Key Considerations Before Implementing Biometrics in Banking: A Latin American Perspective

SECURITY THAT ENSURES DATA PRIVACY AND FACILITATES CONVENIENCE.

Latin American banks are dealing with a multitude of challenges. First, government regulations and safeguards like anti-money laundering laws (AML) and Know Your Customer (KYC) are increasing the complexity and security of bank transactions. Compounding these regulations are dramatically high fraud rates for both customers and employees. All of these point to the need for reliable and highly secure authentication, but they often come at the cost of customer satisfaction and user experience.

Most identity authentication verifies a combination of something you know, something you have and something you are. “Something you know” is most often a password or PIN. “Something you have” is likely an ID or other credential. The problem with these two is, of course, that they are very easily lost, stolen, shared, compromised. For example, employees can share credentials and customers often forget passwords and PINs, resulting in increased IT costs and frustration, as well as lowering productivity. In addition, most passwords and PINs are easily guessed and stolen through no fault of the bank — but the end result is a stain on the bank’s reputation and a costly remediation.

Fingerprint biometrics, on the other hand, offer highly secure and convenient authentication for both bank employees and customers. As banks throughout Latin America implement biometrics programs, others are left to wonder where to begin. This white paper is an excellent first step and will cover six key concepts to consider before beginning a biometrics program.

CONSIDER FLEXIBILITY AND RANGE OF USES.

Will a one-size-fits-all reader meet your institution’s needs? Or do you have multiple use cases requiring different technology?

Ideally, each of your biometric readers is the perfect fit for its individual location, level of monitoring and security needs. A flexible provider with a broad portfolio can determine which reader works best in every scenario, but generally speaking there are three types of fingerprint readers:

**Optical:** Optical readers work like a camera, capturing an image of a fingerprint’s ridges and whorls as it is pressed against the sensor. Most fingerprint standards are based on optical readers, and these readers work with many other products in many industries. Optical readers are most often used at teller and POS stations.

**Capacitive:** Capacitive readers use electrical charges against a fingerprint on the reader’s surface to measure more accurately than optical readers. These are often used on mobile devices and on POS stations.
**Multispectral:** Multispectral readers send light past a fingerprint’s surface layer in the next few layers of skin. Since it measures density beyond the surface, it accurately prevents spoofing, the use of false fingers or overlays. These also offer the lowest false rejections, are the most durable option and the most secure — they’re also often the most expensive.

**CONSIDER THE CAPTURE ENVIRONMENT.**

*Will your fingerprint readers be used indoors or outdoors? Will they be attended (next to a teller) or unattended (at an ATM)?*

A fingerprint reader’s location and exposure determine durability needs. For example, an ATM by the beach faces a constant onslaught of ultraviolet rays and the highly corrosive effects of saltwater. Since it’s unattended, it also needs to be simple to use, with a minimum of rejections, and include fraud prevention. This reader may also benefit from a protective coating and tamper-proof housing. Here, the value of a capacitive reader, which works better in direct sunlight, should be weighed against a multispectral reader, which provides the highest security and durability.

On the other hand, a fingerprint reader at a bank teller’s workstation enjoys a climate-controlled home away from the elements. It may not need liveness detection, since a teller observes all transactions and is likely to question someone placing a fake finger on the pad.

Authenticating employees could also require less extensive protocols. Workstations often use multi-factor authentication (MFA) including more than one factor; for example, logging onto a computer may require a password plus a fingerprint scan.

**CONSIDER SOFTWARE UPDATES AND SECURITY.**

*Will it be easy or costly to update the software supporting your biometric technology?*

Most organizations focus on the hardware requirements of biometrics. While it’s true that hardware is critical, the method in which the software is updated and kept secure is equally important — especially when you are deploying hundreds of readers.

Some biometrics providers require every update be requested and installed individually on each machine. Other providers offer virtualization, where information like updates and enhancements is pushed to the device automatically, without requiring manual installation.

With thin client virtualization, one server runs many — even thousands — of applications and desktops. This dramatically reduces capital and operating costs thanks to fewer licenses and helpdesk calls. It’s also easier to manage, freeing IT departments and swiftly provisioning applications and resources, where local systems often require technical teams to be onsite for each device. Most notably for banks, this system is more secure, since applications, files and customer data are never transmitted or stored on a device.

Not all thin client solutions are created equal, however. Many require a guaranteed bandwidth for streaming, while others send only one image at a time to the server. Also consider interoperability; HID Global’s software development kits (SDKs) enable the use of any device or reader without requiring you to rewrite your software.
CONSIDER CLEANING AND SANITATION.

Can your equipment be cleaned easily and remain functional?

Some biometric readers have elaborate cleaning protocols or require specific solutions or cloths. These finicky products don’t handle high alcohol content well and often raise maintenance issues when cleaned inappropriately. Others work well with standard cleaning materials bought off the shelf, with no special products.

Cleaning teams tend to use whatever they’re already using to clean, from a highly disinfecting product with 70% isopropyl alcohol to cleaning wipes. Health-conscious customers will also use whatever they have on hand. It’s nearly impossible to tell either of these groups to only used approved cleansers, despite the high cost of repair and maintenance others cause. Avoid future problems by selecting hassle-free readers.

CONSIDER YOUR RETURN ON INVESTMENT.

Will your equipment be functional and secure for years to come?

Every new system should be measured not only by its immediate impact, but its future as well. Work with a provider offering flexible solutions; many banks begin using readers with simple technology in most locations and multispectral in only the most sensitive areas. This helps a bank step into the world of biometrics slowly, eventually upgrading seamlessly to more advanced technology. Some may choose to begin with employee authentication before launching into ATMs and customer account verification. The best providers offer a diverse portfolio even within brands, ensuring a strong and perfect-fit relationship for years to come.

Also take care when selecting readers for particular locations. As stated above, outdoor readers at the mercy of the elements should be highly durable, with a rugged housing and a reader that can withstand plenty of touches. Will users have difficult to read fingerprints, whether oily, dry, damaged, wet or aged? Reduce the cost of service calls and customer frustration by investing appropriately.

CONSIDER IMPLEMENTATION AND LONG-TERM SUPPORT.

What happens when you have issues and concerns?

Will your provider help you find the best product for you — or themselves? Engaging in biometrics is a long-term relationship, and your provider’s willingness to truly problem solve and listen from the very beginning is key to the system’s success.

Also consider what happens after your biometric readers have been installed. While most providers offer service packages, the including service may not meet your needs. Look for those with a strong regional presence and understanding, with local technicians that speak the language to reduce mistakes in translation. Ask whether issues or concerns are related to a specific person or a large call center, and whether both technical and sales support are live.
Biometrics offer secure and convenient customer and employee identification. This next-level authorization tool isn’t a futuristic dream. It is already being used in banks throughout the world — and will soon be expected by discerning customers concerned with the ever-present threat of fraud.

Unfortunately, choosing a biometrics provider can be difficult, thanks to different standards of service, security, software and simplicity. Considering the above issues during the selection process ensures success from the start and sets you on the path to a more secure, simpler future.

With a broad portfolio of biometric solutions and deep expertise in the world of identity management, HID Global is available to help at any stage of your biometric journey.

*Discover our portfolio of readers and embedded modules and how biometrics are helping to solve fraud in banking in our white paper, *Trusted Identities: Solving Fraud in Banking.*