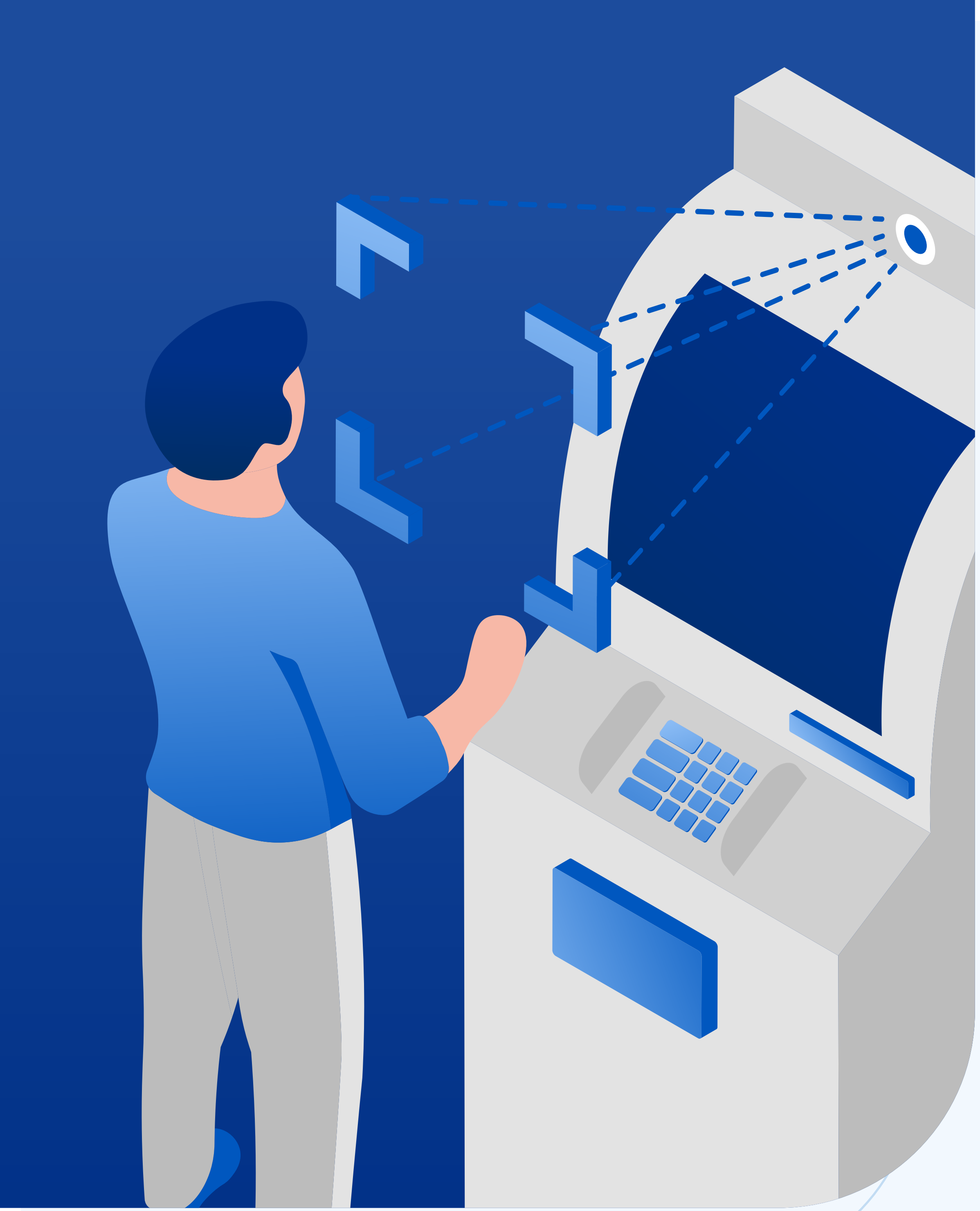
Improving the ATM Experience **With Biometrics Multi-Factor Authentication**

EBOOK



The Challenge of Authentication at the ATM

ATMs in the U.S. and other parts of the world have generally validated the identity of bank customers with something the user has (a card) and something the user knows (a PIN). This decades-old approach is increasingly vulnerable to fraud attacks.

As the banking industry continues to search for ways to shore up security, some measures — such as a credit card with an embedded microchip — effectively address certain aspects of the fraud problem. But only biometrics can answer the question of ***who*** is actually transacting and determine whether it is a legitimate bank customer or a fraudster.

Biometrics: Keeping Balance Between Convenience and Security

By binding a unique individual to his or her true identity, biometrics go beyond what the user has and knows to provide the only means of determining ***who*** is actually using the system. It eliminates the hassle and security risks of PINs and passwords while simultaneously making it easier to confirm if someone is who he or she claims to be. With nothing to carry or remember, biometric security is also inherently more convenient for the bank customers, allowing seamless access with the touch of a finger or the snap of a selfie.

Biometrics are the only true means of making security more convenient while also linking or binding digital identities to the individual — determining who is actually using the system and verifying whether they are a legitimate user for a myriad of new mobile and online applications beyond the ATM. When a biometric solution includes the ability to distinguish live fingerprints and faces from fakes and masks through liveness detection, concerns about privacy and identity fraud are assuaged.

Since 2016, the number of ATMs that leverage fingerprint biometric authentication in South America began to challenge those without biometrics. Brazil, which boasts a high level of adoption, has approximately 190,000 ATM terminals, 90,000 of which utilize fingerprint biometric technology. HID Global's multispectral imaging (MSI) fingerprint readers account for at least 60,000 of that number, biometrically securing more than one billion ATM transactions each year in Brazil alone.

