FINGERPRINTS

DISPELLING BIOMETRIC MYTHS AND LEGENDS

Exposing the Achilles Heel of modern biometric misconceptions

– Fingerprint biometrics has achieved huge success in consumer applications like smartphones, payment cards and door locks.

However several myths and misconceptions surrounding biometrics remain today, that can limit the adoption.

It's time to set the record straight and show the true quality, security and functionality of modern solutions.

TABLE OF CONTENTS

BUSTING MYTHS

– A HERCULEAN TASK

FROM ORAL TRADITIONS and epic poems, right through to today's movie franchises, mankind has been captivated by myths for centuries. As technology has merged with myth, though, it can become hard to differentiate fact from fiction.

The TV, film and literary industries have created our own 21st century myths, in seeking to excite viewers and intrigue audiences, many of which relate to the subject of this paper: biometrics. Think spies lifting fingerprints from martini glasses to spoof.

In parallel, the limitations of early biometrics solutions remain in the mind of consumers. Now outdated, these misconceptions are unreflective of the quality and value of modern-day solutions.

While it's often simply a narrative technique, these prevailing myths and misconceptions can limit faith (and adoption!) of technologies that bring security and convenience to millions around the world.

The evolution in consumer biometrics in the last two decades has been phenomenal – one need only look at the rapid uptake of fingerprint sensors on smartphones. Now it's time to dispel some of the common biometric myths and showcase just how smart today's solutions really are.

BIOMETRICS REAL TALK

Before dealing with the misconceptions surrounding biometrics, let's quickly recap on some leading facts about their use today.

1 | Fingerprint has replaced PINs and passwords as the most popular way to authenticate on mobile

2 | 70% of smartphones shipped feature biometrics, and 82% of consumers that have access to biometrics on their mobile use it

3 | Biometrics is gaining traction in new consumer applications and form factors, as a means of secure and convenient authentication

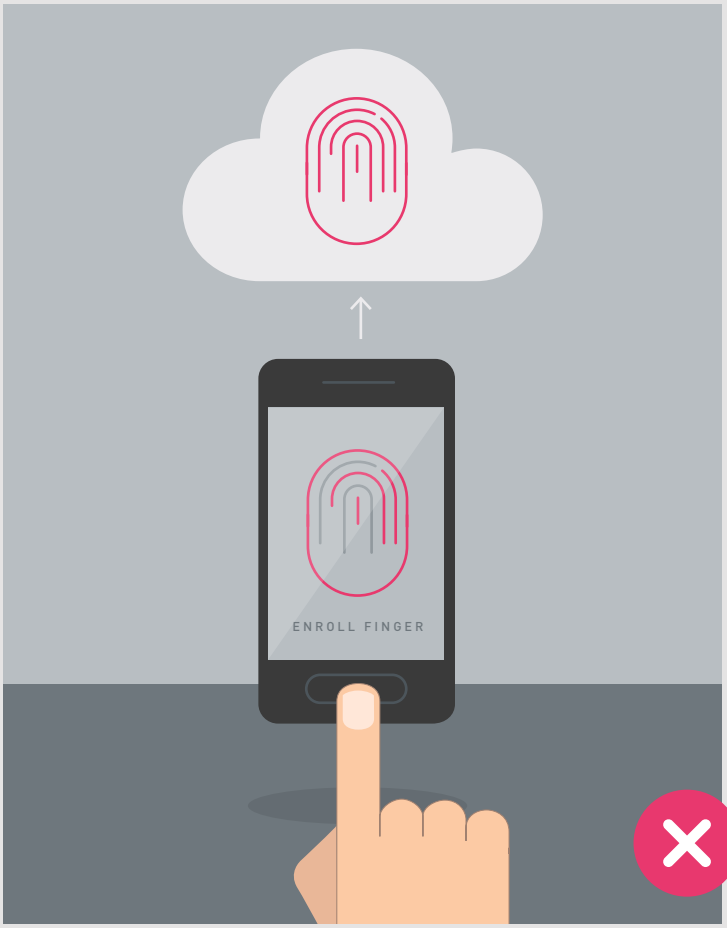
"The use of **biometrics** continues to grow beyond established use cases into new areas of daily life, **transforming how we pay, unlock and access our world.** But before the technology can reach its full potential however, we must **address some of the leading myths** and misconceptions and unpack the true value of using ourselves as the keys to our lives."

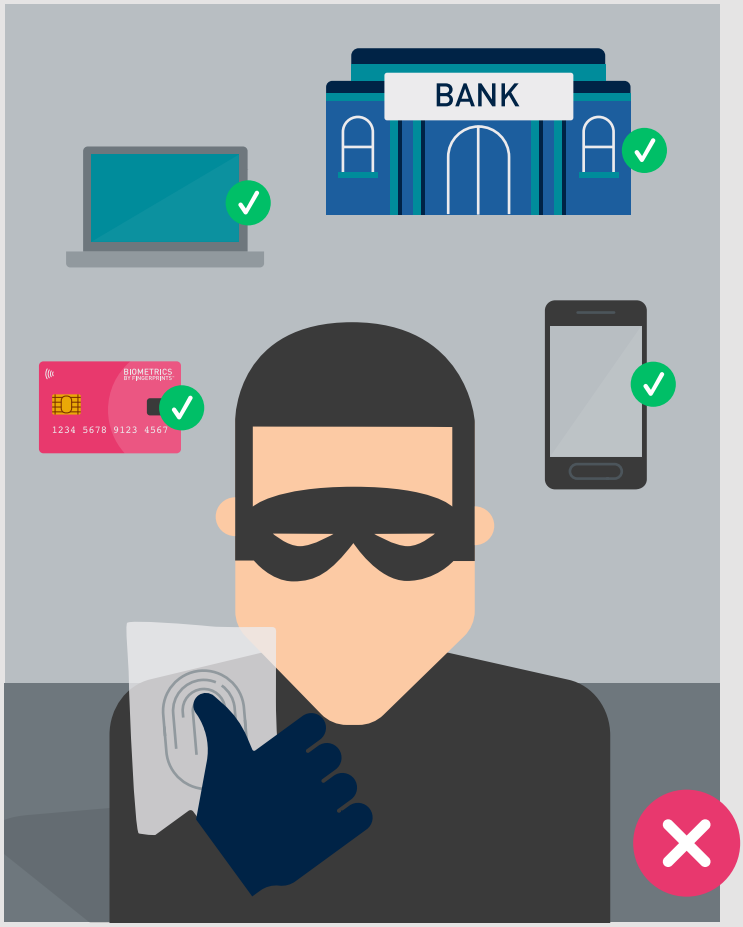
Christian Fredrikson, CEO at Fingerprints

