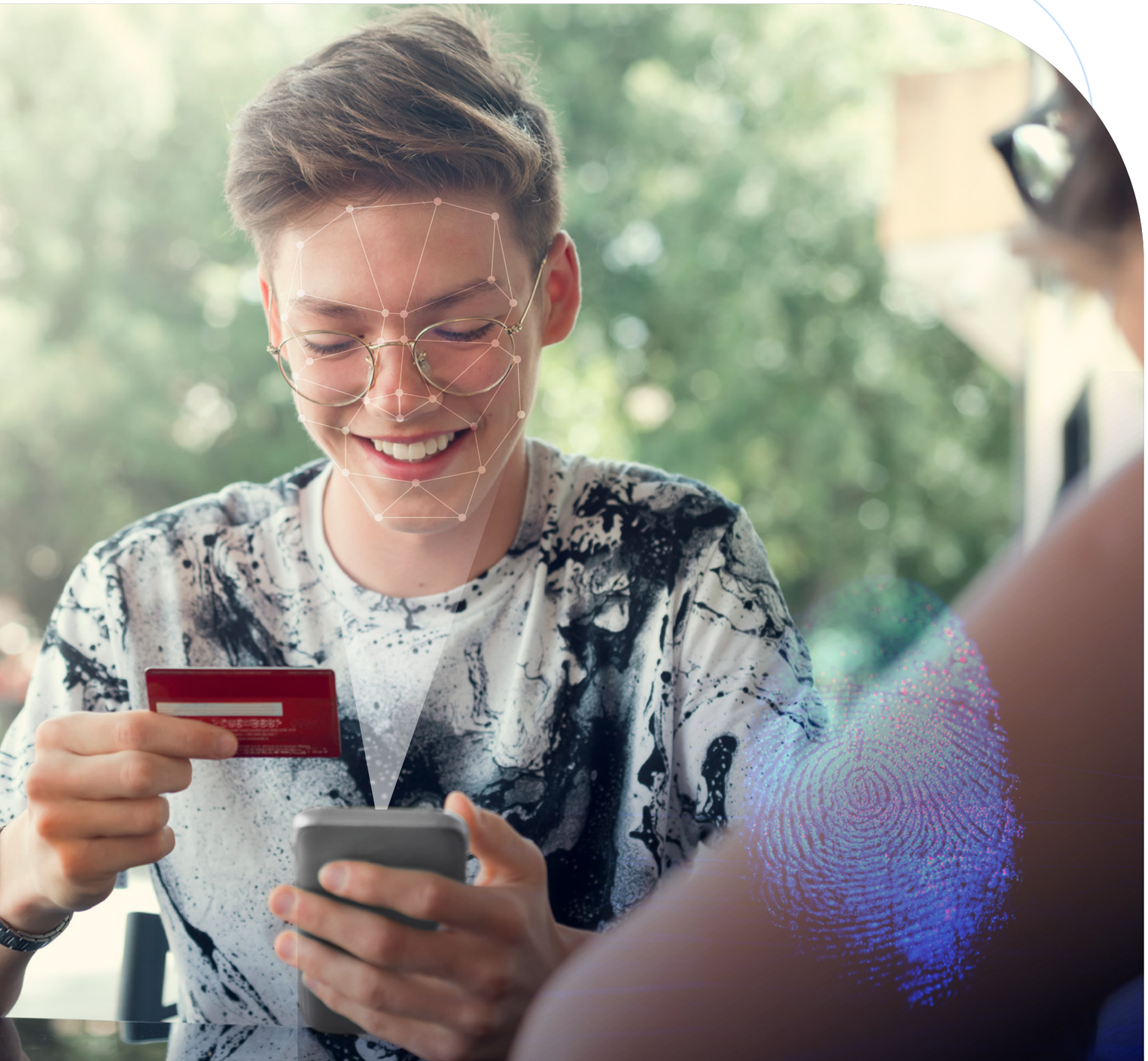
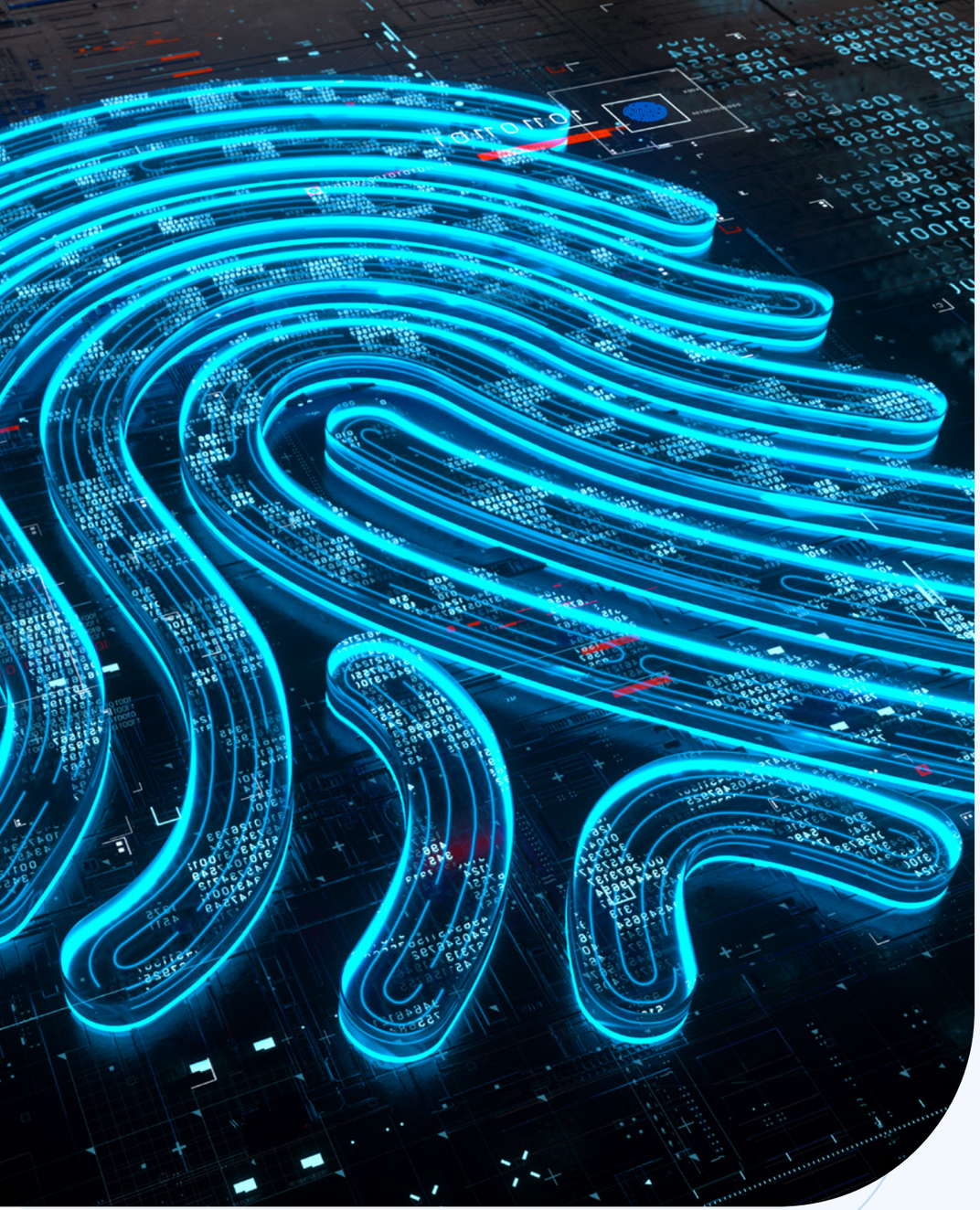


