

Amazon One's palm-scanning payment technology gains traction

 By [Katja Hamilton](#)

29 Aug 2022

Handprint biometric payment technology looks set to turn consumers' traditional point-of-sale experience on its head.



Source: Amazon,

By hovering their palm over a scanner at the till, paying for goods promises to be seamless, contactless and cashless. This thanks to Amazon One scanners, which Amazon introduced late last year, and which this month launched at 65 Whole Foods Market locations in the US.

Whole Foods, a subsidiary of Amazon, is an organic food supplier in the US which has integrated biometric palm-print scanners at its till points, alongside retailers like Amazon Go and Amazon Go Grocery, as well as third-party retailers who purchased the technology from Amazon.

But how exactly does this technology work?

Sign up is quick. Really quick. Consumers just scan their palm, enter their mobile number and provide a credit card and/or merchant membership number.

Amazon says the technology "captures the minute characteristics of their palm - both surface-area details like lines and ridges as well as subcutaneous features such as vein patterns - to create a palm signature".

This signature palm print is stored in the cloud and is used to confirm a user's identity when they're in one of its stores.

Biometric data harvesting

But while many US consumers are excited and [optimistic](#) about the availability of Amazon One, some are more circumspect, wanting more clarity on what Amazon will be doing with the biometric data it collects.

The company's past malfeasance in data collection has come under the microscope of late, as Amazon has a [record](#) of selling biometric facial recognition services to United States law enforcement and [sharing](#) palm-print data with government agencies..

A group of US senators have [expressed](#) their concerns about the palm-scanning system. Senators Amy Klobuchar, Bill Cassidy and Jon Ossoff wrote in an open letter to Amazon chief executive Andy Jassy, "In contrast with biometric systems like Apple's Face ID and Touch ID or Samsung Pass, which store biometric information on a user's device, Amazon One reportedly uploads biometric information to the cloud, raising unique security risks."

There are concerns too about potential hackers stealing the data from the cloud.



Pick n Pay migrates IT infrastructure to Amazon Web Services

25 Aug 2022



But Amazon One [reassures](#) clients that the data Amazon One collects is stored safely in the cloud.

"While the kiosk takes a picture of a user's palm, Amazon One doesn't store the image there but instead encrypts it and sends it to a server for matching," it said in a statement.

"Your palm data is used to generate your unique palm signature and to confirm your identity when you use Amazon One. Your information is not stored on an Amazon One device and is protected at all times, both at rest and in-transit.

"Customer trust is our top priority. We treat your palm signature just like other highly sensitive personal data and keep it

safe using best-in-class technical and physical security controls."

Customer identity at risk

But while Amazon One is putting freedom in our hands as we move to a contactless society, what are we risking for this convenience?

Exposure of someone's biometric information can have far more implications than exposure of a password or credit-card number, because it cannot be undone. It is a serious problem when one's ability to carry out financial transactions depends on it.

Morey J. Haber, chief security officer of BeyondTrust [elaborates](#): "Typically, as a human being, you have a single identity and one set of biometric data, as you cannot alter your fingerprints, voice, face, eyes, EKG, or veins.

"When information technology leverages biometric data for authorisation or authentication, it must compare the results against a banked, electronic profile of your biometric data. Stringent security protections, including encryption, can help keep biometric data at rest protected.

"However, to make use of the biometric data, it must be reassembled (at least in parts) to compare to the assessed input. Storage design flaws, vulnerabilities, and host system misconfigurations are just a few of many ways that could leave biometric data ripe for exposure. Because you cannot change your biometric data. Once your biometric data has been leaked or compromised, it puts you at continual risk for identity-based attacks."



Hands up! Icasa wants your biometrics

Ahmore Burger-Smidt 28 Mar 2022



Jayati Ghosh's article [Biometric data poses grave risks to privacy](#) is well worth a read. In it she details cases in India where identity thefts as a result of purely stored biometric data have had devastating consequences for its citizens, and highlights that the more we normalise these tactics, the harder they will be to escape.

Either way, biometric identification systems are permeating every facet of our lives. If we don't draw a line in the sand here, who knows what our future will look like.

Ghosh sums it up tacitly when she says: "Unless and until citizens and policymakers recognise and address the complex security risks they entail, no one should feel safe."

Amazon One's adoption at Whole Foods locations in the US is the biggest rollout of the technology to date at stores in Malibu, Montana Avenue, Santa Monica, Los Angeles, Orange County, Sacramento, the San Francisco Bay Area, and Santa Cruz. Whole Foods has 500 stores in North America alone.

ABOUT KATJA HAMILTON

Katja is the Finance, Property and Healthcare Editor at Bizcommunity.

- #AfricaMonth: Kennedy Bungane champions Africanbank's expansion - 31 May 2024
- Dubai bounces back: Arabian Travel Market spotlights surging visitor numbers - 8 May 2024
- SA Post Office: Union deal halts layoffs at the 11th hour - 24 Apr 2024
- Transition to ZiG currency sparks trade disruption in Zimbabwe - 11 Apr 2024
- Ntabelang Likotsi champions the first majority Black women-owned mutual bank - 18 Mar 2024

[View my profile and articles...](#)

For more, visit: <https://www.bizcommunity.com>