MYTH 01

Biometric data is stored as images in easy-to-hack databases

if this is accessed, it is permanently compromised,
and cannot be restored.



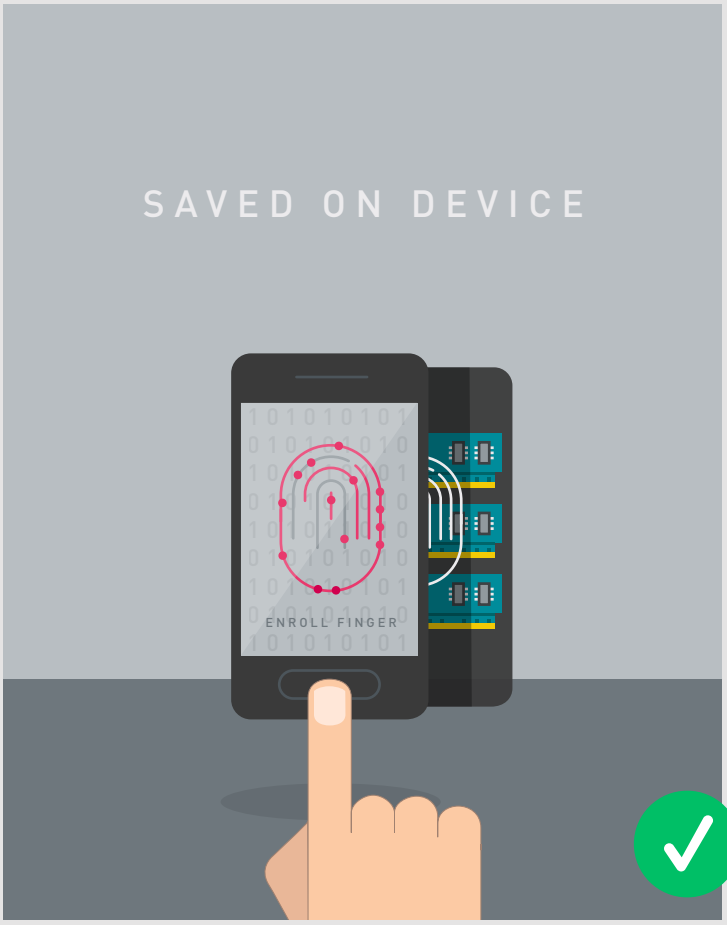


MYTH

When a biometric identifier is registered to a device, it is stored as an image in a database or cloud.

MYTH

Should that image or device get stolen, the user's biometric data is then irreversibly compromised across all applications.



TRUTH

Data captured from a biometric sensor is stored as a template in binary code – put simply, encrypted 0s and 1s. And is stored on the device, nowhere else.

TRUTH

Storing a mathematical representation, an encrypted template, rather than an image, which cannot be used or interpreted on any other device.

PANDORA'S BOX

For many, a leading myth about biometrics is that when a biometric identifier is registered to a device, it is then stored as an image. Should that image be stolen, the user's biometric data is then irreversibly compromised across all applications. This is not true.

In reality, data captured from a biometric sensor is stored as a template in binary code – put simply, encrypted 0s and 1s. Storing a mathematical representation rather than an image makes hacking considerably more challenging. The templates are irreversible so that the fingerprint image cannot be reverse engineered to re-create the original fingerprint image even if hackers should get hold of the data. Encryption of the data makes it impossible to reuse a template from one device in another. In most consumer applications, the biometric template is not stored in a vulnerable cloud-based location, it's securely hosted in hardware and software on the device itself. For example:

In smartphones, the template is stored, and the algorithms involved in the authentication process are run, in the highly-secure Trusted Execution Environment (TEE) in the device. All data is encrypted in such a way that it can only be used on that device.

The chip technology that secures the financial data in your bank card, the Secure Element (SE), offers a dynamic environment to store, process and match biometric information securely for biometric payment cards.

In most current access control use cases, such as building access and USB dongles, the biometric data required to authenticate a user is stored within the device itself, not in a third-party location.

These hardware-backed solutions meet the sweet spot of security: making it difficult enough, and the rewards limited enough, that hackers deem the challenge not worthwhile.