Solving Fraud in Banking
With Trusted Identities

EBOOK



One of the biggest challenges facing banks today is providing secure and trusted services while substantially improving the customer experience.

Bank customers are demanding a seamless and secure experience across all service channels. But increases in service and convenience through technology can create additional opportunities for fraud and identity theft. **Any increase in convenience must be balanced with an increase in security.**

Biometrics have long provided a reliable means to establish authentication of a true identity. **And the latest advances in face recognition in particular have enabled a premium customer experience while also increasing security across all bank systems and service channels.**

Multiple Channels, Multiple Vulnerabilities

Today's banking landscape is characterized by a patchwork of technology systems, each assembled and deployed separately, often by different organizations within the financial institution. To bank customers craving simplicity and a trustworthy transaction environment, the fragmented experience is frustrating. Meanwhile, to those seeking to defraud the bank and its customers, there are many new opportunities that have led to a growing number of hack attacks and data breaches.

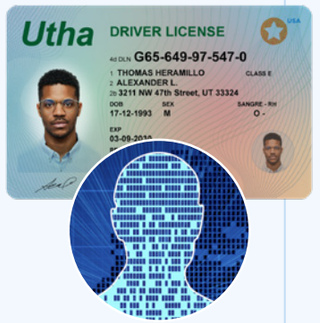
The solution required is an integrated multi-channel identity and access platform that improves the user experience, enables mutual trust, meets compliance requirements, reduces complexity and lowers the total cost of ownership. Biometrics are at its core.

