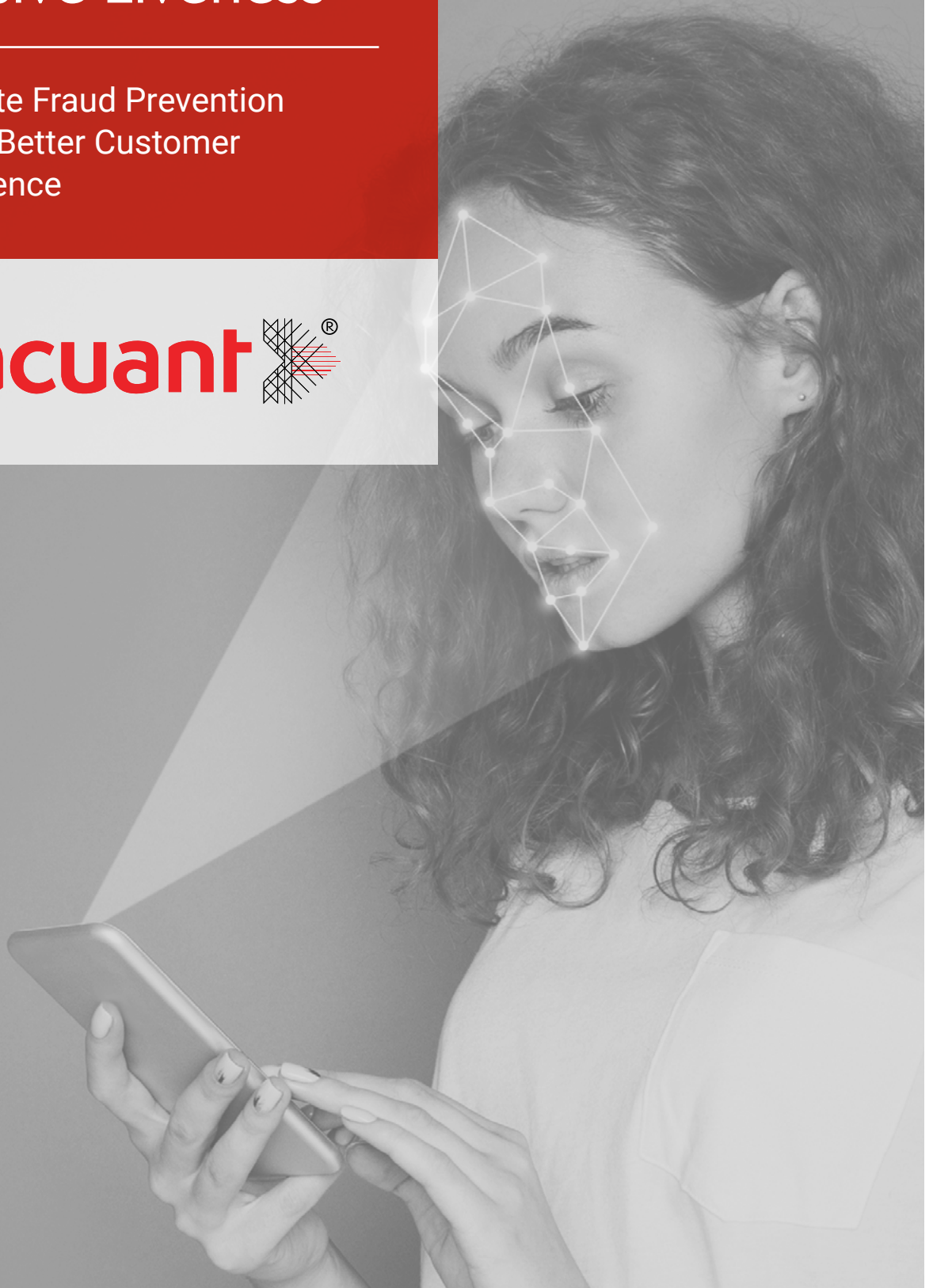


Facial Recognition Match with Passive Liveness

Ultimate Fraud Prevention
with a Better Customer
Experience

acuant 



INTRODUCTION

Document Authentication is an important first step to reducing fraud. It allows businesses to accept and verify government identity documents to help determine who a business is working with. However, in the online world, where private information and documents end up on the dark web for use by fraudsters around the world, how do you ensure that the person who presented the document is the person on the document?