MYTH 02

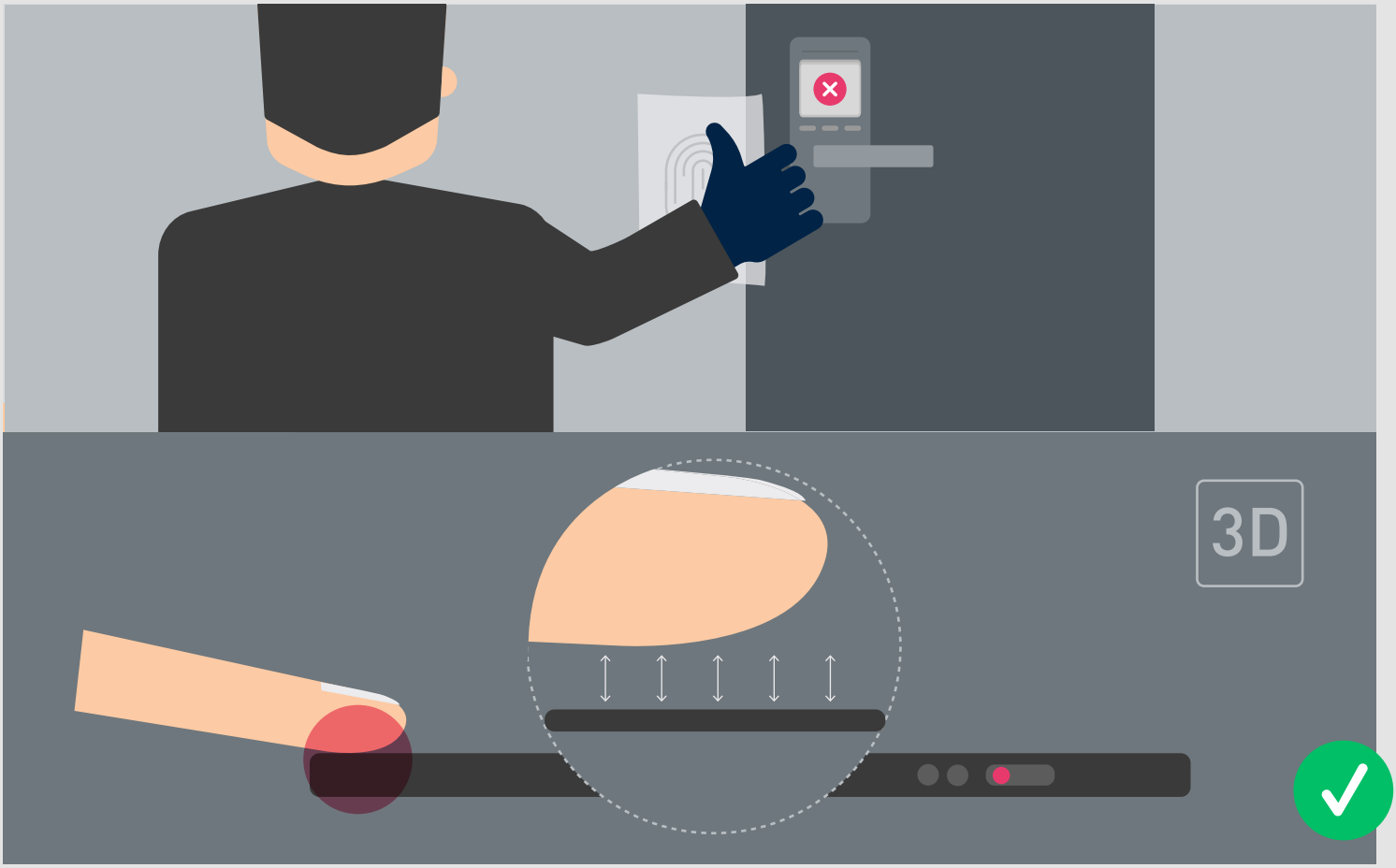
Fingerprints can be easily replicated to trick devices

MYTH

It is easy to create a 3D spoof from the fingerprint captured from e.g. a glass where someone has touched.

MYTH

It is easy to get hold of the personal devices that belongs to the correct fingerprint, without the owner noticing and blocking.



TRUTH

Anti-spoofing measures are now included as standard, preventing a 2D print or simple spoof from passing as a real finger. You need correct 3D-information to even try to gain access. Not only you need the right fingerprint in 3D, you also need to get hold of the device you want to access (the person's card, smartphone etc.) before the person notices it and blocks the card / phone etc. Making this an impractical and non scaleable attack.

BEWARE OF THE GUMMY BEAR!

The myths are numerous here. From cello tape and gummy bears, to printouts of fingerprints, many believe it's simple enough to simulate a biometric identifier to deceive devices and gain access. This process is known as spoofing.

Though historically, a gummy bear may have tricked sensors, modern solutions now have several sophisticated defences to make such simple spoofs impossible. Anti-spoofing measures are now included as standard.

Better software is key here. Improving the image quality captured and enhancing the matching algorithms is defending solutions from increasingly complex attacks. Fact is that all certifications by payment networks and FIDO require tested and proven anti-spoofing qualities.

The latest sensors cannot be fooled by a 2D replication of the fingerprint captured from something like a glass someone has touched, as it has then lost all its 3D information (e.g. the depth and height of the ridges and valleys). In real life it is extremely difficult to create a 3D copy of a fingerprint that would work effectively.

Plus, on top this, the criminal needs to have access to the person's device where this fingerprint is enrolled e.g. smartphone, payment card, before he/she notices and blocks it. This is not scalable nor common, in comparison gaining access to someones PIN code over the shoulder or skimming a contactless card is easier and a bigger problem.