The Promise of Biometrics

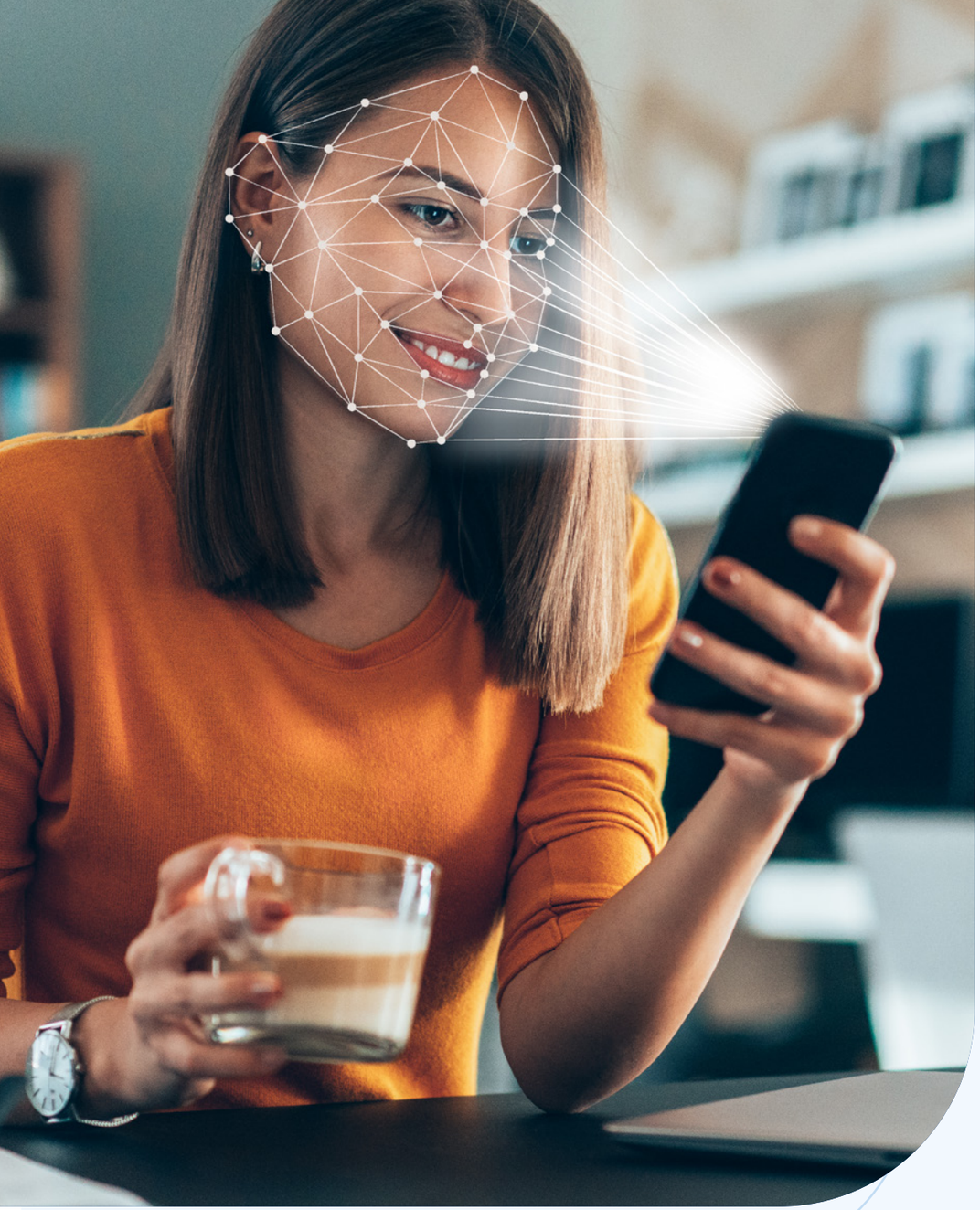
Biometric authentication plays a critical role in delivering trusted identities, because only biometrics can directly confirm you are who you say you are. **Biometrics provide the means to unambiguously validate an identity claim, and can achieve this while eliminating the cost, complexity and vulnerabilities of other identity authentication methods.**

In order to **eliminate identity theft and fraud**, it is imperative that we distinguish between:

The use of biometrics as an **authentication factor:**
Biometrics can be used as effective authentication factors because they are unique to each individual. If you scan your face to gain access to your smartphone, you are proving you are the one that matches the enrolled template. Biometric authentication can take place independently of true identity.



