



## Biometric Payments - What You Should Know

technology payments biometrics

**Summary:** Biometric payments are expected to exceed \$1.67 trillion per year by 2023. Is your institution ready for this?

Did you know that the idea of using the iris pattern of your eye for identification was first brought up in 1936? Frank Burch, the ophthalmologist responsible for this idea, would likely be surprised by how long it took to actually put his idea to use.

Yet, today people are still incredibly skeptical when it comes to security measures that involve storing their fingerprints or irises in any sort of database. Despite such concerns, [biometric payments](#) are expected to exceed \$1.67T per year by 2023. With this level of growth, it is important to know what this means for your financial institution.

[Searchsecurity.com](#) defines [biometric payment](#) as a POS technology that uses biometrics, such as a fingerprint, to identify the payer and authorize the transfer of funds.

According to a new report from Goode Intelligence, a biometrics research and consulting firm, global biometric payments are gaining speed at a rapid rate. At present, 68% of global biometric payments are made through mobile devices, but that too is expected to shift as biometrics become more widely embraced by retailers as an additional level of security. By 2023, Goode predicts that 54% of biometric payments will be made remotely, with 46% made in person. Perhaps more importantly, the firm also believes that biometric payment cards could even replace PIN codes for debit cards and predicts that globally there will be roughly 579mm biometric payment cards being actively used by 2023. As this happens, you will need to support the changing needs of your merchant customers, so it would be prudent to start planning.

When it comes to the US, while adoption is all but a certainty, it may be a bit slower. A study by The Clearing House found that 89% of consumers in North America, which use fintech apps, have concerns about companies sharing their data and protecting their personal information--with 60% specifically worried about sharing biometric information and social security numbers. But in the end, convenience is expected to win out, particularly as more businesses add biometric sensors and major technology companies introduce biometric software solutions designed to enable faster secure payments.

Community financial institutions will not have the luxury of sitting on the sidelines and should begin taking steps towards their own biometric transformations--particularly as efforts to introduce open banking initiatives in the US seem to be gaining traction. Start by outlining any necessary changes to your systems, products and processes. Talk to your core provider about their upcoming advancements too. Some things may be easier than you think. Then, begin educating employees about the ins and outs of biometric security measures and some of the specific ways that they can potentially improve specific features and services offered. Also, communicate your progress along with the current security measures to your customers. Lastly, work the pertinent changes into your budget for the next few years to ensure you are investing wisely for your institution's and customers' needs.

## ON DEMAND HELP FOR FINANCIAL INSTITUTIONS

Financial institutions face many difficult challenges every year, but you are not alone. Our experts stand ready to help you address a variety of issues. Find out more about [our solutions](#) today.

*Copyright 2021 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.*