Facial Recognition Match can offer robust fraud prevention, but it must include a liveness test. A liveness test ensures that there is a real person present instead of a photo, video playback or even a mask. We will explain why Passive Liveness is key to anti-spoofing and providing a frictionless customer experience.

Why A Liveness Test is Critical	1
How Single Frame Passive Liveness Works	2
Benefits of the Single Frame Approach	3
Machine Learning Is Key to Effective Liveness Detection	4
Acuant FaceID with Passive Liveness	5

WHY A LIVENESS TEST IS CRITICAL

Facial Recognition Match using One-to-One facial recognition technology matches a person's selfie with the image on their presented ID. This is very different than surveillance.

Employing a liveness test is critical in preventing spoofs, known as Presentation Attacks, such as photos from passing as the real person during facial recognition matching. Common Presentation Attacks include printed photographs, cut-out photos, screen displays, video replay and masks. Until now most systems used some form of active liveness, such as blinking, smiling or moving a head back and forth to detect liveness, assuming that a photo cannot mimic the actions of a live person. However, active liveness tests create friction, take time, and inform fraudsters of the steps necessary to break the system. In fact, many are now easily broken.

Passive liveness on the other hand, eliminates these concerns, requiring no additional steps from the user. However, like active solutions, some passive liveness solutions capture video or multiple images during the "selfie" process to detect subtle changes that indicate liveness. These solutions create more processing needs and more data transmission requirements on the device or to a server. Passive liveness detection uses only a single frame to accurately determine liveness, which results in faster processing speed, more robust spoof proofing and a better customer experience.

One-to-One

Verifies an individual identity by comparing a target image with data held on file to confirm a match. A person knows that the facial recognition match is being done and consents. And with Acuant, you know that data and images are encrypted and never stored to protect Personally Identifiable Information (PII).

One-to-Many

Compares a target image with a database of subjects of interest. A person might be identified in a public setting and it does not have to involve consent or knowledge.

HOW SINGLE FRAME PASSIVE LIVENESS WORKS

Single frame passive facial liveness works by examining a single image to make a liveness determination. It works with images taken from most any smartphone or web camera and does not require special hardware or software for image collection. The passive liveness algorithm is trained to work on images that meet minimum requirements to support broad use cases. Most face biometric systems determine matching based on a selfie; these systems already ensure the capture of a quality image that includes a forward-looking face at an acceptable resolution. If the selfie is good enough for the face recognition technology, it is good enough for the passive liveness check.

Passive liveness processes the selfie image via Computer Vision Machine Learning (CVML). There are three main parts to the algorithm: face detection, quality engine and liveness engine. The face detect engine uses 68 focal points to ensure that the image represents a single person and rejects images with multiple people. The quality engine gauges facial position for good analysis, measuring roll, yaw, pitch and angle of the face. Machine Learning examines a wide variety of image elements to help distinguish between a photo of a live person and a Presentation Attack. The software fuses the output of these analyses to produce a liveness score between 0 and 100. With the score, a liveness assessment - Live, Not Live or Poor Quality – is also presented.

Passive Liveness Detection Process



User takes a selfie



Selfie image is used by the facial recognition system to determine a match



The same selfie image is used for the liveness check



Proprietary algorithms analyze the image for liveness



The system returns a liveness score

HOW SINGLE FRAME PASSIVE LIVENESS WORKS

A Single Frame Approach Offers Advantages for Both Users and Developers

1

It does not require movements, gestures, nor extra video frames in order to recognize the user as a live person. The technology works passively in the background when a selfie is captured for facial recognition, keeping the user experience as simple and fast as possible. The user's only required action is to capture a selfie.