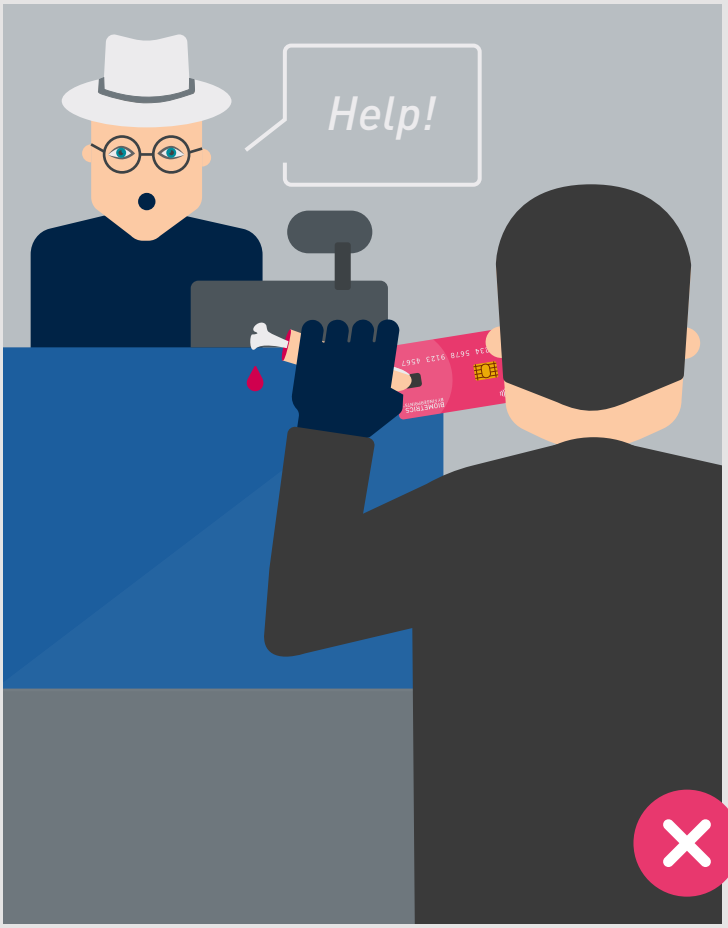
Beware, this isn't for the faint hearted

MYTH 03

Detached fingers are commonly used to access data

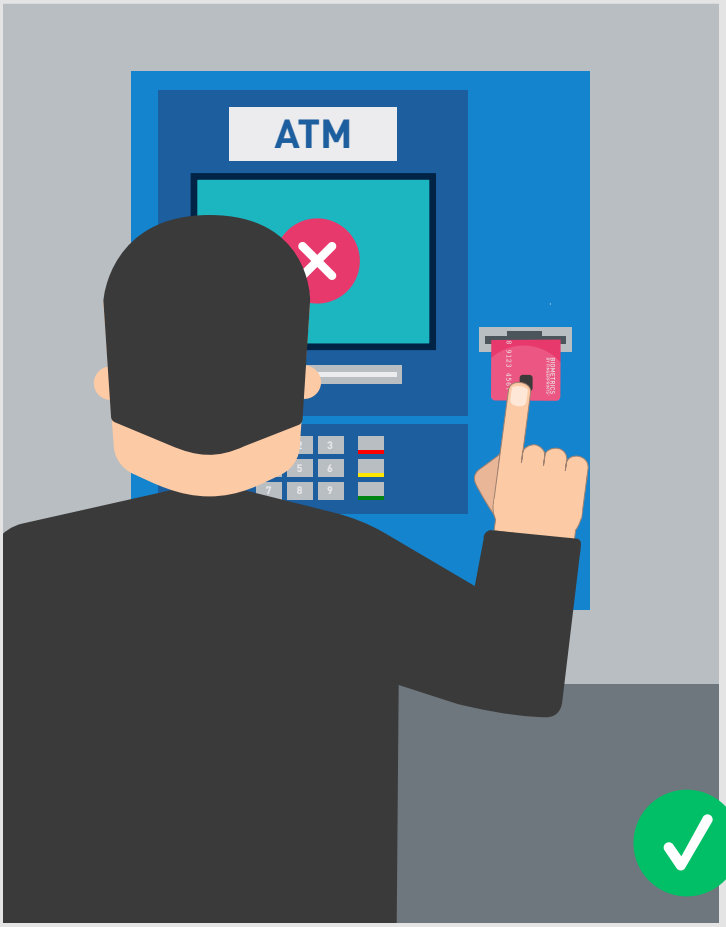
MYTH

Detached body parts, such as a finger or an eye can easily be used to access data.



MYTH

Like using it to verify payment with the correct card and or smartphone.



TRUTH

Removing a finger to access a victim's device (e.g. a payment card) might be compelling in films but, in reality, is a very extreme and unlikely scenario. Fraud takes the path of least resistance and, sadly, criminals have less complex techniques available, such as force and violence, to access data.

CHOP AND CHANGE

Using severed-off fingers to access locked rooms, a torn-out eye to get past an iris scanner?

Hollywood's portrayal of biometrics may be gruesome and compelling, but the probability of it happening in normal everyday life consumer use cases is very farfetched.

As mentioned earlier, biometric solutions now have sophisticated means to avoid this kind of risk. In addition, the attacker also would need to have access to the person's smartphone, payment card or other application on which the biometric is enrolled. Making this a very extreme and unlikely scenario.

Much more common is social engineering attacks, tricking the victim to give out his or her PIN or password. Biometrics protect completely against these attacks, as the biometric feature cannot be handed over.