The use of biometrics to prove a claim of **true identity:**
When biometrics are used to assert true identity, they are supported by government-issued identification data. If you biometrically match your face to the photo image on your passport or driver's license, you are proving that the identity represented on that document is yours. The same is true if your biometrics are being utilized as part of an in-person or remote identity-proofing process.



Biometrics as an Authentication Factor

Let's consider the example of biometrically-enabled smartphones. Today, a person can take a selfie and bind their smartphone to their face with a credit card and a billing address. This mobile device can then be associated with multiple payment accounts, all tied with the captured face biometric.

The result is a convenient way to perform "card not present" (CNP) transactions both online and at retail stores. In this smartphone scenario, the face biometric was not used to verify a claim of **true identity** – it was simply used as a credential to replace a PIN or password on the device. The transaction is certainly more convenient, but it is less trustworthy than an in-person transaction with a card — opening the door to fraud.

What is needed is **an unbroken chain of trust** for transactions that are based on verifying a claim of **true identity**, rather than simply verifying ownership of a digital identity that someone might be using fraudulently. This can be accomplished by verifying the face biometric to a government-issued credential such as a drivers license or a passport at the time of binding the smartphone to the user.

True Identity and the Chain of Trust

The previous example lacks an initial claim of true identity to act as the foundation for subsequent transactions. That initial claim of identity — otherwise known as a trust anchor — previously required an in-person identity proofing process in which a user would enroll biometrics at a bank branch. While this offered extremely high levels of trust, it was prohibitively inconvenient.

Thankfully, advances in mobile biometrics have given rise to a remote trust anchoring solution that is taking the world by storm: eKYC (Electronic Know Your Customer).

To anchor trust remotely, one simply has to use their smartphone to take a picture of their government issued ID — like a driver's license — and a selfie. Document reading software verifies the ID, while biometric matching compares the selfie to the photo image of the document. State-of-the-art liveness detection and anti-counterfeiting measures ensure the software isn't being tricked into a false positive. The result is a representation of true identity that can be referenced for subsequent transactions, created from the comfort of your home.

More Biometrics Mean
More Security

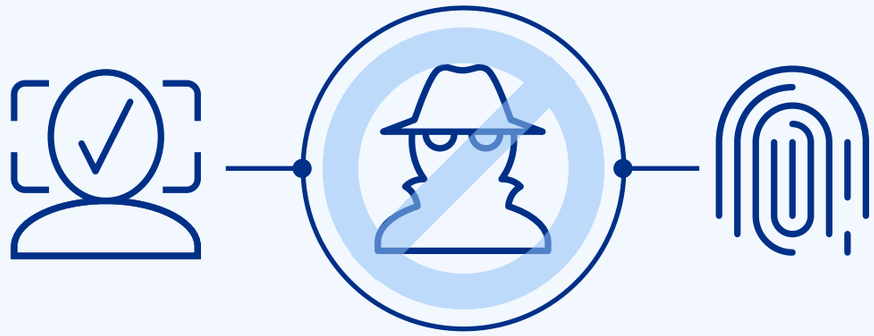
With HID Global's comprehensive multi-factor biometrics solution, a customer's true identity only gets stronger over time. Once a trust anchor is created with a selfie and an ID document, a user can add his or her fingerprint to their account. Bank customers can use their face to validate presence and identity, and the touch of a finger to validate intent to sign. With two biometrics anchored to a bank account, the level of trust is strong enough that a user doesn't even need to bring a card to ATMs or bank branches — they just need to be themselves.

Eliminating Fraud With Biometric Multi-Factor Authentication

Now imagine opening a banking account with that trust anchor in place. The strong association of a person's true identity during account creation, and each subsequent transaction, delivers a high level of trust in a manner that is very resistant to identity fraud and theft.

With this increasingly popular approach — establishing true identity in a manner that can be independently verified not only at account creation but at each transaction — identity theft and fraud can be eliminated.

But a trust chain is only as secure as its weakest link. **We need to shift our attention from weak authentication factors like PINs and passwords to a focus on the viable ecosystems that can now support the establishment and proof of true identity.** Multi-factor biometrics satisfy the criteria, and they are available right now.

