Identity Verification Done Right: A Primer for Background Screeners

A follow-up guide to "Identity Verification Done Right: Reducing Fraud Without Friction," PBSA 2026 Annual Conference, Arlington, TX

Janice Kephart, ZipID, Inc. | **Chuck Salvia**, Salvia Consulting

Why this guide

Our panel had 45 minutes. This primer goes further than the live session could. It expands the data points and the provider questions we presented, and it adds material from Janice Kephart's PBSA 2026 Mid-Year session, "Identity Fraud is Surging: Using the I-9 as Employers' Strongest Trust Signal" alongside more recent hiring fraud data. Our goal is a practical reference for all those that deal with new hires: what identity verification is, where it belongs in the hiring workflow, and what to ask before trusting any provider with it and understanding why those questions matter to both you and your clients.

The one question running through all of it: ***how do we know the person is who they claim to be?***

1. Screened does not mean authenticated

A background check confirms that records exist for an identity. It does not confirm that the person presenting that identity is its rightful owner. The fraud data says that gap is now being used at scale:

- **Gartner** projects that about 1 in 4 job candidate profiles worldwide could be fake by 2028.
- **Pindrop, a deepfake detection company,** found signs of fraud in 1 in 6 of its own remote applicants. One candidate, "Ivan X," applied to its deepfake detection team, was rejected, and reapplied eight days later under a new face, reaching the interview stage.
- **Entrust's 2026 Identity Fraud Report** shows physical counterfeits at 47% of document fraud and digital forgeries at 35% and puts fraudulent driver's licenses at 37% of U.S. ID fraud.
- **The Social Security number is the weakest link.** GAO has tied 1.3 million SSNs to employment fraud, and IRS/TIGTA has identified more than 818,000 SSN misuse cases. Children's SSNs carry roughly 51 times the misuse risk, because no one checks them for years.
- **Synthetic identities are a significant fraud threat.** Most of the new-account fraud has been estimated to involve synthetic identities. GAO has flagged it as a growing concern and examined SSA's eCBSV service as a tool to combat it.
- **DOJ indictments of North Korean IT worker schemes** (2018 to 2024) describe roughly 300 U.S. companies infiltrated using at least 160 stolen U.S. identities, generating about $88 million, with forged documents, deepfakes during hiring, and U.S.-based "laptop farms."
- **E-Verify does not close the gap.** At Glenn Valley Foods in Nebraska, a decade-long E-Verify user, a June 2025 ICE action detained 76 workers, about 70 of whom were using stolen SSNs and fake identities. E-Verify compares data against federal records. It does not authenticate the document, match a face, or confirm the person is the rightful owner of the SSN.

2. What identity verification is

Identity verification is not a records search. It is a live test of the person and the document, in three parts:

1. **Document authentication.** Is the ID genuine and unaltered? These tools check security features, read the barcode and machine-readable zone, and compare encoded data to the printed front against a template library of document types. None (yet) provide a full forensic view of this data to end users.
2. **Liveness.** Is a real person, and a real document, physically present? Not a screen, a photocopy, a replayed video, or an injected deepfake. Where there is a synthetic face or ID, the liveness check is the most important initial check.
3. **Face match.** Does the selfie match the one pictured on the ID? This is a 1:1 biometric comparison of a selfie to the document portrait.

Fraud in any one of these three is identity fraud. Two things get faked. **The person:** an impostor holding a real ID, a proxy in the interview, a live face swap or AI avatar (Palo Alto Networks built one in about 70 minutes with no prior skill), or a different person showing up after hire. **The document:** a genuine ID with the wrong holder, a genuine ID altered, a counterfeit, or a wholly synthetic identity. None of these shows up in a records check.

3. Three layers that work together

Person and document (Janice Kephart, ZipID). Document authentication, liveness, and face match bind the human to the credential. This is the step that defeats impostors, proxies, deepfakes, and altered or counterfeit IDs.

Direct-source validation (Chuck Salvia, Salvia Consulting). With applicant consent, SSA's Consent Based SSN Verification (CBSV) confirms whether name, SSN, and date of birth match SSA records and flags a death indicator. IRS IVES returns income and employment transcripts directly from the IRS. In case data Chuck presented, 10 of 79 credit union applicants (12.7%) and 17 of 93 university contractors (18%) failed identity validation. Across tens of thousands of CBSV transactions over 16-plus years, Salvia Consulting found 7.5% to 8.8% returned a "No Match," depending on customer population and industry. A No Match is not proof of fraud, but it shows that locating records is not validating identity. An SSN trace helps you find records. CBSV helps you validate the identity behind them.

Verified identity data at intake (Janice Kephart, ZipID). Once the person is bound to a genuine document, the name and date of birth read from that verified document, not what the applicant typed, should drive every search that follows. A nickname, maiden name, or transposed birth date can send a criminal search down the wrong path. Capturing data from the verified ID before the first search runs gives the screener, and the employer's I-9, a clean, auditable identity anchor.

Not all biometrics are equal. The strength of that anchor depends on the face matching algorithm underneath it. Error rates in NIST testing differ by orders of magnitude between the top-ranked algorithms and those further down the list, and the gap is widest in real hiring conditions: phone cameras, poor lighting, older ID photos, and a diverse applicant pool. A product marketed as "biometric verification" but built on a lower-tier engine passes more impostors and stops more lawful applicants. Before putting its name on a result, a screener should know whose algorithm produced it.

