# Digital Identity Verification Evaluation Checklist

When evaluating vendors, it's important to ask the right questions. Financial institutions, insurance companies, healthcare providers and government agencies should look for answers that demonstrate that a provider can deliver the functionality required, while also helping to prevent application fraud.

## Key Questions to Ask When Evaluating Digital Identity Verification Solutions

### QUESTIONS ON VERIFICATION METHODS

1. Does the solution allow for the following verification methods?

| | | | |
|---|---|---|---|
| Identity document capture | ☐ | One-time passcode (OTP) | ☐ |
| Identity document verification | ☐ | Knowledge-based authentication (KBA) | ☐ |
| Facial comparison | ☐ | Trusted identity networks | ☐ |
| Liveness detection | ☐ | | |

2. Can different verification technologies be used for different transactions? ☐
3. Can multiple identity methods can be used together to help meet Know-Your-Customer (KYC) compliance requirements? ☐

### QUESTIONS ON VERIFICATION CAPABILITIES, ORCHESTRATION AND COVERAGE

1. Does the solution support the orchestration of identity verification with a single API integration that offers the flexibility to optimize the process with minimal impact? ☐
2. Is the solution scalable? ☐
3. Does the solution cover all identity documents required for your customers and/or region? ☐
4. Does the solution offer name/fuzzy matching capabilities to account for any variance between the Machine-Readable Zone (MRZ) and Visual Inspection Zone (VIZ) on an identity document? ☐
5. Does your solution support varying levels of identity assurance (i.e. LOA-3 and above)? ☐

| QUESTIONS ON KEY PERFORMANCE INDICATORS | |
|---|---|
| 1. Are your average response times for each type of verification method under the industry benchmark of 15 seconds? | ☐ |
| 2. Are error rates (false positives or false negatives) generally under the 5% industry benchmark? | ☐ |
| 3. Do you have a guaranteed SLA for response times? | ☐ |
| 4. Is there provision for service resilience if one of more identity verification method is unavailable? | ☐ |

| QUESTIONS ON DATA PRIVACY AND AUDIT TRAILS | |
|---|---|
| 1. Is the solution provider able to give you a clear indication of what happens to the identity data once captured and how data is stored? | ☐ |
| 2. Does the solution provide a comprehensive audit trail? | ☐ |

| QUESTIONS ON USER EXPERIENCE AND WORKFLOW | |
|---|---|
| 1. Is the solution fully automated, or does it use a mix of automated and manual verification? | ☐ |
| 2. Can the solution support e-signatures? | ☐ |
| 3. Does the vendor offer downstream authentication and fraud detection capabilities to support the entire digital identity lifecycle – pre- and post-onboarding? | ☐ |
| 4. Can the solution be white-labeled? | ☐ |
| 5. Does the solution offer a mobile optimized UX? | ☐ |

## About OneSpan

OneSpan helps protect the world from digital fraud by establishing trust in people's identities, the devices they use and the transactions they carry out. We do this by making digital banking accessible, secure, easy and valuable. OneSpan's Trusted Identity platform and security solutions significantly reduce digital transaction fraud and enable regulatory compliance for more than 10,000 customers, including over half of the top 100 global banks. Whether through automating agreements, detecting fraud or securing financial transactions, OneSpan helps reduce costs and accelerate customer acquisition while improving the user experience. Learn more at **OneSpan.com**.

**SOCIAL MEDIA**