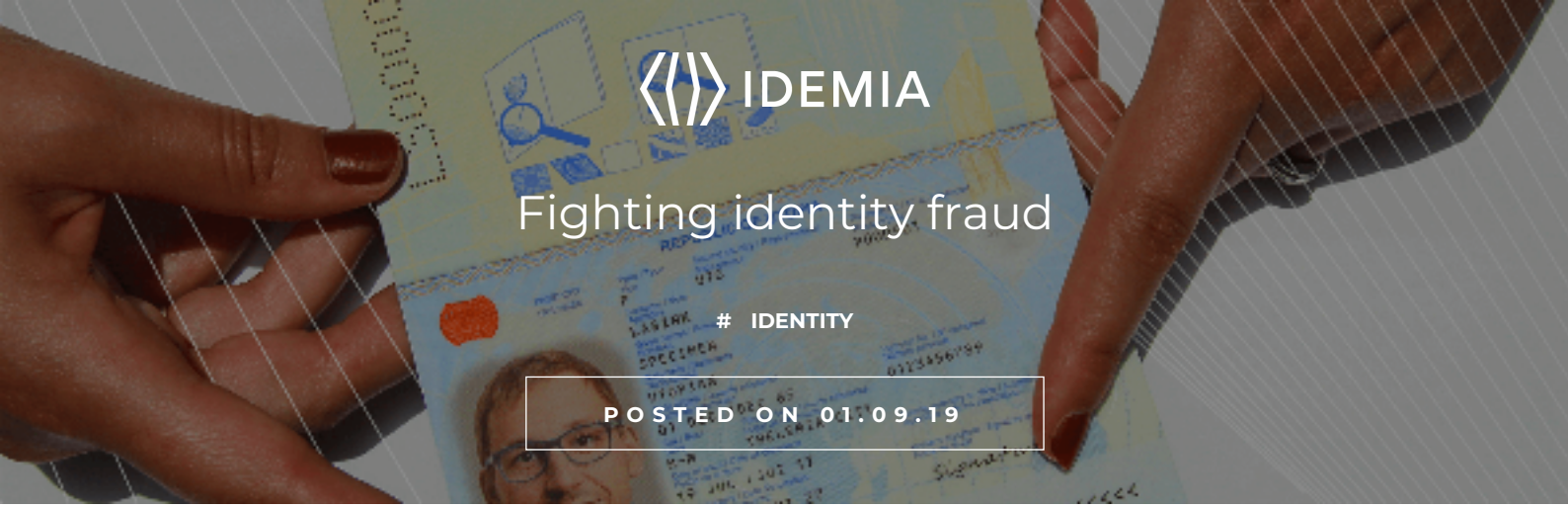

# Fighting identity fraud

# IDENTITY

POSTED ON 01.09.19

It's true, digitalization has disrupted the world as we know it – changing the way we pay, travel, have fun and identify ourselves. But let's not forget that at the start of every transaction, whether in the physical or digital space, is a reliable, fraud-resistant identity document. We sat down with Isabelle Poulard, VP Passport and Driver License at IDEMIA to take a closer look at how IDEMIA protects citizens' identities and combats fraudsters.

*At the start of every transaction, whether in the physical or digital space, is a reliable, fraud-resistant identity document. Understanding the new methods used by fraudsters is key to combating them and protecting citizens' identities.*

*Isabelle Poulard, VP Passport and Driver License at IDEMIA*

## How do fraudsters produce false identity documents? Are some methods more common than others?

Fraudsters rely on three main tricks to create fake identity documents. Counterfeiters create a completely new identity document, either from scratch or by integrating parts of genuine documents. We rarely see this type of **ID fraud** because the manufacturing process is far too complex and the fraudsters always take the path of least resistance. They usually find it easier to alter the personal data (photo, date of birth, name, etc.) on a lost or stolen document, this second type of fraud is called forgery. We call the third form of ID fraud "lookalike" fraud. In this case, imposters use a genuine ID document of someone with a physical resemblance. Lookalike fraud can become even more sophisticated if the imposter manages to apply for an official document using a morphed photo.

