https://www.axios.com/2020/02/18/biometrics-banking-retail-privacy

Some banks have dropped the creepier biometrics: Republic Bank of Kentucky said in 2016 that it would let customers log in to their mobile banking app by fingerprint or eye vein scan — now it offers the finger option plus facial ID.

"If it weren't for being able to use your thumbprint on your iPhone, I think biometrics would still be something on the fringe of authenticating," Trace Fooshee of Aite Group, a banking consultancy, tells Axios.

What they're saying: "A biometric is a very sensitive piece of personal information.

Reality check: Banking and credit card companies say biometrics — which, so far, are usually optional — are invaluable in fighting fraud and that spoofing is rare.

But banks — and, increasingly, retailers — have been working in overdrive to use biometrics both in back-end systems (where consumers won't see them) and public-facing ones:  
  
Chase, Bank of America, Citi and Wells Fargo have introduced various biometric ID options, including voice, fingerprint, eye or facial recognition.

Between the lines: What customers don't see is banks' and retailers' heavy use of "passive" or "behavioral biometrics" to thwart fraud.

Why it matters: These companies are amassing giant databases of our most personal information — including our gait, how we hold our cellphones, our typing patterns — that raise knotty questions about data security and privacy.

Several banks gave "no comments" to Axios when asked about their biometrics programs; Amazon did too.

https://www.santander.com/en/stories/biometrics-the-future-of-security-in-digital-banking

These types of features are called biometric data and they are becoming increasingly important when it comes to security in digital banking.

As we have said, biometrics uses those unique, non-transferable features of the human being, so the authentication of security systems consists in creating and saving a model or data map that represents the user exclusively and serves to confirm their identity when they request access, whether to physical or virtual spaces.

https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-in-banking-is-not-secure

And biometric data is more sensitive than other personal information banks store on behalf of their customers because unlike a credit card number (or even a name!), stolen biometric data cannot be replaced: It corresponds to a person's face or fingerprints.  
  
Being particularly susceptible to attacks, banks should think twice about generating a honeypot of such personal data.

Instead of dabbling in biometrics, banks could focus on software and instructions that push customers to more secure password practices.

So any regulation of banks’ use of biometrics should be designed to impose sufficient financial loss on the banks to incentivize them to design systems that effectively safeguard biometrics.

If the compromised data happens to be biometrics, issues of identity theft may simply be unresolvable.

In that case, banks rely on Apple to tell them whether there is a fingerprint match, and do not access any biometric data themselves.

The biometric data that they get from processing those geometries (what banks call “templates”) can also be abused if they are accessed in combination with the algorithm used to extract the templates from the original images.

If the eye’s iris is the biometric scan, for example, someone could display a photo of a customer’s face into the phone camera to gain access.

Ultimately, it is not clear that biometrics in banking will actually provide better protection than passwords.

At this point, bank hackers are probably not looking for biometric data when attacking a bank.

It is not enough for banks to simply avoid storing images of fingerprints, faces or irises.

An estimated 17.6 million Americans were subject to identity theft in 2014, mostly through breached bank accounts and credit cards.

But even if it leaks as a by-product of a financial breach, criminals will find ways to abuse biometric data or resell it for further exploitation.

https://www.idmission.com/en/blog/5-ways-biometrics-improve-your-banks-bottom-line

Biometrics Enhances the Customer Experience  
  
A growing number of banking customers are avoiding retail bank branches, and their actions have nothing to do with social distancing or lockdowns or COVID-19.

Here are the top five ways that biometrics improves your bank’s bottom line.  
  
1.

Biometric identity verification eliminates the friction so common with manual identity verification by letting bank customers identity themselves with their faces or their fingerprints.

Biometrics Reduces Overhead  
  
Biometrics gives your bank the option of reducing your footprint.

With biometrics, retail banks keep sensitive data secure by ensuring that only authorized users are permitted to access it.

Biometrics Makes Banking Transactions More Secure  
  
Before fraudsters can steal from your bank, they must first steal an identity.

Deploying biometric identity verification across your banking platforms has a significant positive impact on your bottom line.

For example, banks are using technology like IDmission’s Biometric Identity Verification to identify customers in a split second, all from the customer’s phone.