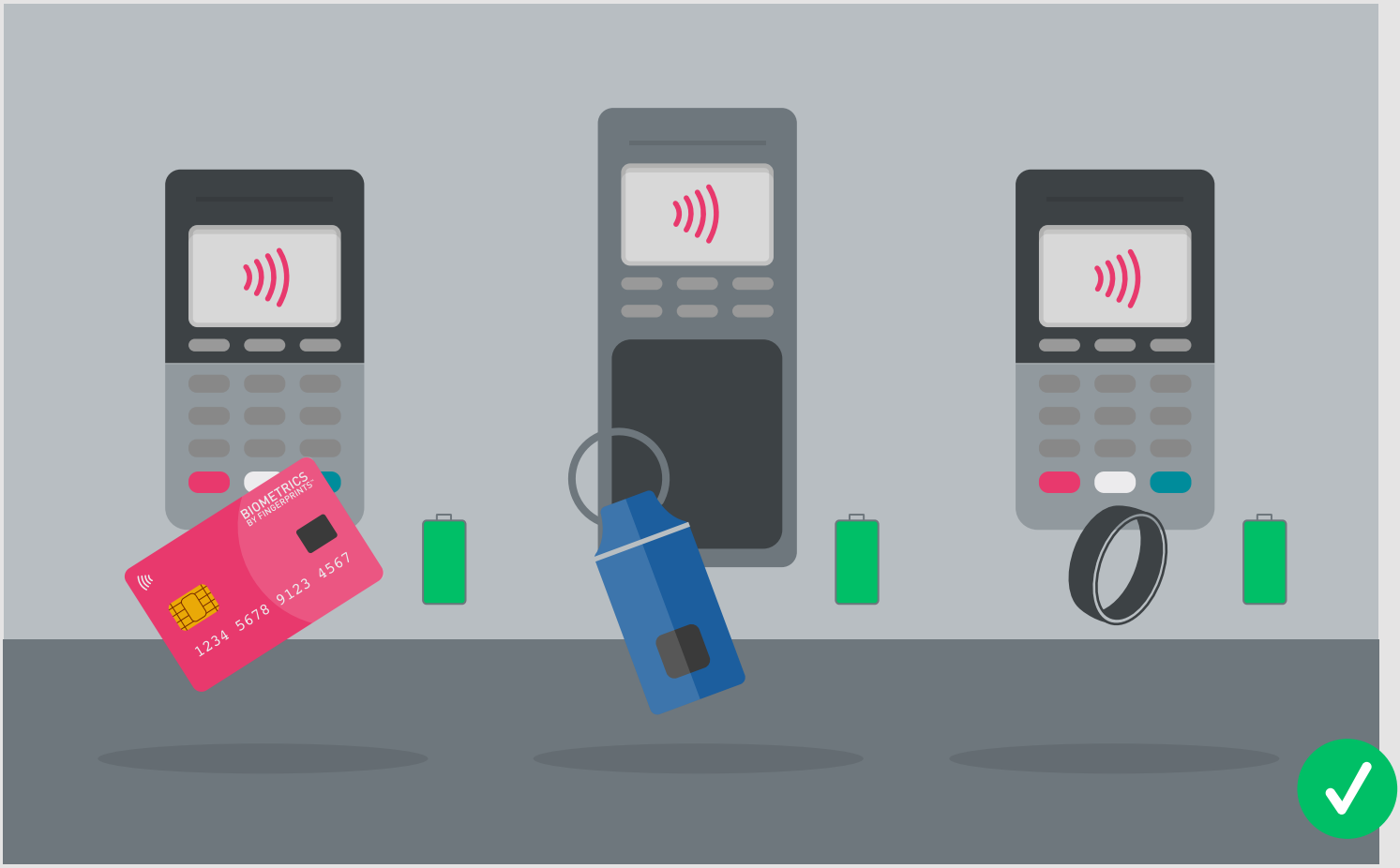
MYTH 04

New biometric form factors must have batteries and need re-charging

such as payment and access cards

MYTH

New biometric form factors, such as payment and access cards, need batteries and re-charging.



TRUTH

For payments cards, ultra-low power sensors are able to operate on the energy harvested from the POS terminal and the NFC field in the same way contactless cards are powered today. This same ultra-low power technology is being utilized for other contactless use cases too, such as access control cards, small fobs and rings.

WHO´S IN CHARGE HERE?

This statement sounds plausible, even believable; but it's not. Mobile phones have big batteries to power sensors, so surely new form factors with biometrics need one too?

Not quite.

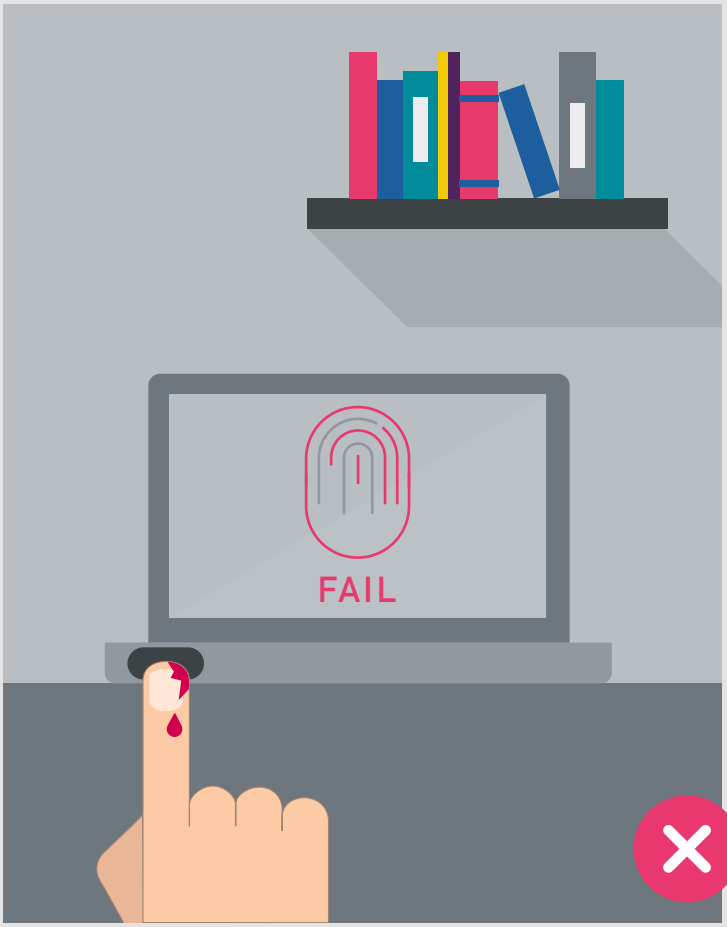
Experts in the R&D team have invested heavily to tailor the proven mobile sensor to integrate effectively into new smaller and less powerful form factors.