2

The developer uses the same frame for liveness checking as for face matching.

3

A single frame solution is deployed as a separate independent function, requiring no changes to the user or communication interfaces. Your back-end application simply performs one liveness check API call. This makes integration quick and straightforward for developers.

4

A single frame solution is imperceptible to users without indication of when it is happening or what it is looking for. This means that fraudsters will not get any heads up or clues on how to beat it.

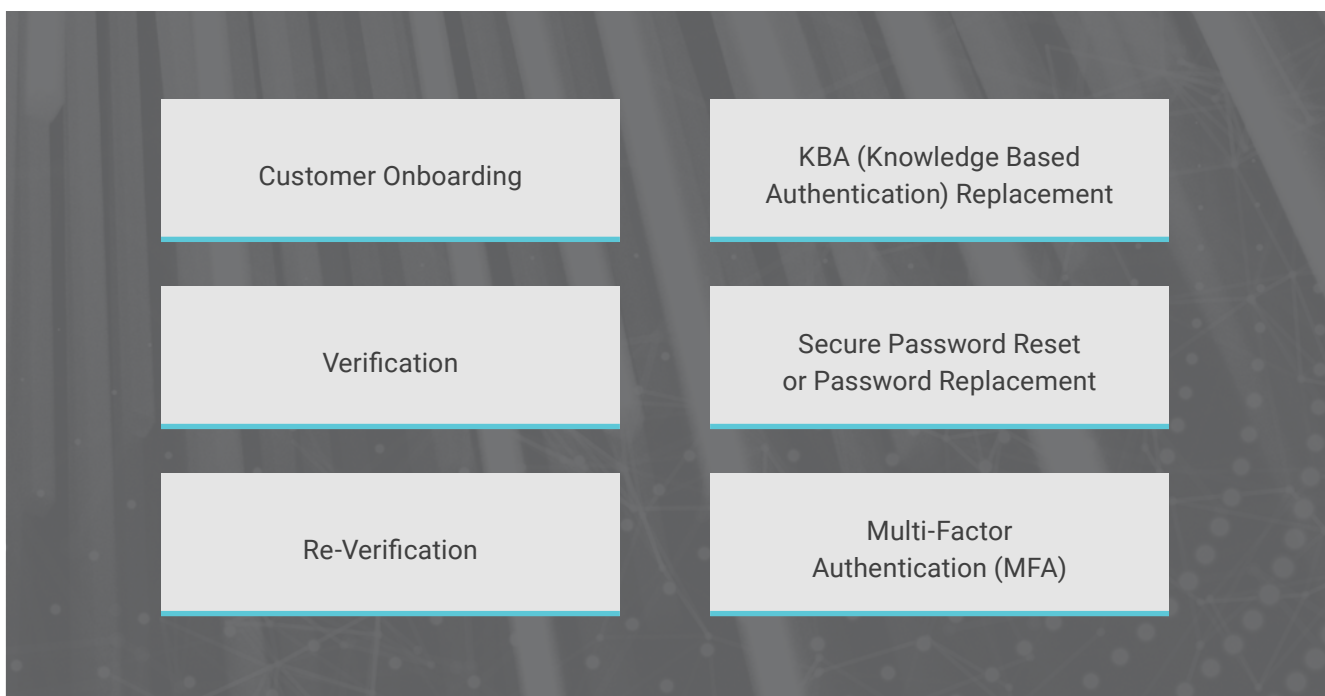
5

Finally, the single frame approach minimizes the amount of data that needs to be sent from the device. A single image can be as small as 50kb versus solutions that send multiple frames or videos of photos. And, if you are already sending the image to the back-end, there is zero extra data transmission overhead. The result is an easier, faster, more secure and less costly liveness solution.

