authID.ai Achieves Perfect Score for ISO Level 2 Biometric Presentation Attack Detection

May 03, 2022

Verified™ successfully recognized and prevented 700+ presentation attacks for a perfect 0% intrusion rate

LONG BEACH, NY , May 03, 2022 (GLOBE NEWSWIRE) -- authID.ai [Nasdaq: AUID], a leading provider of secure, mobile, biometric identity authentication solutions, today announced that the company's Verified™ platform has achieved conformance with ISO 30107-3 Level 1 and 2 standards for Presentation Attack Detection (PAD). Testing was performed by iBeta Quality Assurance, one of the few Independent Test Labs in the nation accredited by NIST NVLAP (NVLAP Testing Lab Code 200962-0) to perform biometrics testing.

With over $43 billion lost to digital identity fraud per year, authID is committed to bringing best-in-class technology to defend private and public sector enterprises from cybersecurity risks caused by credential compromise and identity theft. To that end, IBeta conducted rigorous testing specifically intended to defeat authID.ai's passive liveness detection algorithms by performing presentation attacks on the subsystems. With a total of 360 attempts on Level 1 and 360 attempts on Level 2, Verified successfully recognized and prevented all 720 presentation attacks for a 0% failure rate—passing with a perfect score for both levels.

"This independent confirmation further demonstrates how Verified can provide additional fraud protection and security to authID customers," said Jeremiah Mason, SVP, Product, at authID.ai. "Our ISO 30107-3 Level 2 compliant PAD system, along with authID's ability to bind a user's biometrics to their identity, prevent presentation attacks and provide stronger safeguards against fraud and account takeover, by authenticating the person instead of what they know or have."

Presentation attacks occur when fraudsters attempt to attack a biometric system by creating spoofs or fakes that are then presented to the biometric sensors. Such spoofs can use a printed photo, an image or video of a person on a tablet, 3D masks, models, or other forms of impersonation.

If identity spoofing succeeds, organizations and their users can be exposed to heightened security risks and data breaches that can damage user trust and have severe financial implications. Last year in China, a two-person team successfully employed presentation attacks using darknet-sourced biometric data to gain $75 million from fake tax invoices sent to the artificial clients of a Shanghai shell company.

authID's Verified platform detects these attacks through a combination of active consent and passive liveness challenges on the user's facial image in addition to other security features. authID's active consent prompts users to smile when capturing their selfie, which provides the first test to help ensure that the person engaging with the system is present, live, and intends to authenticate.

Verified's passive liveness process captures images from a user's mobile phone camera or desktop webcam, and analyzes them against several quality metrics. These frames are then sent through a pipeline of multiple presentation attack detection algorithms to detect spoofing attempts. The aggregate scores of these processes are returned by the system to indicate whether a biometric sample is authentic and should be considered for facial verification.

"Active consent and passive liveness are critical in ensuring that account takeover, identity theft, or other digital fraud don't plague your systems and users, which saves businesses money and protects their reputation in the long run," said Tom Thimot, CEO of authID.ai. "We are proud to bring our best-in-class AI and Presentation Attack Detection technology to customers across a range of market segments to make the digital world a safer place for all."

About authID.ai
authID.ai (Nasdaq: AUID), formerly Ipsidy, provides secure, mobile, biometric identity verification software products through an easy-to-integrate Identity as a Service (IDaaS) platform. Our suite of self-service biometric identity proofing and authentication solutions frictionlessly eliminate passwords through consent-based facial matching. Powered by sophisticated biometric and artificial intelligence technologies, authID.ai aims to strengthen security and trust between businesses and their customers. We Are Digital Identity. For more information, go to www.authid.ai.

Media Contact
Natalie Shutts
The Bliss Group
nshutts@theblissgrp.com