ATM Banking With Biometrics Multi-Factor Authentication

Initially, thanks to its low cost and high performance, fingerprint biometrics dominated the biometric ATM landscape. But recent advances in matching algorithms and camera technology have allowed facial recognition to enter the arena too, enabling an additional ultra-convenient layer of security.

Of course, with new technology adoption comes new risks. As biometric applications become increasingly widespread and are relied upon for securing personal transactions, deployed solutions are likely to be targeted for attack. Consequently, it is becoming increasingly important for those deploying biometric authentication to understand that not all biometric devices and solutions are created equal.

Requirements for Successful Biometric Implementation

Fingerprint and face biometrics are a powerful combination at the ATM. Not only do they boast the unmatched security of multiple biometric factors, but they are also complementary in nature when it comes to user experience. Face recognition is a passive and contactless biometric that identifies and authenticates users automatically without adding any friction to the user experience. Meanwhile, fingerprint recognition requires a user to actively present his or her biometrics to the sensor, making it the perfect method for users to sign off on transactions, confirming consent and authenticating their identity with a single touch.

Regardless of the biometrics being used, best practices should be observed for the successful implementation of a secure, convenient and trusted authentication solution. Key focus areas should include the following:

1
Biometric Sensor Reliability

2
Liveness Detection

3
Tamper Protection and Trusted Connections

4
Knowing Your Customer and Protecting Their Privacy

1

Biometric Sensor Reliability

Biometric sensors need to be capable of working reliably under the broadest range of real world conditions. To solve this problem, HID Global uses multispectral imaging (MSI) technology to ensure that unique biometric characteristics can be extracted from both the surface and subsurface of the skin. Pioneered by HID's Lumidigm® fingerprint sensors, MSI technology uses multiple sources and types of light along with advanced polarization techniques to capture information from deep within the finger — all the way down to capillary beds and other sub-dermal structures.

The advanced functionality of MSI is no longer confined solely to the fingerprint — **HID Global has expanded MSI technology to include face biometrics.** Combining MSI with advanced camera sensing technologies, HID's camera can identify customers in direct sunlight or complete darkness, addressing lighting challenges for ATMs. Because it scans a user's face using color (RGB), Near Infrared (NIR), 2D and 3D imaging, it can't be fooled by impostors using photographs, videos on phones or even realistic masks. This means face biometrics are finally robust enough to provide resilient anti-spoofing capabilities and protect all ATM transactions.

2

Liveness Detection

Security is an arms race, and when it comes to biometrics, it's being fought between presentation attacks — spoofing — and liveness detection. In a presentation attack, a fraudster uses a fake fingerprint, a mask or a high-definition photo in order to fool a biometric sensor into authenticating them. **Liveness detection is a layer of protection against these spoofs.**

In addition to the anti-spoofing characteristics inherent to MSI technology, which scans fingers and faces with multiple imaging technologies, HID's hardware includes field-updatable liveness detection capabilities. Combining MSI with advanced machine learning algorithms, HID's liveness detection can be updated as new threats and spoofs are identified, enabling fingerprint readers or facial recognition cameras to very quickly respond and adapt to emerging threats.

3

Tamper Protection and Trusted Connections

Every new data breach serves as a reminder that all user data is valuable and private. A biometric device must therefore be both tamper resistant and able to connect to a financial institution's systems through a cryptographically secure channel. Device authentication and secure encryption of data-at-rest, as well as in transit between the biometric device and the institution's IT systems where data is stored, ensures that customer data and financial transactions are conducted over a truly secure connection.

HID Global's biometric solutions that support this combination of tamper protection and trusted endpoint connections have been successfully deployed in ATMs worldwide, protecting billions of ATM transactions annually.

4

Knowing Your Customers and Protecting Their Privacy

Banks need to know who their customers are, and they need to protect their personal information. Meeting Know-Your-Customer (KYC) regulations in today's digital world is made easy with HID Global's eKYC solution that leverages facial biometric and document authentication for secure mobile enrollment. The backend HID biometric server — which can be deployed on premise or in the cloud — facilitates the matching at every customer touchpoint: mobile banking, at the branch or at the ATM.

Every user is anchored with an irrefutable trusted identity thanks to the eKYC onboarding process, and the dual-biometric authentication (face and fingerprint) used at each subsequent transaction ensures the highest level of trust is carried forward in an unbreakable chain.

When it comes to privacy, this means no one but a user can gain access to his or her data. No more vulnerable cards, passwords, PINs or security questions means that fraudsters are out of luck.

Conclusion

The goal of any transaction at the ATM is to conveniently provide bank services while ensuring the identity of the individual to whom the service is being provided. Managing risk is a matter of balancing and, ideally, combining security and convenience. Dual biometric authentication provides this capability with the highest level of certainty.

We all have only one true identity, and this identity must be protected in a sensible, balanced and efficient way. There are no longer valid technical or business reasons to rely on outdated security systems and practices. **Biometrics offers us the ability to make productive use of the myriad of digital credentials that we use and manage today — and to do so in a manner that is more secure and convenient, and actually protects our identity.**

We no longer have to choose between greater security or convenience. With biometrics we can have both.

Biometrics
for the ATM Experience

Combining fingerprint and facial recognition allows rapid and secure access to ATMs. This is a profoundly positive user experience as it meets the intrinsic needs of the customer: convenience and security.

Discover better banking with biometrics:

Website | Biometric Banking Revolution

eBook | Better Banking Experiences Start With Strong Authentication and Face Biometric

Infographic | Here's Why Your Bank Needs Biometrics hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 (55) 9171-1108

For more global phone numbers click here

2021-12-22-eat-improving-atm-experience-with-biometrics-multi-factor-authentication-eb-en
PLT-06359

Part of ASSA ABLOY