The biometric payment card is a great example. Now ultra-low power sensors can operate on the energy collected from the POS terminal and the NFC field in the same way contactless cards are powered. As a result, biometric payment cards forgo the need for a battery and are able to deliver the same UX of contactless, just with greater security!

This same ultra-low power technology is being utilized for other contactless use cases too, such as access control cards, small fobs and rings.

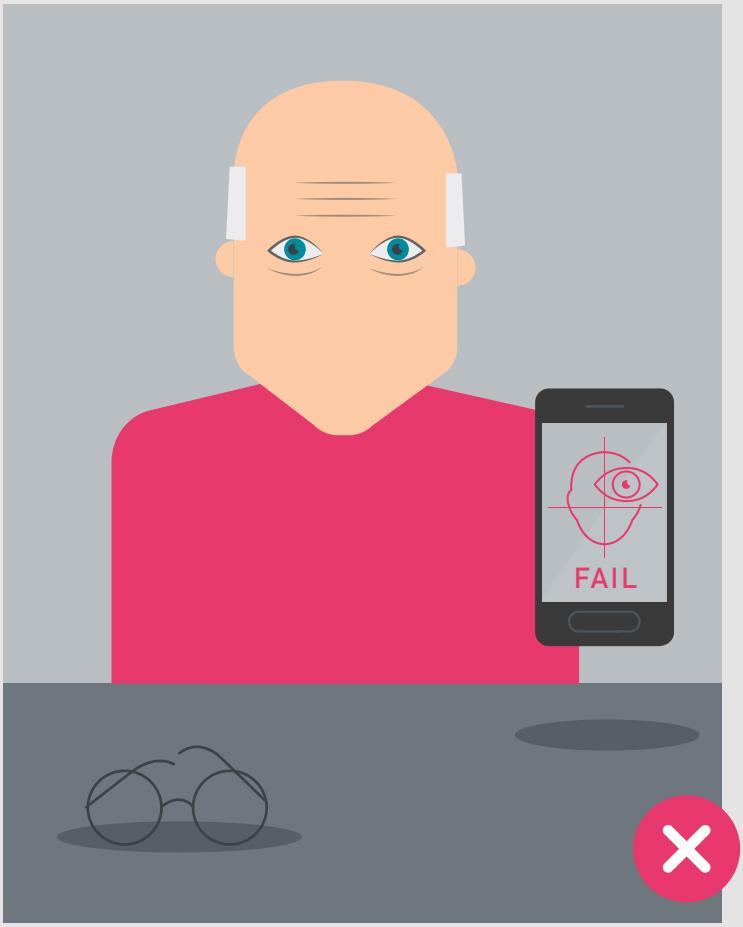
MYTH 05

If I change with age, or I get surgery, I'll be locked out by my own biometrics



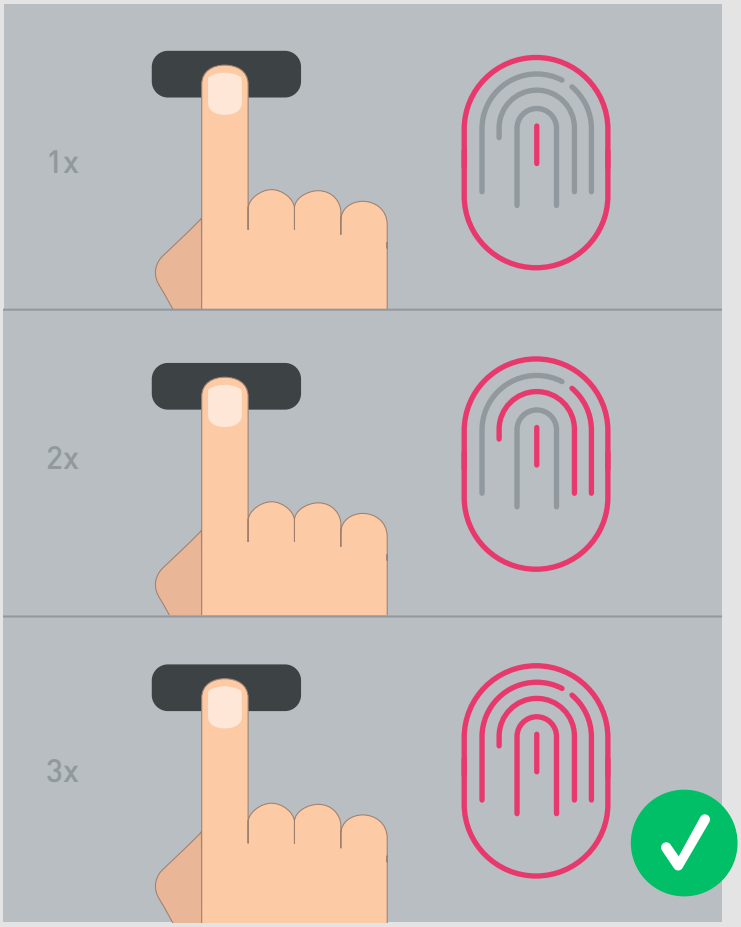
MYTH

If I cut my finger, I won't be able to access my devices.



