This is a research preview. If you work in media and wish to know more and report about this, please get in touch here **Contact Us**

Deepfakes Vs Biometric Identity Verification

During the past year, we have worked on new research. We wondered how strong commercial biometrics KYC (Know Your Customer) solutions are to detect presentation and replay attacks with deepfakes like face morphing, face swap, and face reenactment. Today, this technology allows us to replicate anyone's face without a training dataset; one picture, such as the picture on the ID card, passport, or driver's license, is sufficient to create a real-time deepfake video. In the wrong hands, it can be a powerful weapon. For this reason, we tested 10 of the top identity verification providers. We found out that all of them, systematically, are vulnerable to spoofing by deepfakes.

But let's take a step back. When we say "identity verification solution" we are referring to software mostly used by banks, fintech, insurance, gambling, trading, crypto companies (and many others) to prove that their customers are who they say they are, and by that to comply with KYC/AML (Anti Money Laundering) regulations. Usually, a KYC solution is composed of 3 steps:

1. ID Authentication: the user presents their ID card to the camera and relevant information is extracted to verify whether the document is legit and compliant with national formats.
2. Face Matching: the user takes a selfie which will be matched automatically with the picture on the ID previously presented.
3. Liveness Check: the user performs a series of actions in order to prove that he/she is a real human being, and not a photo or a replayed video of someone else, or a person wearing a mask.

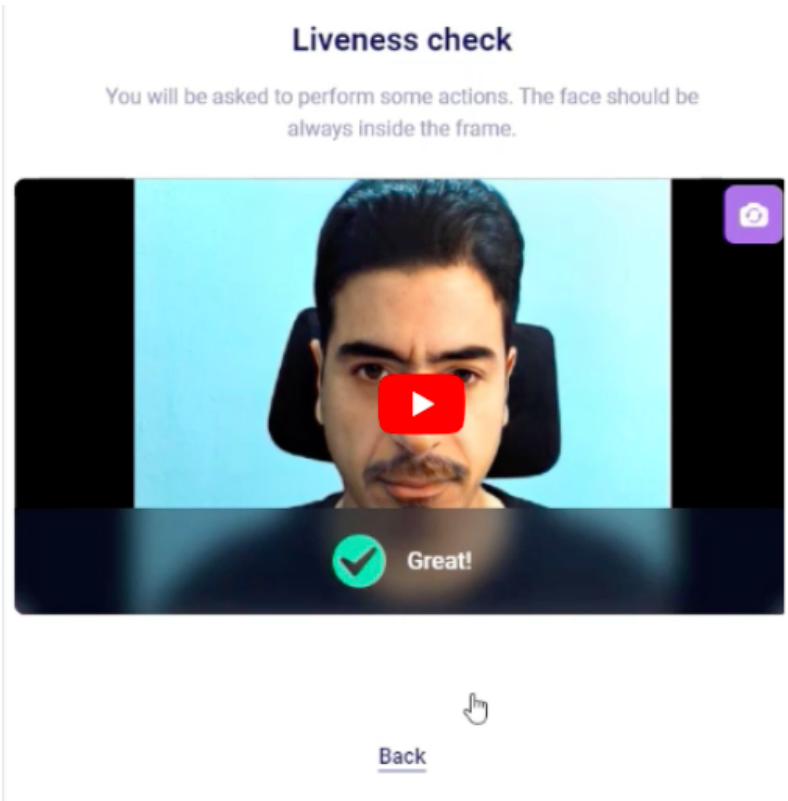
If no warning is triggered during this procedure, the user's identity is proven, and they can open a bank account, or start trading stocks, buying crypto, betting, etc.

Now that we have clarified this point, let's move on to the spoofing scenario.

Spoofing simulation scenario

I, as a fraudster, want to open a bank account or a crypto wallet online to launder money generated from illegal activities. First of all, I need to find an ID. One doesn't really need to use the darknet for that. There are plenty of forums online with databases containing tens of thousands of ID cards and passports obtained from data breaches. Most of their owners are unaware that their documents are online available to be purchased. Here, in addition, anyone can find guidelines on how to bypass two-factor authentication, get temporary phone numbers or temporary emails that look real, etc.

Now we have someone's driver's license and the knowledge to bypass the most basic onboarding security checks. Once we have filled a KYC form with all required information, we are asked to verify our identity through the process we described above. Since our driver's license is real we aren't worried about the ID authentication, which passes. For face matching and liveness we inject a real-time deepfake that hides our own face and instead use the face of the driver's license owner without raising any red flag, as you can see below. We passed all biometric checks. We are authorized to proceed, impersonating someone else.



As we mentioned in the beginning, we have penetrated 10 among the top identity verification providers installed worldwide in national banks, financial institutions, government services, telcos, crypto exchange platforms, etc. In April 2021 Chinese fraudsters managed to perform a 500 million yuan fraud (approximately USD 76.2 million) with a series of replay attacks, through deepfake videos, against the tax office identity verification system.

The threat of deepfakes attacks to biometric and identification systems is not hypothetical anymore. For this reason, Sensity has built a KYC identity verification solution able to detect in real-time deepfake spoofing attempts.

Sensity Team

This is a research preview. If you work in media and wish to know more and report about this, please get in touch here Contact Us