Biometrics Under Attack:

Lessons from Building Stable Identity Verification

Q&A session

Please note that the questions have not been edited: they appear exactly as they did in the chat.

Question 1

How do you test deepfakes?

Answer

We create them. Seriously, we generate deepfakes ourselves and feed them into our system as part of internal testing plus use those which we get from public resources. We include deepfakes in our internal testing pipelines and simulating real-world scenarios like face-swaps, lip-syncs, and synthetic personas. Our team closely monitors fraud trends, including tools and techniques shared in open communities, to ensure we’re testing against what attackers are actually using. When our models show weaknesses, we go back and improve them.

Question 2

How fast can you respond to a new spoofing technique?

Answer

One of the key advantages of having our own internal lab and a tightly integrated R&D loop is the ability to move quickly. Once a new spoofing method is identified, whether it’s a novel 3D mask, a screen replay variant, or an AI-generated face, we first replicate and validate it in our lab under controlled conditions. If it’s effective, we use that data to retrain and harden our models. In many cases, especially if the infrastructure is already modular and the model is retrainable, we can deliver an improvement within days or weeks. This includes white-box testing, live simulation, and QA.

Question 3

How do you ensure Responsible AI and privacy compliance while using real world data for training your models?

Answer

All our solutions are delivered on-premises or in private environments, which means we never have access to customer data by design.

This presents a unique challenge when it comes to training AI models, but it's one we've solved through our internal R&D lab. Instead of relying on customer data, we generate and curate our own diverse datasets in-house. This includes extensive testing against a wide variety of real-world scenarios, but always in a controlled and privacy-compliant way.

Our lab replicates complex edge cases, creates synthetic and adversarial data, and constantly evolves our datasets based on observed attack trends - all without compromising any user privacy. This approach not only aligns with global privacy regulations, but also ensures our AI systems are reliable, explainable, and ethically trained.

Question 4

What happens if liveness fails? can we set up fallback logic?

Answer

Yes, absolutely. The system is modular, so each step - document check, liveness, face matching, age estimation, works independently and exposes its result and confidence level.
If a component fails or returns low confidence, you can configure fallback logic:

- Skip to a secondary method (e.g. active liveness if passive fails)
- Trigger manual review
- Request document re-capture
- Or even branch the flow by risk level or region

We don’t hardcode any of that, the integration is API-first, and fallback logic is defined on the customer side. But we do provide best-practice recommendations based on our experience.

Question 5

How do you work with countries local biometric agency, for resident authentification?

Answer

We don’t run national ID systems ourselves, but our technology is often used by government agencies including border control and civil ID programs in over 80 countries.

When needed, we work with local partners and integrators to make sure everything meets the legal and technical requirements. Our role is to provide reliable building blocks like document checks and liveness that can support secure resident authentication.

Question 6

Could governments introduce restrictions on the use of artificial intelligence in the future?

Answer

Yes, and many already did it. Regulations like the EU AI Act are setting the tone for responsible AI development worldwide. But at the same time, AI is too deeply integrated into modern systems to be “contained” or rolled back. The key isn’t banning it - it’s making sure it’s used responsibly, with transparency and clear guardrails. AI is here to stay, and the focus is now on regulating how it’s built and applied, not if it should be used.

Question 7

How can a company incorporate regula?

Answer

Regula’s technology is delivered as SDKs and APIs, making it easy to integrate into both existing and newly built infrastructures. You can embed our modules, like document verification, biometric checks, or age estimation, directly into your identity verification flow using our API.

The platform is fully modular: some customers use the entire identity stack, while others start with just one component.

You can even test everything live on our demo portal before integration:
Regula Document Reader SDK
Regula Face SDK

Question 8

Hi, is “liveness” foolproof? How can we always stay ahead of fraudsters?

Answer

Unfortunately, nothing is truly foolproof, especially when it comes to fraud. It’s a constant race. As fraudsters develop new tricks, we have to stay one step ahead.

That’s why it’s not just about one technology. You need a combination of tools and business processes working together to validate users as thoroughly as possible. Liveness is a strong layer, but it works best as part of a bigger picture and that’s how we help our customers design their flows.

Question 9

What would be a good complimentary identification method for your solution? Do you consider multi-factor compound verification schemes?

Answer

Yes, definitely. Our SDK is built to be modular and flexible, so it can easily work alongside other verification methods. We don’t insist on using only our biometric check, in fact, many of our customers combine our components with other layers of security.

