

A close-up photograph of a person's hand holding a smartphone. The hand is positioned in the foreground, with the fingers slightly curled around the device. In the background, a laptop keyboard is visible, showing keys like 'Q', 'W', 'E', 'R', 'T', 'Y', 'U', 'I', 'O', 'P', 'A', 'S', 'D', 'F', 'G', 'H', 'J', 'K', 'L', 'Z', 'X', 'C', 'V'. The lighting is bright, and the overall scene suggests a professional or office environment.

# **4 Fingers Are Better Than One**

## A Primer on Hand Recognition

**VERIDIUM**  
HANDS ON SECURITY

# Security in the Palm of Your Hand

More financial services companies are embracing biometrics for user authentication in their mobile apps every day. From Visa to smaller banks, using a fingerprint or selfie to authenticate a payment or transfer is much more secure than simply entering in a password. But one of the first mobile-only banks, bunq, has chosen an even more secure biometric for authenticating transactions – hand recognition.

bunq needed an easy and convenient way to authenticate transactions that was also highly secure. They opted for a biometric that eliminated security risks and was still easy and convenient to use – 4 Fingers TouchlessID.

Now, whenever a bunq customer wants to perform a transaction that requires a greater degree of security, they are prompted to scan their four fingers to authenticate. This combines an easy-to-use, seamless experience with optimized security practices.

“  
We chose  
4 Fingers with  
VeridiumID because it  
supports our guarantee  
for an easy-to-use and safe  
banking experience using the  
latest technology for biometric  
authentication on the market.  
”

*- Ali Niknam, CEO and Founder of bunq*



# The Birth of Digital Fingerprinting

While the modern use of fingerprinting has been around since the late 1800s, the invention of the computer and image scanning is what truly led to mass adoption of fingerprints as a security tool. Moving beyond law enforcement's use of fingerprints to identify criminals, digital image scanning allowed biometric security systems to be built. Early models were large and expensive, requiring costly computer systems hooked into wall- or table-mounted hand scanners, but they worked. You can lose a key or forget a passcode, but you always have your biometrics in hand.

However, the birth of global communication and the rise of the computer has provided the catalyst needed to launch fingerprinting into an everyday technology we use to unlock a tool that early adopters of fingerprinting couldn't even have dreamed of – the miniature computers we carry in our pockets.



# The Rise of Mobile Biometrics

When Apple introduced the iPhone the company revolutionized the mobile phone industry. Moving beyond phone calls and texting to being able to read email, listen to music, and download games all on a single device was a game changer, and it's easy to forget that it was only 10 years ago that this amazing device was released.

While Apple certainly didn't invent the smartphone, they created the first popular, easy-to-use, widely adopted one, and that trend would carry over into the addition of biometric sensors to mobile devices. In 2013 Apple once again delivered a game-changing technology with Touch ID. At the time the iPhone was already the top-selling smartphone, and this widespread popularity meant that millions adopted mobile fingerprint authentication practically overnight.

Touch ID offered consumers whose only experience with biometrics was in the movies to use the technology first hand and become comfortable with it. Over time, Apple has expanded its use beyond just unlocking the iPhone to enabling security features and authenticating ApplePay transactions, and other manufacturers have adopted the same features. However, the embedded mobile fingerprint sensor is a far cry from the security of more traditional digital fingerprint capture.



# What's Wrong With Touch ID?

There are a number of issues with Touch ID and its Android-based cousins. These weaknesses in the technology, while they don't negate its use as a mobile biometric tool, should raise an eyebrow in those looking to deploy mobile biometrics for more advanced security needs.



## Embedded Fingerprint Sensors only Capture a Partial Print

Existing mobile fingerprint sensors are, by necessity, very small. If you look at the buttons they're embedded in, they are a fraction of the size of our actual fingertip. This only allows them to authenticate against a small section of the **minutiae** on the fingertip. Ultimately, this means the number of points that can be compared to authenticate the print are far fewer than in traditional fingerprints, which makes the biometric less accurate and, even worse, easier to spoof.

Minutiae are the key points of interest in a fingerprint, including the bifurcations (a ridge splitting into two) and ridge endings, as well as any scars or other distinguishing characteristics.

