NASS Summer Conference 2024

Evolving Threat Landscape and Advanced Solutions in Identity Verification

Over the past several years state and federal governments have prioritized the expansion of digital services, opening new channels to engage with constituents. Digital Services Expansion was ranked as the #2 priority overall for State CIOs in the most recent NASCIO CIO Survey. This expansion includes the enabling of new online services which were previously only available through in-person engagements. These more complex and sensitive transactions require states to increase website and portal security and implement remote identity verification to prevent fraudulent activity. The most secure and accurate method for verifying identity for remote transactions is through the use of biometric verification, which leverages software that guides the end user through a process of presenting and capturing their identity credential and a selfie image and submitting this information for comparison against a government source of truth, such as a motor vehicle record. This process, commonly referred to as IDV, is secure, effective, and pervasive in many commercial markets as well.

Biometric Verification – Now Mainstream

Biometric identity verification has emerged as a highly accurate method, particularly through image matching alternatives using 1:1 facial recognition. This method involves matching a selfie to a verified credential to verify identity. This form of Biometric Identity Verification is now mainstream, as evidenced by the federal government's General Services Administration (GSA) Equity Study on remote Identity Proofing. This project evaluates verification solutions across multiple demographics to measure and prevent skin-tone bias and ensure that government websites are accessible to all individuals. A select group of technology vendors accepted to participate in this important ongoing study and results are stated to be released by the end of 2024. For more information on this study participants, see: https://www.nextgov.com/digital-government/2023/08/gsa-looking-participants-its-facial-recognition-study/389550/

AI and Deep-Fakes – Detection and Prevention

The IDV process employs multiple technologies including Document Authentication, Liveness Detection, and Facial Recognition to complete an identity verification. Like any security or fraud prevention technology, IDV solutions must continuously evolve to stay ahead of fraudsters who continually try and compromise the system to perpetrate identity theft and other crimes. State CIOs and other technical leaders have long considered both Generative Artificial Intelligence (GenAI) and AI generated deep-fakes and injection attacks as emergent threats. These technologies are used by fraudsters to imitate someone's likeness by creating a digital AI generated image or video and presenting it as a legitimate live image or video feed of a live person. Deep fakes are increasing in quality and the ease in which they can be created, lowering the barriers to entry for creating sophisticated and highly realistic forgeries of documents, credentials, images, and videos. AI can also help fraudsters create completely synthetic identities (non-existent individuals) and use these identities to open accounts, apply for government services or register to vote.

Deep-fake Presentation Attacks

While AI has created new attack vectors, these attacks can be detected and prevented. In order to combat and defend against these presentation attacks, identity solution providers continually train and improve their presentation attack detection algorithms to be able to identify deep-fakes. The next generation of solutions use Machine Learning (ML) and Artificial Intelligence (AI) to continually improve its library of algorithms or models to maintain its position as a market leader in liveness detection and fraud prevention in remote transactions. By using the latest AI technology and continually training the models with AI generated images, videos, and other fraudulent presentations, the models become more accurate in their ability to detect deep-fakes and other document or credential manipulations used by todays fraudsters.

Injection Attacks

Liveness detection refers to the ability of a system to determine whether the biometric data being presented is from a live person rather than a static image, video, or other forms of spoofing attacks. Employing AI models trained to detect inconsistencies in textures from face swaps and morphs and utilizing layered models such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and generative adversarial networks (GANs) for comprehensive fraud detection is especially important. Additionally, behavioral analysis and pattern recognition techniques are essential for identifying anomalies in user actions and detecting virtual cameras and software signatures, thereby blocking potential vulnerabilities. Preventing injection attacks through stringent security measures ensures that only genuine interactions are processed. Continuous training of AI models and adherence to industry standards, such as those set by Then National Institute of Standards and Technology, are vital to maintaining the integrity and trust of identity verification systems.

NIST – Independent evaluation of IDV solutions promotes trust and confidence

The National Institute of Science and Technologies (NIST) at the U.S. Department of Commerce helps businesses and government entities better understand, manage, and reduce their cybersecurity risk and protect their networks and data. NIST plays a key role in identity verification as the standards body that defines minimum technical capabilities, and security standards around digital identity, facial recognition (FR), face liveness detection, and the identity verification process. Market leading solutions work to adhere to appropriate standards and submit their FR and Liveness Detection algorithms for testing by NIST through the FRTE and FATE evaluation programs. FRTE evaluates facial recognition algorithms for speed and accuracy in one-to-one (1:1) and one-to-many (1:N) comparisons, demographics, face masks and other attributes, while the FATE program evaluates performance against image quality, age estimation and presentation attacks. Solutions should be given high consideration for participation and rankings achieved in these tests.

NIST also administers the National Voluntary Laboratory Accreditation Program (NVLAP) and oversees accreditation programs offered by independent laboratories for conformance to ISO/IEC 30107-3 (Biometric PAD - Part 3: Testing and Reporting and ISO/IEC 30107-1

Biometric PAD – Part 1: Framework. iBeta is the most widely used laboratory for this testing. These tests help benchmark model performance and provide the ability to compare solutions across multiple criteria. Solutions that carry the trust mark for iBeta conformance at PAD level 2 have demonstrated their ability to detect and prevent deep-fake presentation attacks for thousands of scenarios using digital and physical presentation attack methods.

Similarly, NIST works with other third-party organizations to confirm conformance with NIST standards for the strength of an identity proofing event. As an example, the Kantara initiative is a NIST sanctioned conformance initiative that confirms that solutions conform to the NIST standard for Identity and Authentication levels 1 through 3 (IAL 1, 2, 3; AAL 1, 2, 3) as set by NIST 800-63 standards for identity privacy and security. Companies that carry the Kantara trust mark have demonstrated through testing and audit that they meet NIST standards for these critical levels of proofing, which correlate to the strength of the proofing or authentication event. As an example, Incode's Solution carries the Kantara trust mark for IAL2. Kantara lists accredited assessors and conformance levels on their website at: https://kantarainitiative.org/trust-status-list/.

Ongoing testing and conformance certification is critical to ensuring that technical solutions are maintaining and improving accuracy across the developing threat landscape. These programs, like the technology they test, are continually evolving and improving to provide state agencies with the ability to benchmark and evaluate solution performance.

The Future for Eliminating Identity Fraud - Leveraging the System of Record

In identity management, the "system of record" (or SOR) is often used to reference each Department of Motor Vehicles' (DMVs') biographic and face-image database. The DMVs' SOR receives this designation because, in the U.S., it is generally considered the most thoroughly, in-person vetting process of identities, done so by trained examiners, and regularly maintained though legal requirements. One leading vendor is pioneering new methods in remote, biometric IDV architecture that leverages the SOR through a revolutionary matching service that simply matches a selfie, voluntarily submitted by an individual, against their DMV record to confirm identity. This process leverages data from the driver license to identify the individual in the DMV system of record and then performs a match of the selfie image to the image on file at the DMV. The process is consent-driven and is performed without capture or storage of any state held individual Personally Identifiable Information (PII). By employing standards-based and conformant technology to perform a match against the system of record in a way that protects the privacy and security of individuals' and states' data, the verification process is even more accurate and does require correlation against any third-party data resources, which drives up costs and increases the security threat profile.

In summary, identity verification solutions must evolve to address the increasing sophistication of identity fraud, leveraging advanced technologies such as AI, ML, and biometric verification while ensuring compliance with security standards and accessibility guidelines. Incode is committed to providing innovative identity verification solutions that

are secure, efficient, and compliant with the highest standards and offer an identity solution that can meet the requirements of state agencies and offices.