We fully support multi-factor and compound verification setups. The more layers you have - whether that’s biometrics, documents, behavior, or something else - the more resilient your system becomes. It’s all about building the right combination for your risk level and use case.

Question 10

Having worked at the border I have seen interesting results, usually negative, with a 40% success rate for passing through e-Gates that a human would never accept. Why is this?

Answer

That’s a really interesting observation, and unfortunately not uncommon. e-Gates often rely on tightly integrated systems, but the actual performance can vary widely depending on the biometric engine used, the quality of input data (like lighting, sensor resolution), and, importantly, the configuration and threshold settings.

In many cases, these systems are optimized more for speed than for security, which can result in higher false accept rates. Also, if the vendor behind the biometric system hasn’t properly tested their solution against a wide enough range of real-world edge cases (lighting conditions, aging, spoofing materials, ethnic variability), the accuracy drops significantly.

That’s exactly why at Regula we invest heavily in controlled lab testing and real-world attack simulation to ensure the system not only works under perfect conditions, but also under pressure.

Question 11

What is the highest percentage of surety can one get … will it ever be 100%?

Answer

We never want to say never, but realistically, 100% certainty is extremely unlikely.

It’s always a cat-and-mouse game between fraudsters and those trying to stop them. As attackers evolve and use better tools, we need to stay ahead with even better ones. That’s the nature of this space - it’s a constant war, and the goal is to minimize the risk as much as possible without compromising usability.

What really matters is building systems that are resilient, adaptable, and continuously improved. That’s where investment in testing, monitoring, and feedback loops, like the ones we have in our lab, makes the difference.

Question 12

How do you comply with personally identifiable information and data residency law of UAE? Do you have data center here or does your solution work on-premise?

Answer

We don’t store or process any biometric or document data on our side because Regula’s solutions are deployed on-premise or in a private cloud fully controlled by the customer. That means all sensitive data stays within the customer’s infrastructure and under their compliance framework, including local data residency regulations.

We don’t operate a SaaS model or centralized cloud service, our customers retain full ownership and control over the data.

Question 13

How often does the IBeta certification test happens? When you say that Regula has level 2 certification for PAD which includes deepfake detection, does this include the more recent sophisticated ways of deepfake generation?

Answer

There’s no fixed schedule for iBeta certification retesting unless it’s required by local regulations. In general, when we introduce a major improvement to our liveness technology, we go through the certification process again. What matters to us is that we maintain or exceed the quality level we achieved not just on paper, but in the real world.

Now, deepfakes are a tricky topic. iBeta PAD tests focus on presentation attacks, things like screens, masks, printed faces, which are how deepfakes are usually delivered in practice. So even if the fake is generated by advanced AI, it still has to be presented somehow, and that’s what PAD testing targets. So yes, our certification is very much relevant to real-world deepfake attempts.

Question 14

Can I use Regula biometrics without the whole stack?

Answer

Yes, you can because it’s modular. Some customers use the full stack, while others integrate selected components like document verification, passive liveness, or biometric verification. What sets Regula apart is the flexibility of our product configuration - all modules can be deployed independently or combined into an end-to-end identity verification workflow, depending on business needs, risk level, and existing infrastructure.

That said, we increasingly see a shift toward integrated identity flows, since fraud often happens in the gaps between disjointed systems.

Question 15

Can we run your biometrics on-prem?

Answer

Yes. Our biometric modules are designed to be deployed on-premises or in a private cloud fully under the customer's control. We don't offer a shared SaaS or public cloud solution and that's intentional. Many of our customers operate in regulated environments or require full control over data processing. That's why we provide the biometric SDKs and modules as Docker containers, ready for local deployment, whether that's on physical infrastructure or in your private cloud like AWS, Azure, or GCP.

Question 16

How much does it cost to get started?

Answer

We don’t publish pricing publicly, because it really depends on what exactly you need, our stack is modular, so some teams go for the full workflow, others only need document checks or liveness.
But we’re always happy to provide a tailored quote, just send us your use case.
That said, our pricing is definitely competitive. We develop all technologies in-house - so no licensing chains, no markup-heavy middleware. Even Gartner highlighted this in their latest Magic Quadrant report, noting that our pricing stands out because we control the full stack ourselves.
And if you’re just getting started, we also offer a free trial so you can explore the product before making a decision. Please contact us at kate.johnson@regulaforensics.com to get more details.

Thank you!

kate.johnson@regulaforensics.com

Regula

Decades of Forensics for Seamless Identity Verification.

Bringing together 34 years of experience in forensics, border control and business, to create industry standards to trust and follow.