless compliance for products relying on those results.

- European Accreditation – Mutual Recognition / IAF-ILAC Recognition: european-accreditation.org/mutual-recognition/iaf-ilac-recognition
- Regulation (EC) No 765/2008: EU framework for accreditation overview
- ILAC Mutual Recognition Arrangement (MRA): ilac.org/ilac-mra-and-signatories

FaceTec's $600,000 Spoof Bounty Program

Launched in the fall of 2019 to proactively identify any potential vulnerabilities in its 3D Liveness detection and security layers, FaceTec's Spoof Bounty Program invites ethical hackers, researchers, and security experts worldwide to attempt to bypass the technology. It operates across five escalating levels covering basic presentation attacks (e.g., photos/videos) up to sophisticated injection attacks (e.g., emulators, API exploits, and real-time face swaps).

Key Details:

- **Eligibility and Rules**: Open to individuals or teams. Participants must use provided test accounts/environments and adhere to ethical guidelines. Attacks must be reproducible, novel (not previously patched), and target the latest SDK versions.
- **Payout Structure**: Bounties scale by level, with the total pool distributed based on severity and impact. Claims require video proof, detailed methodology, and independent verification.
- **Submission Process**: Submit via the program's email: bounty @ FaceTec dot com, including attack demos and reports. FaceTec evaluates within days, with payouts upon confirmation.
- **Achievements and Status**: For over 5 years, no bounties have been claimed despite extensive global participation and integration with third-party testing (e.g., Praetorian's 160+ hours in 2025 found zero viable exploits). This underscores the program's role in enhancing real-world security against emerging threats like AI-generated deepfakes. For details, visit Spoof Bounty Program.

These tests and initiatives confirm FaceTec's leadership in secure 3D biometrics, with cumulative resistance to over 150,000+ lab attacks plus>3.5 billion real-world 3D Liveness checks annually.