Bank employees are required to present a keycard (something they have), a PIN (something they know), and a selfie (something they are, the biometric component).

Customers who enjoy the benefits that biometric identity verification offers continue doing their banking with your bank.

From reducing costs to increasing sales, biometrics is paving the way for banks to undergo digital transformation.

Biometric identity verification uses behavioral or physical characteristics to identify whether a customer or employee is allowed access to devices, systems, or data.

Biometric identity verification makes banking transactions more secure by adding another layer of security.

If your bank is looking for ways to protect your bottom line in the face of increasing uncertainty, you should consider biometrics.

Biometrics improves your bottom line by making banking transactions more secure, enhancing the customer experience, increasing security across all access control points, increasing sales, and reducing overhead.

Deploying biometric identity verification gives you options.

Biometric identity authentication helps you do both.

Biometrics Increases Security Across All Access Control Points  
  
If your bank has dozens or hundreds of branches, you know the challenge of employee access control.

Today’s facial recognition engines use artificial intelligence, machine learning and liveness detection (both active and passive detection) to make it next to impossible for fraudsters to fool these systems with stolen identities, since stealing someone’s face is still fairly difficult to do.  
  
2.

Biometrics reduces customer churn.

Reap the Benefits of Biometrics in Your Bank  
  
One thing you can be sure about is that the world won’t look the same after the COVID-19 pandemic has passed.

Last time we checked, almost 40% of potential new banking customers abandon traditional onboarding processes and head to a digital alternative provided by a competitor.

For example, with facial recognition systems, instead of presenting a bank card number and PIN, customers must also present their face to a facial recognition system, typically in the form of a selfie that they take with their smartphone.

https://id4d.worldbank.org/guide/biometric-data

Minimal training or low capacity of the operator capturing the biometrics Lack of incentives and/or time for capturing quality data Poorly implemented enrollment and quality assurance process  
  
Biometric system characteristics: Quality of the biometric scanners and software, including the Automated Biometric Identification System (ABIS) and other software development kits that may be used The statistical nature of biometrics Changing properties of biometric characteristics (i.e., facial appearance over time) Non-optimum threshold setting for matching algorithm—i.e., the tradeoff between the FMR and FNMR  
  
Some of these issues may be addressed through: Designing a multi-biometric system (see above) to ensure that most people are able to provide at least one viable sample  
  
Optimizing enrollment procedures, including by using: Better capture devices and software with built-in quality assessment to improve data quality and reduce FTE Quality Assurance Process and standards (e.g. NFIQ-II) Conditioning materials (gels, alcohols, etc.) that improve finger image contrast Uniform background for facial images Choice of capture devices (small versus large scanners, 4-4-2 versus single fingerprint scanners, optical versus capacitive)

Additional analysis on biometric modalities and their use for authentication can be found in the ID4D Technology Landscape report.

In addition to biographic data, many ID systems collect fingerprints, iris scans, facial images, and/or other biometry to use for biometric recognition—automatic recognition of individuals based on their biological or behavioral characteristics (ISO/IEC 2382-37).

In particular, the collection and use of biometric data presents some particular data protection and exclusion risks and can significantly add to the cost of the ID system and add operational complexity.

The ease with which individuals can interact with the technology used to capture the biometric data and its utility for different purposes (e.g., some biometric modes may be more convenient for authentication than others)  
  
Cost.

Biometric recognition encompasses both biometric identification—the process of searching against a biometric enrollment database to find and return the biometric reference identifier(s) attributable to a single individual (i.e. 1:n)—and biometric verification—the process of confirming a biometric claim through biometric comparison (i.e. 1:1) (ISO/IEC 2382-37).

Key considerations for using biometrics Inclusion Reliability Data Protection Sustainability Certain biometrics may be difficult or impossible for some people to reliably provide, necessitating multimodal biometrics and/or appropriate technical and procedural measures to reduce exclusion.

Certain biometric modalities may be optimal for conducting duplicate biometric enrollment checks (i.e., 1:N/N:N matching, while others may be optimal or sufficient for use during authentication (1:1 matching).

This is also true for any other type of authentication method and is not limited to the use of biometrics.

To ensure that each person in a database is unique, ID systems can use biometric identification to perform a duplicate biometric enrollment check.

The biometric data for the child must be uploaded when they turn five years old, and the identity re-registered at age 15.

