12 April 2022

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 the Fraud.com Udentify 1.0 application and associated server v2.1 on both an Android and iOS device. The testing was conducted from 3 March through 12 April 2022 on two smartphones (iPhone XR with iOS 14.6 and Galaxy S20 with Android 10.0).

Testing was conducted in accordance with the contract for a level of spoofing technique that only utilized simple, readily available methods to create artefacts 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 photos and videos of their likeness. The test time for each PAD test per PAI was limited to 24 hours. This is considered a Level 2 PAD test effort (second of three levels).

The test method involved enrolling 6 subjects and having them authenticate five times successfully. Six species of presentation attacks (PAs) were then attempted ten times each. As each attempt was conducted, the application would generally provide instructional messages.

A successful match would state 'Authentication success', or a failure message that stated 'Somethings Wrong! You did not successfully perform face recognition'. Across both devices, over 600 total presentation attacks were attempted. At the conclusion of the PAD testing, the subject returned and authenticated five times successfully to verify that the facial recognition application was still able to recognize the genuine subject.

iBeta was not able to gain unauthorized access with the PAs yielding an overall Presentation Attack (PA) success rate of 0%, which then equates to the overall combined Imposter Attack Presentation Match Rate (IAPMR) of 0%. The bona fide False Match Rate (FMR) also calculated at 0%. Other metrics may be found in the final report. The Udentify 1.0 application and associated server v2.1 was tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and was found to be in compliance with Level 2 on both the iPhone XR and Galaxy S20.

Best regards,

Ryan Borgstrom
iBeta Quality Assurance Director of Biometrics
RBorgstrom@ibeta.com
303.627.1110 extension 182