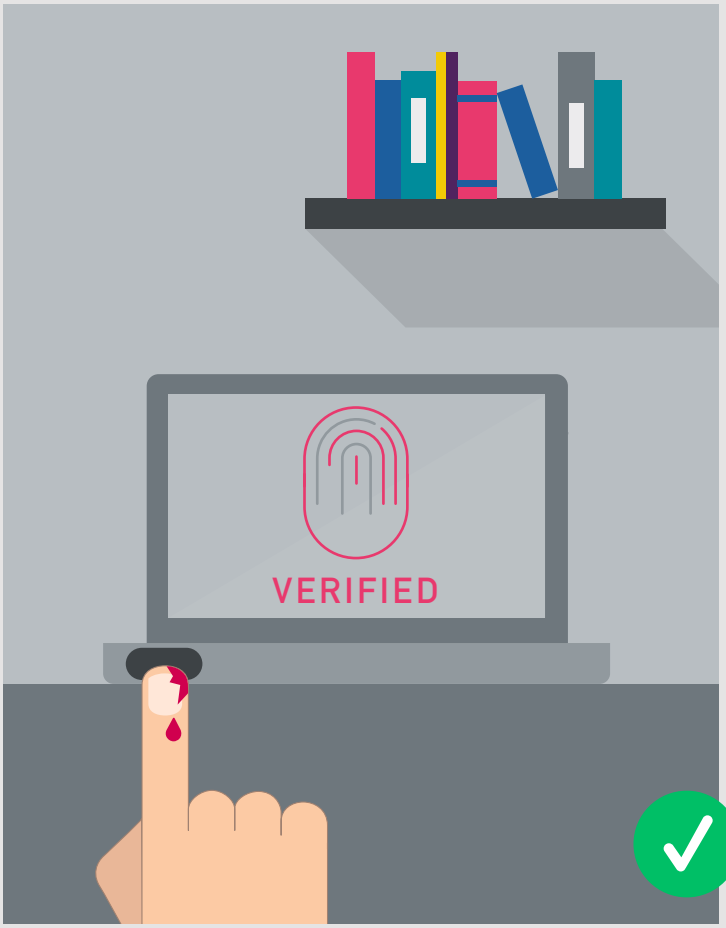
MYTH

When I change with age, I'll be locked out by my own biometrics.



TRUTH

Modern biometric technology features smart 'self-learning' algorithms. So when you touch the sensor a new area is learned everytime, therefore even if you hurt a part of your finger, the device still knows you well enough to verifiy it's you with the part that's left of your fingerprint.



TRUTH

Incremental changes, that happen over years – such as aging hands or eye debilitation - can be accounted for and are integrated into templates as part of the self-learning algorithms.

DAY AND AGEING

Many believe that once biometric data is captured, it remains static. And, as a result, any changes to their physiological circumstances will lock them out of their devices. But this isn't strictly true.

As you might expect, serious changes to an individual's physiological nature would affect their ability to use biometrics. Incremental changes however, that happen over years – such as aging hands or eye debilitation - can be accounted for.

Modern biometric technology features smart 'self-learning' algorithms. This means they update and incorporate evolutions as they happen. These can also take micro-cuts into account, too. Most cosmetic changes do not impact the key recognition points used by biometric systems.