There are three categories of people that present difficulties for biometric recognition, including: People who cannot physically provide an acceptable biometric (e.g., amputees, survivors of leprosy, etc.) to enroll in the first place  
  
People for whom acquiring reliable biometric samples is difficult (e.g., manual laborers, elderly people, children, people with visual impairment, persons with albinism, etc.) which could make enrollment or authentication difficult  
  
People who decline to provide their biometrics (e.g., because of religious or cultural constraints, such as the appropriateness of data capture techniques that require physical contact to get accurate readings)

This involves comparing a template generated from a captured biometric against all or a subset of templates stored in biometric database to detect a duplicate registration (a 1:N search), after which the new template is added to the database.

Practitioners will also need to make related decisions regarding the technical standards used for biometric recognition, as well as back-end systems used for biometric deduplication.

Comparison of biometric technologies commonly used in ID systems Finger Iris Face USE Number available 1-10 1-2 1 Ease of capture

Biometric recognition has rapidly proliferated in modern ID systems in part because it is currently the most accurate and efficient technology available for deduplicating large populations to ensure statistical uniqueness—particularly in countries without existing authoritative sources of identity information—and because it can provide a relatively high level of assurance during authentication.

For authentication, there must be alternative methods of proving someone’s identity when biometric verification fails or is not possible, in order to ensure that people are not denied access to rights and services for which they are eligible and entitled.

Biometric deduplication may be the best solution to establish uniqueness in large population, however, not all biometric modes provide the same level of accuracy.

This section provides a brief comparison of the primary biological biometrics used in national-scale ID systems for biometric recognition.

This involves a one-to-one (1:1) comparison of a template generated from a captured biometric against a single stored template (e.g., one stored on an ID card or mobile phone, or in a database).

More data points (e.g., fingerprints and iris scans or fingerprints and face) help ensure statistical uniqueness to a higher degree of accuracy, which may be necessary in large populations (see Gelb & Clark 2013b)

As shown in Table 28, different biometric modes vary in terms of their: Accuracy .

Types of biometrics Countries that plan to use biometric recognition for deduplication and/or authentication can chose from a variety of biometric characteristics (i.e., “modes”).

Indonesia’s population register (SIAK) covers all ages, however biometrics are collected at age 17 (or younger for married women) for the issuance of a national ID smartcard (e-KTP).

In addition, a more comprehensive ID4D Guide on Biometrics is forthcoming.

Peru’s ID system also collects infant biometric information (such as footprints and a photo) in combination with parent’s fingerprints.

The use of biometrics creates additional risks to privacy and data protection that must be mitigated through legal, technical, and operational controls.

Other groups with difficulties Manual laborers, persons with disabilities, people with cuts on their fingers, people with diabetes May be more invasive than fingerprints, stigma in some cultures; difficult for persons with visual impairments or albinism Not always optimized for recognition of darker skin tones, some algorithms have difficulty for persons with albinism Source: Adapted from the Digital Identity Toolkit and Technology Landscape for Digital Development, and informed by expert consultations.

In practice, many countries adopt a multimodal strategy and collect more than one type of biometric data.

The choice to use biometrics—as well as the particular type of biometric data collected—should be informed by these risks and costs, as well as the objectives, planned use cases, and other constraints to the ID system identified in the planning phase.

More modes can help increase the possibility that all members of the population are able to provide a biometric sample (e.g., fingerprints may be difficult to collect for manual laborers, but iris scans may work).

Countries may also implement a mandatory renewal period in order to update children’s biometrics and other information.

For example, there are specific groups and conditions—both of which may be overrepresented in developing countries—where FTE errors during enrollment and FNMRs during biometric verification are likely to be more common.

Given that it is currently not feasible to capture stable biological biometrics at birth—nor are there yet clear use cases as part of a foundational ID system—countries have a few options for the use of biometrics for children in an ID system.

Biometrics can add significant costs to registration as well as the authentication infrastructure.

Challenges for accuracy and inclusion In deciding the set of biometrics to use, special attention needs to be given to the ability to collect these characteristics from the entire population.

The choice of which biometrics to use—if any—will have implications in terms of the trustworthiness and inclusivity of the ID system, as well as potential risks.

Biometric data