

LexisNexis® Risk Solutions IDVerse® Pricing Document

G-Cloud 15 Framework



LexisNexis®
RISK SOLUTIONS

Contact:
LexisNexis Risk Solutions
Global Reach, Dunleavy Drive
Cardiff, CF11 0SN
Office: 029 2067 8555
Email: ukigcloudenquiry@lexisnexisrisk.com

This proposal includes data that shall not be disclosed outside your organisation or any other department necessary to process an order, and shall not be duplicated, used, or disclosed, in whole or in part, for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offeror as a result of, or in connection with, the submission of this data, your organisation shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. The entire proposal shall be subject to the restrictions contained herein. In addition, this data is exempt from disclosure pursuant to the Freedom of Information Act, 5 U.S.C. 522(b)(3) and (4). LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. © 2026 LexisNexis Risk Solutions. Other products or brands referenced within this response are trademarks of RELX Inc., its subsidiaries or affiliates.

Table of Contents

IDVerse®	3
How would this work?	4
Pricing	6

IDVerse®

IDVerse® is a cutting-edge document authentication and biometric verification solution that will help you confidently approve trusted transactions while detecting deepfakes and forged documents. Powered by state-of-the-art, proprietary AI models and a deep neural network, IDVerse delivers fully automated authentication of ID documents and verification of ID holders' identities within seconds.



-  Balance security and compliance with seamless user experience with a quick, efficient and secure onboarding process.
-  Reliably lock fraudsters out of your systems by leveraging *good* AI in the fight against *bad* AI.
-  Drive efficiency and profitability by automatically adapting to dynamic, ever-changing identity fraud threats at scale.

Harness the Power of AI Against Deepfakes & Fraudulent Documents. *To outpace identity fraud and deepfakes, and reliably automate authentication of ID documents and verification of ID holders' identities, IDVerse leverages artificial intelligence and advanced face matching capabilities.*

IDVerse® uses advanced AI-driven technology to authenticate documents and facial biometrics to detect liveness, helping prevent fraud and ensure compliance – all in a fully automated process. IDVerse provides an AI-powered identity verification solution that instantly authenticates identity documents, matches consumers' faces to their ID photos, and detects fraud attempts in real time. Supporting up to 16,000 types of identity documents worldwide, the IDVerse solution enables secure, efficient and compliant identity verification across industries.

Our next-generation engine technology, Doc 5 and Liveness 5, represents a major leap forward in document processing and biometric verification. These engines are designed to deliver exceptional accuracy, speed, and user experience across a variety of platforms. With Doc 5, we've redefined how physical ID documents are captured and processed, using advanced AI, real-time frame analysis, and enhanced error reduction to ensure reliable, high-quality data extraction. Liveness 5 introduces cutting-edge facial recognition technology, eliminating the need for rigid positioning while maintaining robust security and ease of use.



Key IDVerse Features & Differentiators. *Our IDVerse solution enables more holistic identity verification and stronger fraud detection, with minimal friction for legitimate customers.*

IDVerse helps detect fake users and flags attacks from manipulated media and generative AI. Its face matching technology enable consent-based selfie matching against an identity using smart devices, ensuring the person is present, authentic, and not an AI-generated deepfake.

Unlike rules-based systems, IDVerse continuously learns and adapts to emerging fraud tactics, as well as changes to smartphones and their capabilities. It proactively identifies and flags fraudulent submissions, including known deviations from expected inputs such as the image quality of the latest smartphone. Deep neural network technology helps ensure industry-leading verification accuracy.

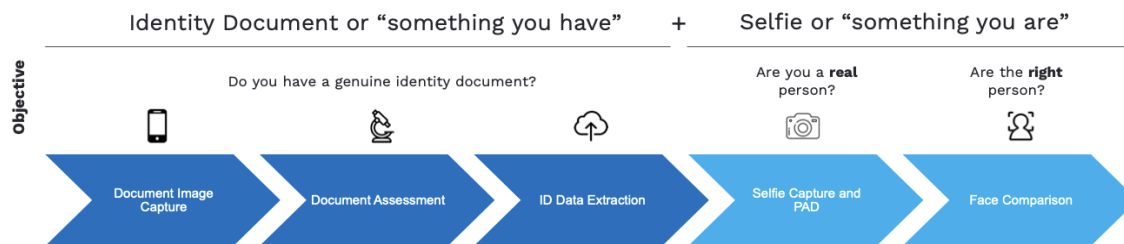
How would this work?

Your organisation would trigger an IDV via our platform or API and using their smartphone the individual follows a very simple process:

- Review and give privacy consent.
- Capture their identity document.
- Review the extracted personal information.
- Capture a short liveness video / selfie.