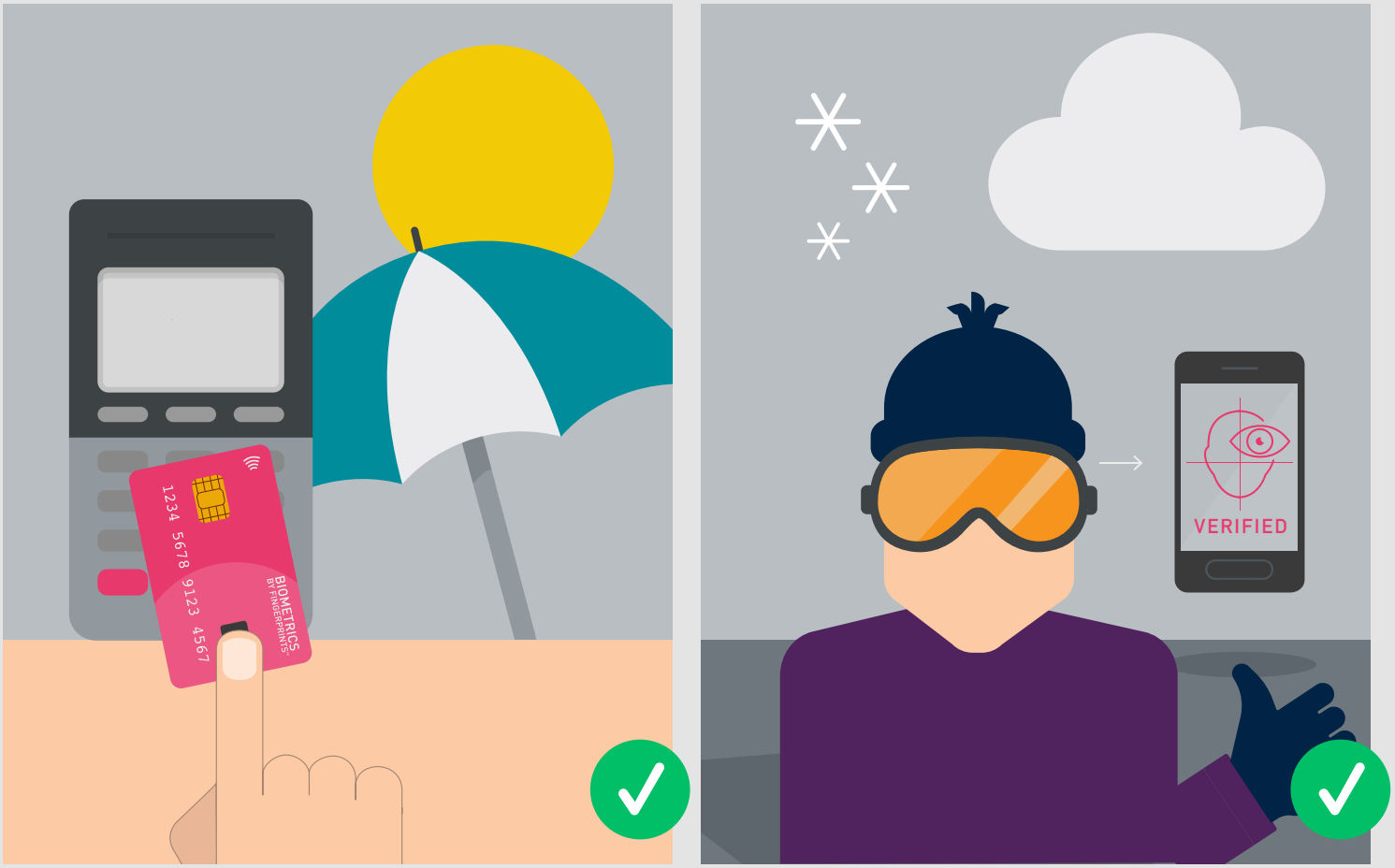
MYTH 06

Environmental changes will stop me from accessing my device

such as wet or dry fingers, wearing glasses or in sunlight.

MYTH

Environmental and temporary changes will stop me from accessing my device, such as wet or dry fingers, wearing sunglasses, a cold day or even a black eye or eyepatch.



TRUTH

In recent years, biometric solution providers have invested millions in R&D to ensure users can still be recognized during changes of climate or environment. By combining various biometric identifiers, users can overcome different conditions by utilizing another form – for example using touchless face or iris recognition while cooking instead of fingerprint.

TIMES CHANGE, BUT THEY OFTEN CHANGE BACK

In recent years, biometric solution providers have invested millions in R&D to ensure users can still be recognized during changes of climate or environment. Whether that's face and iris recognition adapting to bright sunlight or a fingerprint scanner still being able to read a cold finger, major improvements have been made to minimize FRR (false rejection rates – the number of times the right user is falsely rejected).

It's also where those smart algorithms come in again, learning and adapting to the small changes your fingerprint may experience when too hot or cool, for example.

Multi-modal biometrics solutions are already playing a role in countering temporary lock-out. By combining various biometric identifiers, users can overcome different conditions by utilizing another form – for example using touchless face or iris recognition while cooking instead of fingerprint.

BIOMETRICS

A HERO'S WELCOME

UNLIKE DEMONS AND DRAGONS, belief in the value of biometrics is only growing.

Biometric advances have surpassed many of the assumptions relating to limited functionality, security or complexity. While some myths remain, consumers are increasingly getting to grips with these advancements and understanding the value biometrics can add to their daily lives.

This is reflected by the extension of biometrics into new markets and use cases. Payments is a great example, with biometric payment cards one form factor gathering real momentum. Though, as we've seen, new myths are emerging there too...

Fingerprints™ has been a leader of innovation in biometrics for the last two decades. We're proud of the expertise and R&D that's been poured into making our range of biometrics solutions deliver stronger security and a better user convenience.

As solutions expand and diversify, the myth-busting fight will continue. But one thing's for sure, the future of biometrics is a story you don't want to miss.

ABOUT US

TRUSTED COMPANY

- Fingerprints sensors authenticate devices billions of times per day
- Hundreds of millions of sensors shipped yearly
- Integrated in over 400 smartphone models

OUTSTANDING PERFORMANCE

- Best in class security and accuracy measures
- Unrivalled low power consumption
- High image quality – optimized biometric performance for small sensors

ENHANCING DESIGN OPPORTUNITIES

- Our small sensors together with software enable brands to be as creative as they like
- Sensors in different sizes, shapes and colors
- Ready for cost-effective, high volume production

THE HISTORICAL MILESTONE OF

1 BILLION SENSORS

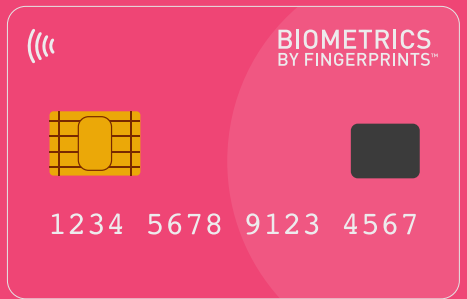
SHIPPED WAS REACHED IN *MAY 2019*

21 OF 21

CONTACTLESS BIOMETRIC PAYMENT CARD PILOTS

1 OUT OF 1

COMMERCIAL LAUNCHES



OUR PRODUCTS EXIST IN MORE THAN

+100

DIFFERENT ACCESS ***DEVICES AND APPLICATIONS***

FINGERPRINTS