1 August 2025

To whom it may concern,

iBeta Quality Assurance conducted Presentation Attack Detection (PAD) testing in accordance with ISO/IEC 30107-3. iBeta is accredited by NIST/NVLAP (NVLAP Lab Code: 200962) to test and provide results to this PAD standard (certificate and scope may be downloaded from the NVLAP website).

This testing was conducted with TransUnion's TruValidate Anti-Deepfake Liveness v3.3.5 (iOS) application installed on an Apple iPhone 13 Pro running iOS 18.4.1 and supported by the MD5 967584f471bf7446ebd0a63c2577369e algorithm, and TransUnion's TruValidate Anti-Deepfake Liveness v3.3.5 (Android) application installed on a Samsung Galaxy S20+ 5G running Android 13 and supported by the MD5 c9c39f17f38b588349a5bdabf79befb8 algorithm. iBeta conducted active liveness testing from 16 May to 1 August 2025.

Testing was conducted in accordance with the contract for a level of spoofing technique that only utilized mid-level methods to create an artefact of the genuine biometric for use in the presentation attack. The subjects for the test effort were cooperative – meaning that they were willing and able to provide any and all biometric samples, including high quality biometric facial samples. The test time for each PAD test per Presentation Attack Instrument (PAI) was limited to 24 hours. This is considered a Level 2 PAD test effort (second of three levels).

The test method was to apply 1 bona fide subject presentation that alternated with 3 artefact presentations such that the presentation of each species consisted of 150 Presentation Attacks (PAs) and 50 bona fide presentations, or until 24 hours had passed per species per device. The results were displayed for the tester as "Deepfake Verification Success" for a successful presentation or "HACK" for an unsuccessful presentation.

iBeta was not able to gain a liveness classification with the presentation attacks (PAs) on either the iPhone 13 Pro or Galaxy S20+ 5G. With 150 PAs for each of 5 species, the total number of attacks was 1500 (750 per device), and the Attack Presentation Classification Error Rate (APCER) was 0%. The Bona Fide Presentation Classification Error Rate (BPCER) was also calculated and may be found in the final report.

TransUnion's TruValidate Anti-Deepfake Liveness v3.3.5 (iOS) and TruValidate Anti-Deepfake Liveness v3.3.5 (Android) applications and backend supporting components were tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and found to be in compliance with Level 2.

Best regards,

Ryan Borgstrom
iBeta Quality Assurance Director of Biometrics
(303) 627-1110 ext. 182
RBorgstrom@ibeta.com