## What does forging a document involve?

Forgery applies on lost or stolen documents. The fraudster impersonates the rightful owners by changing the portrait of the document. If you've ever closely inspected your **identity card**, you've likely noticed multiple visual elements to protect the photo such as engraved textures or holograms partially covering the main portraits; secondary photos printed using other techniques, etc. They all contribute to the security of your document. To alter the portrait, forgers need to get past all these barriers – whether that means peeling back the top layer of an ID card or the data page of a passport, grinding down the back of the document in order to use the front on a new document or recovering the original photo by its own picture (using stickers, overlays...).

## How is IDEMIA working to combat forgery?

IDEMIA produces ID cards and **passport** data pages using polycarbonate, a material that cannot be split once the various plastic layers that constitute the document have been laminated. This material derails even the most industrious fraudsters from employing two of three forging methods. We further bolster document security with our latest innovation **LASINK™**, which allows the document holder's portrait to be engraved in color directly into the document. This patented technology combines the robustness of polycarbonate, the quality of a color picture and most importantly, a main portrait that is very difficult to copy and very easy to authenticate. LASINK™ can indeed be authenticated by police officers as well as by non-expert eyes – meaning bank or insurance officers, merchants, pharmacists or universities – with a simple tool or a mobile app. Alternatively, we add a secondary portrait, also embedded in the document itself such as our Stereo Laser Image (SLI®), which consists in a very sharp 3D photo. If a fraudster attempts to alter the primary photo, the SLI will no longer match the main portrait. If the fraudster tries to forge the SLI as well, it will be clearly visible even to the untrained eye, as the 3D effect either will disappear or be altered. In the end, we want identity documents that are easy to inspect yet hard to reproduce.

## You mentioned imposters using lookalike photos – can you explain how that works?

With advancements in **identity protection**, identity cards and passports are so well protected against counterfeiting and forgery that it sometimes proves easier for attackers to focus on "lookalike frauds". In general, the imposter will try to look like the photo on a stolen, yet genuine document. Fraudsters will often change their haircut, hair color or add glasses or a beard to deceive law enforcement. When we consider that photos on ID documents remain valid for several years, it makes spotting a fraud very difficult to the human eye.

## What is IDEMIA doing to stop these imposters?

For manual control, the prevention consists in personalizing advanced photo quality. We have done a lot of work on the subject and developed software that allows governments to improve the "readability" of the primary photo printed on the document by enhancing contrast and sharpness in order to ease the comparison between the photo and its owner.

Nevertheless, the best prevention against an imposter remains facial biometrics where a photo of the individual taken on the spot is compared to the picture on the document or in the chip of the biometric passport.

However, as I said, the fraud can become more sophisticated if a morphed photo is used to apply for an official document (passport, ID card, driver license) at the enrollment stage. Morphing consists in blending the digital image of two individuals, creating a hybrid image that looks like both original faces. This is particularly tricky because the synthetic image contains the characteristics of both individuals, thus the importance of a solid enrollment process.

## So what can be done to prevent morphing at the enrollment stage?

To further protect documents, we encourage governments to exercise the utmost vigilance in ensuring the authenticity of the evidence provided to them when issuing identity documents including the photo. The best way to counter face-morphing attempts is to ban print photos and capture live photos by an agent on the spot or through controlled and secured channels (accredited photographer or in a secure kiosk).

## As digital and technological advancements continue to change our world, the future of identity documents begins to take shape.

## How are things evolving from a security standpoint?

Security features clearly need to be adapted as the machine inspection of documents will become more commonplace. To that end, we have developed security features such as DocSeal, a signature of the user portrait and data, also printed on the document, that can be inspected by the camera of a simple smartphone and that enables to detect any modification of the user's personal data. The document as a physical object, issued by a government from a face-to-face enrolment, is also the perfect basis and tool for the creation of mobile identities. By **mobile identities**, we mean here identities that are dematerialized and stored into a mobile device to be used and inspected in the physical world. Protecting these mobile identities is as critical as protecting physical identity documents. This is why we are also developing security mechanisms to protect these mobile identities against cloning and usurpation and to uniquely link identities with the rightful owners and their smartphones.