MACHINE LEARNING IS KEY TO EFFECTIVE LIVENESS DETECTION

A human reviewer cannot quickly determine which images or deepfake videos are real. Only machine learning can recognize synthetically produced images at scale, as it far outperforms humans in tasks that are repetitive or require the examination of minute detail. This is true in the case of determining liveness in selfie images. However, the effectiveness of machine learning depends on training the system with large quantities of labeled real and spoofed image data, allowing the system to understand what makes a real live image and what makes a spoofed image. That same system can now run against data it has never seen before. This new data provides a test of how good the system is. Acuant constantly adds new data, helping the machine learning system increase its accuracy over time.

Use Cases



The top section of the page features a background image of a woman's face on the left, partially obscured by a white beam of light from a projector. On the right, there is a profile view of a woman's face. A large red rectangular box is centered in the upper half, containing the title in white text.

ACUANT FACEID WITH PASSIVE LIVENESS

Acuant FaceID offers passive liveness that was awarded Presentation Attack Detection (PAD) Level 1 and Level 2 Compliance by iBeta, an independent third-party tester, in accordance with the ISO/IEC 30107-3 standards. It passed iBeta Quality Assurance PAD testing with a perfect score. Algorithms are also NIST tested to be best-in-class offering you ultimate fraud prevention.

WHY CHOOSE ACUANT

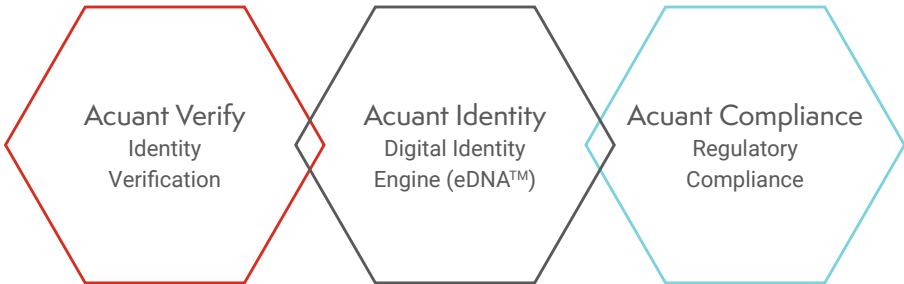
We provide options based on your use case, level of risk, deployment timeline, IT resources and compliance needs - contact us to learn more about which option is right for you.

Access our entire Trusted Identity Platform for all your identity verification and AML/KYC compliance needs - all with one API via our orchestration layer.

Our tech is privacy minded. Data and images are encrypted, never stored and validated using tokens.

Solutions are omnichannel, supported in iOS, Android and HTML - deployable on smart devices, desktops and kiosks.

We enable easy API integration, custom mobile apps and have developer friendly SDKs.

A diagram consisting of three overlapping hexagons. The leftmost hexagon is red and contains the text 'Acuant Verify Identity Verification'. The middle hexagon is black and contains the text 'Acuant Identity Digital Identity Engine (eDNA™)'. The rightmost hexagon is light blue and contains the text 'Acuant Compliance Regulatory Compliance'.

Acuant Verify
Identity
Verification

Acuant Identity
Digital Identity
Engine (eDNA™)

Acuant Compliance
Regulatory
Compliance



About Acuant

Acuant's Trusted Identity Platform powers trust for all industries with automated identity verification, regulatory compliance (AML/KYC) and digital identity solutions. Omnichannel deployment offers seamless customer experiences to fight fraud and establish trust from any location in seconds. Patented technology is powered by AI to deliver unparalleled results and efficiency in real time. With leading partners in every major industry and completing more than 1 Billion transactions in over 200 countries and territories, Acuant is the leader in global coverage.

HEADQUARTERS | **LOS ANGELES, CA**

MANCHESTER, NH

TEL AVIV, ISRAEL

PALO ALTO, CA

BRUSSELS, BELGIUM

SPOKANE, WA

MEXICO CITY, MX