## Partial Prints are Susceptible to Presentation Attack

Spoofing a fingerprint, more accurately referred to as a presentation attack, is one of the most common attack methods for biometrics. In most cases, it refers to using a copy, either a photo or mold, of a person's fingerprint to trick a biometric authentication system into allowing access. There are a variety of techniques used to stop this type of attack, but researchers have shown that the process of **spoofing a mobile fingerprint sensor is deceptively easy.**



In 2016, Computer Science researchers Kai Cao and Anil Jain of Michigan State University showed that you can spoof a mobile fingerprint sensor for less than \$500 using an ordinary printer and conductive ink. The process only takes 15 minutes and requires a 300 dpi-quality image of the subject's fingerprint. What makes this spoofing process special is that the use of the conductive ink bypasses Liveness checks on the device.



## Usability is Determined By Device

Another drawback to existing mobile fingerprinting solutions is that the use of the captured print is often heavily affected by the device you own. Apple's Touch ID only works with a specific selection of Apple and third-party apps, and the same goes for the various Android equivalents. This makes its use outside of personal security and authentication extremely limited. For example, even if your company integrates the Touch ID API into a corporate app to use it as a security solution for logging into company email, not every employee will have an iPhone, limiting its use across the organization.

As mobile- and biometrics-based security adoption continues to grow, individuals and businesses need a biometrics solution that enables a stronger level of security. This can be achieved by increasing the number of minutiae captured far beyond a partial fingerprint, or even a single fingerprint, with hand recognition.








# Mobile Hand Recognition Is The Next Step

Of course, the first question you're asking is "but if the fingerprint sensor on my smartphone only captures a partial print, how do I perform hand recognition?" Simple, by not using the embedded sensor.

The key to performing mobile hand recognition is to use one of the most powerful sensors already on the device, rather than a dedicated fingerprint sensor – the camera. Modern smartphone cameras are more than powerful enough to capture a high enough quality photo to extract fingerprint minutiae. This allows for a contactless fingerprint capture and hand recognition on any smartphone, with seamless integration with the right app across a company's entire workforce or customer base.

The same device may allow for facial recognition using the front-facing camera, but there are disadvantages to face biometrics that don't exist with hand recognition. For one, facial recognition algorithms aren't as accurate as fingerprints by nature. Secondly, the front-facing camera on most smartphones isn't as powerful as the rear-facing camera, which is used for hand recognition, ensuring more detail is captured in the image. It's also easier to get false rejections due to environmental issues, such as poor lighting. By using your hand, the rear-facing camera, and an LED flash you can eliminate lighting and other environmental issues while using a more reliable biometric in the first place.

	UNIVERSALITY	UNIQUENESS	PERMANENCE	COLLECTABILITY	PERFORMANCE	ACCEPTABILITY	SECURITY
	HIGH	LOW	MEDIUM	HIGH	LOW	HIGH	LOW
	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH	HIGH

## Introducing: 4 Fingers TouchlessID

Taking the combined advantages of hand recognition and the potential of modern smartphone cameras, we realized that there's a need for a powerful biometric that doesn't require the user to touch a sensor and is compatible with a wide range of devices, rather than a single manufacturers. Hand recognition would provide a much more powerful and secure mobile biometric, and by making it touchless, it would be extremely convenient for the user to perform authentication.

**Enter 4 Fingers TouchlessID.**





## Advantages of 4 Fingers TouchlessID

There are many advantages to 4 Fingers TouchlessID. It's fast and easy to use. You don't need any special hardware in the mobile device, just a 5MP camera and LED flash, making it compatible with older smartphones that might not have a fingerprint sensor. This offers a variety of high-value use cases for:

- Banks for adding a more secure biometric authentication to mobile transactions.
- Law enforcement for capturing fingerprints in the field.
- Hospitals for providing a sanitary way to authenticate at workstations
- Adding additional layers of security to existing corporate biometric systems

In fact, we're working with the National Institute of Standards and Technology to include 4 Fingers TouchlessID in their federal certification program for contactless fingerprint capture, setting it up to become a standard in some of these areas, such as law enforcement and immigration.

## Conclusion

The development of easy-to-deploy mobile hand recognition will be an important turning point in both the adoption and acceptance of mobile biometric authentication. With support for more advanced security demands and universal compatibility with a much broader range of devices, more companies will be able to embrace biometric authentication for their secure access needs. Whether using biometrics as part of an Active Directory login solution or as part of a mobile app to authenticate financial transactions, you need a secure, convenient, flexible biometric, like hand recognition, to support these numerous use cases.



100 Hancock Street  
10th Floor  
Quincy, MA 02171  
877.301.0299



Chalfont Park, Building 1  
Gerrards Cross SL9 0BG  
United Kingdom  
44.1753.208780