Why Mastercard's new face recognition payment system raises concerns

May 24 2022, by Rita Matulionyte

Credit: Tima Miroshnichenko from Pexels

Mastercard's "smile to pay" system, announced last week, is supposed to save time for customers at checkouts. It is being trialed in Brazil, with future pilots planned for the Middle East and Asia.

The company argues touch-less technology will help speed up transaction times, shorten lines in shops, heighten security and improve hygiene in businesses. But it raises concerns relating to customer privacy, data storage, crime risk and bias.

How will it work?

Mastercard's biometric checkout system will provide customers facial recognition-based payments, by linking the biometric authentication systems of a number of third-party companies with Mastercard's own payment systems.

A Mastercard spokesperson told The Conversation it had already partnered with NEC, Payface, Aurus, Fujitsu Limited, PopID and PayByFace, with more providers to be named.

They said "providers need to go through independent laboratory certification against the program criteria to be considered"—but details of these criteria aren't yet publicly available.

According to media reports, customers will have to install an app which will take their picture and payment information. This information will be saved and stored on the third-party provider's servers.

At the checkout, the customer's face will be matched with the stored data. And once their identity is verified, funds will be deducted automatically. The "wave" option is a bit of a trick: as the customer watches the camera while waving, the camera still scans their face—not their hand.

Similar authentication technologies are used on smartphones (face ID) and in many airports around the world, including "smartgates" in Australia.

China started using biometrics-based checkout technology back in 2017. But Mastercard is among the first to launch such a system in Western markets—competing with the "pay with your palm" system used at cashier-less Amazon Go and Whole Foods brick and mortars in the United States.

What we don't know

Much about the precise functioning of Mastercard's system isn't clear. How accurate will the facial recognition be? Who will have access to the databases of biometric data?

A Mastercard spokesperson told The Conversation customers' data would be stored with the relevant biometric service provider in encrypted form, and removed when the customer "indicates they want to end their enrollment." But how will the removal of data be enforced if Mastercard itself can't access it?

Obviously, privacy protection is a major concern, especially when there are many potential third-party providers involved.

On the bright side, Mastercard's customers will have a choice as to whether or not they use the biometrics checkout system. However, it will be at retailers' discretion whether they offer it, or whether they offer it exclusively as the only payment option.

Similar face-recognition technologies used in airports, and by police, often offer no choice.

We can assume Mastercard and the biometrics provider with whom they partner will require customer consent, as per most privacy laws. But will customers know what they are consenting to?

Credit: AI-generated image

Ultimately, the biometric service providers Mastercard teams up with will decide how they use the data, for how long, where they store it, and who can access it. Mastercard will merely decide what providers are "good enough" to be accepted as partners, and the minimum standards they must adhere to.

Customers who want the convenience of this checkout service will have to consent to all the related data and privacy terms. And as reports have noted, there is potential for Mastercard to integrate the feature with loyalty schemes and make personalized recommendations based on purchases.

Accuracy is a problem

While the accuracy of face recognition technologies has previously been challenged, the current *best* facial authentication algorithms have an error of just 0.08%, according to tests by the National Institute of Standards and Technology. In some countries, even banks have become comfortable relying on it to log users into their accounts.

Yet we can't know how accurate the technologies used in Mastercard's biometric checkout system will be. The algorithms underpinning a technology can work almost perfectly when trailed in a lab, but perform poorly in real life settings, where lighting, angles and other parameters are varied.

Bias is another problem

In a 2019 study, NIST found that out of 189 facial recognition algorithms, the majority were biased. Specifically, they were less accurate on people from racial and ethnic minorities.

Even if the technology has improved in the past few years, it's not foolproof. And we don't know the extent to which Mastercard's system has overcome this challenge.

If the software fails to recognize a customer at the check out, they might end up disappointed, or even become irate—which would completely undo any promise of speed or convenience.

But if the technology misidentifies a person (for instance, John is recognized as Peter—or twins are confused for each other), then money could be taken from the wrong person's account. How would such a situation be dealt with?

Is the technology secure?

We often hear about software and databases being hacked, even in cases of supposedly very "secure" organizations. Despite Mastercard's efforts to ensure security, there's no guarantee the third-party providers' databases—with potentially millions of people's biometric data—won't be hacked.

In the wrong hands, this data could lead to identity theft, which is one of the fastest growing types of crime, and financial fraud.

Do we want it?

Mastercard suggests 74% of customers are in favor of using such technology, referencing a stat from its own study—also used by business partner Idemia (a company that sells biometric identification products).

But the report cited is vague and brief. Other studies show entirely different results. For example, this study suggests 69% of customers aren't comfortable with face recognition tech being used in retail settings. And this one shows only 16% trust such tech.

Also, if consumers knew the risks the technology poses, the number of those willing to use it might drop even lower.

Provided by The Conversation