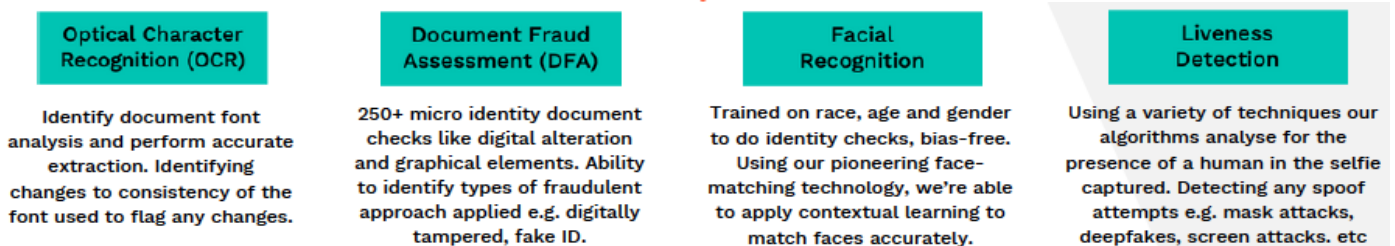
Our UI acts as an orchestration layer with embedded flexible and adaptive decision logic that will allow a client to easily design and maintain dynamic user journeys for identity management. The UI is Web Content Accessibility Guidelines (WCAG) 2.0 compliant with visual and voice instruction (changeable voices and multilingual support). Our CX is intuitive and accessible for the customer to allow for a natural onboarding experience, with precision protection.

Five key steps in AI IDV



1. **Document Capture:** our engines ensure we capture the best photo of the identity document.
2. **Document Fraud Analysis:** verifies the evidence is a real physical identity document and not a photocopy or off a screen; is valid and the visible security features are genuine, whilst detecting fraudulent attempts, e.g., through fake, tampered, or synthetic IDs.
3. **ID Data Extraction:** personal information from the ID document is extracted using the OCR engine.
4. **Liveness:** asked the user to take a short selfie video that confirms they are a live person and the IDV is happening in real-time (i.e., that they are not a pre-recorded video or image, not wearing a mask etc.).
5. **Biometric Face Matching:** using the face matching engine to ensure that the live and present person is the same person shown on the trusted identity document.

Our Four Core Engines



Pricing

LexisNexis Risk Solutions is pleased to provide the following pricing for G-Cloud 15.

One-Time Service Add-on Fees	
Amazon Web Services (AWS) Instance	£6,250 per additional AWS Instance
Channels	£1,250 per additional channel / per instance
Flows	£1,250 per additional channel / per instance
Single Sign-on (SSO)	£1,250 per additional AWS Instance
URL masking	£1,250 per additional AWS Instance
Additional Professional Service Fees	Determined by project scoping for bespoke deployments
SMTP Email Configuration	£3,375 for 2 days
mTLS Encryption	£8,438 for 5 days

Transactional Fees notes:

Minimum monthly commit of £650

If workflow requires SMS to initiate document capture, SMS costs to be added to per transaction (£0.09)

20% Support & Maintenance fee to be calculated from transactions volume pricing

Base Service	List Price	Committed Monthly Volume Tiers					
		10000	15000	25000	50000	100000	250000
Doc Only	£0.24	£0.22	£0.20	£0.18	£0.16	£0.15	£0.14
Single Doc Flow	£0.48	£0.47	£0.45	£0.43	£0.37	£0.31	£0.25
Multi-Doc Flow (for each additional document, in addition to Single Doc Flow)	£0.24	£0.22	£0.20	£0.18	£0.16	£0.14	£0.13
Multi-Check Flow (in addition to Single Doc Flow)	£0.24	£0.22	£0.20	£0.18	£0.16	£0.14	£0.13
Additional SMS	£0.09						
Single Doc Flow and Multi-Doc Flow Add-ons:							
UK Digital Right to Work	£0.53	£0.00	£0.00	£0.00	£0.00	£0.00	£0.00
FraudHub	£0.06	£0.06	£0.05	£0.05	£0.04	£0.04	£0.03
FraudHub and Blocklist	£0.11	£0.09	£0.09	£0.09	£0.07	£0.06	£0.05
Face Access	£0.12	£0.10	£0.10	£0.10	£0.08	£0.07	£0.06
Proof of Address	£0.13	£0.11	£0.09	£0.09	£0.08	£0.06	£0.05

Please note that there are bespoke product terms applicable to the solution in addition to the Call-off form.

What isn't included in the price: Any material enhancements or new functionality added to the product during the term of the contract (unless otherwise agreed in writing).