4. Where to verify: the Form I-9

Every employer must complete an I-9 for every hire. Federal regulation (8 CFR 274a.2) already requires the employer to determine that documents reasonably appear to be genuine and relate to the person presenting

them. Most employers have no reliable means to do that by eye.

Building identity verification into the I-9 turns an existing obligation into the strongest trust signal in the hiring process. Done right, that means document authentication, liveness, and face match completed before Section 2; autofill only where the law permits; and the result and audit trail captured automatically. For screeners, it is an employer obligation, not a consumer report, which is how identity verification can complete a background check without adding a new FCRA question. Confirm how this applies to your program with your own counsel. Identity risk also does not end at hire. It should be re-evaluated at reverification, role changes, and access to sensitive environments.

5. Questions to ask any identity verification provider

At the conference we presented four questions on accuracy. Recent breaches make clear that accuracy is half the test. In September 2026, identity verification vendor IDScan.net confirmed a breach after more than 153 million driver's license records linked to it were offered for sale. The same month, the Department of War disclosed a months-long breach exposing unencrypted SSNs of about 3 million people, and the FBI confirmed a breach of its jobs portal. A provider that collects ID images, selfies, and SSNs is now holding the most valuable data in your workflow.

Accuracy and testing

1. **Are you NIST tested?** NIST's Face Recognition Technology Evaluation is the leading independent test of face matching algorithms. Being tested is not the same as performing well: ask for the specific submission and where it ranks. "Accurate" is not an answer.
2. **Whose algorithm is it?** Most platforms license someone else's, and some license lower-cost engines that rank well down the NIST results. Ask whose algorithm it is, which version, and when it was last updated, then look it up on the NIST site. A vendor that will not name its engine is telling you something.
3. **What are the published error rates?** Ask for the false match rate and false non-match rate at the threshold they actually run, and how performance varies across age, sex, and skin tone in NIST's demographic results.
4. **What happens when it goes wrong?** A false match passes a fraudulent hire. A false non-match can block a lawful worker and invite a discrimination claim. Ask how failures get human review.
5. **How is liveness tested?** Ask for independent presentation attack detection results (for example, iBeta testing to ISO/IEC 30107-3) and what the platform does about injection attacks, where a deepfake is fed into the camera stream rather than held up to it.

Security of the platform

6. **What independent security attestations do you hold, and what do they cover?** Ask for a current SOC 2 Type II report or ISO/IEC 27001 certificate, the scope of each, the date of the last third-party penetration test, and whether ID images and biometric data are encrypted at rest and in transit and segregated by customer.
7. **If you were breached tomorrow, what would an attacker get?** Ask exactly what is stored (raw ID images, selfies, face templates, extracted PII), where it is hosted, which subprocessors and offshore staff can access it, how access is logged, and how fast you would be notified.

Privacy and protection of the PII itself

8. **How do you limit collection and use?** Ask whether the provider collects only what verification requires, obtains and records applicant consent and notice, never sells or reuses the data, and does not train its models on your applicants' images without permission. Ask how it handles state biometric privacy laws such as those in Illinois, Texas, and Washington.

Retention

9. **How long do you keep it, and who decides?** Ask for the default retention period for images, templates, and extracted data; whether you can set it to match your clients' own records schedule (I-9 records follow their own federal retention rule); and whether deletion is automatic and certified. Data that is not kept cannot be breached. The IDScan reporting raised exactly this issue, with at least one customer saying it had never authorized the vendor to retain data from its accounts.

If a provider cannot name a test, a number, a certification, and a deletion date, that is your answer.

Key takeaways

- Hiring is now an identity assurance problem, and screeners are the first line of defense. Records, source data, and biometrics each answer a different question.
- Bind the person to the document with an ID authentication tool and a face biometric, not one or the other.
- The I-9 is the natural, already-required place to do it.
- Vet providers on security, privacy, and retention as hard as on accuracy.

About the authors

Janice Kephart is Founder and CEO of ZipID, Inc., a biometric Form I-9 compliance and identity verification platform. She served as Border Counsel to the 9/11 Commission and as Senate Judiciary Committee counsel, drafting the *Identity Theft and Assumption Deterrence Act*. She is an author of REAL ID and the biometric border entry-exit mandate, has testified before Congress 19 times, and is a former Homeland Security Director at MorphoTrak and former director of the federal Biometric Interagency Working Group. janicek@zipidapp.com

Chuck Salvia is Founder and Owner of Salvia Consulting, providing instant IRS employment verification (IVES), and SSA Consent Based SSN Verification (CBSV) services. He spent nearly ten years as COO of IDValidation, which he built from a start-up to include SSA's CBSV service along with the forerunner to IVES which is the IRS Form 4506-C service. From 2013 to 2016 he chaired the Government Identity Verifications, Exclusions & Sanctions sub-committee of the National Association of Professional Background Screeners (now PBSA). Chuck@SalviaConsulting.com

Sources: Gartner (2026); Pindrop Security; Entrust Identity Fraud Report 2026; Palo Alto Networks; GAO; IRS/TIGTA; U.S. Department of Justice; Salvia Consulting case data; NIST Face Recognition Technology Evaluation; September 2026 breach reporting by KrebsOnSecurity, Help Net Security, Military Times, ABC News, TechCrunch and The Register.

For educational purposes only; not legal advice. Reflects the authors' views, not PBSA's, and is not reviewed or endorsed by PBSA. Consult your own counsel on FCRA, I-9, and privacy obligations.