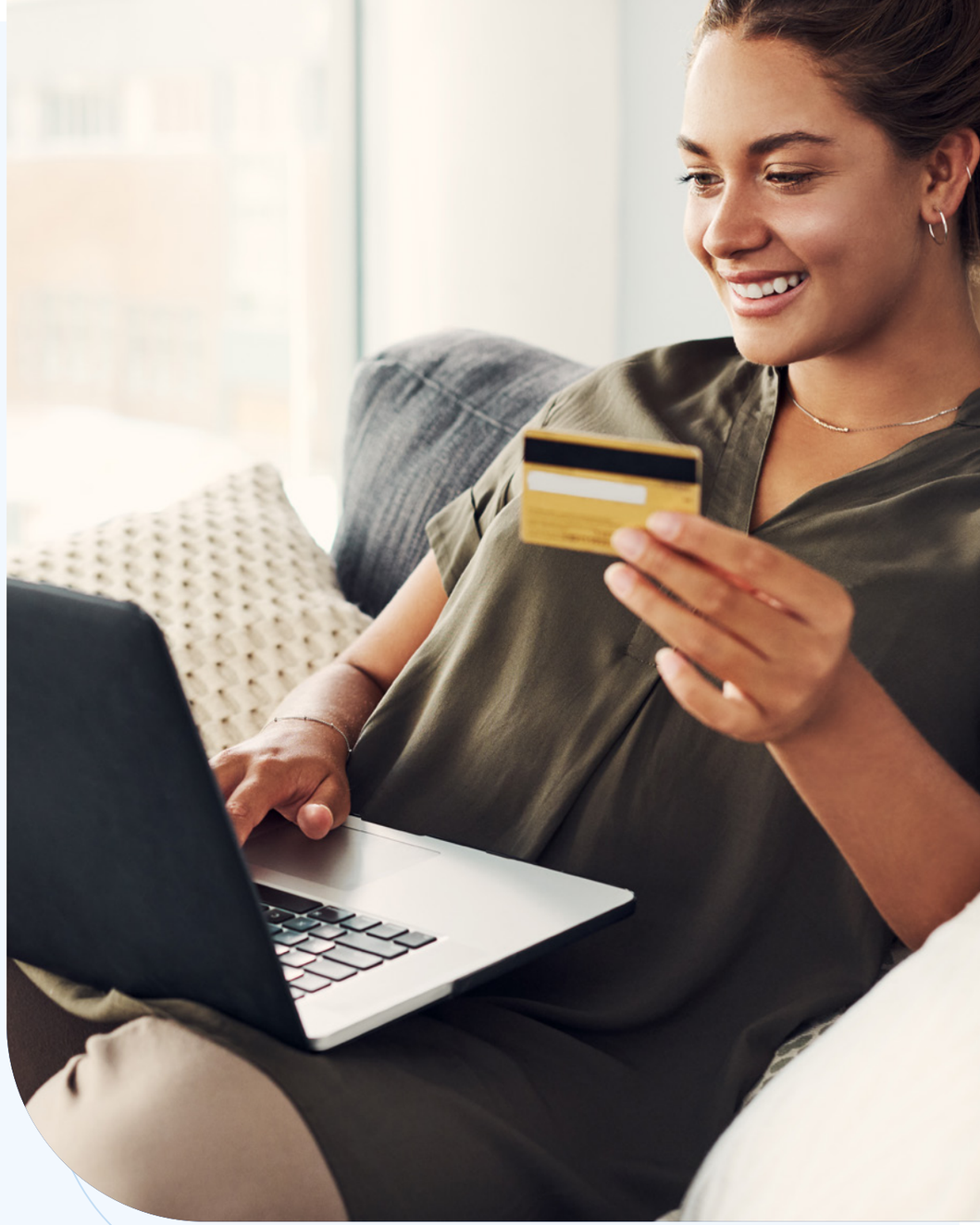


What's Next

The financial industry is at the forefront of implementing biometrics. HID Global's biometric solutions are a big part of this adoption curve, with more than 81 million Brazilian bank customers using biometrics to authenticate over one billion transactions per year.

But to fully realize the short- and longer-term benefits of biometrics, there must be an integrated platform that recognizes true identities from establishment to authentication — a chain of trust. **Biometric solutions will greatly improve the customer experience while increasing trust and lowering costs if they include mobile-relevant, multichannel-capable identity and access management approaches that are secured end-to-end and are easy to buy and to deploy.**

The opportunity to deliver a game-changing user experience across all banking channels is here. By leveraging biometrics for identity authentication, banks can empower users to bank wherever, whenever and however they want — protected by unbreakable trust chains. Combining biometrics multi-factor authentication with mobile certificates, document authentication, deep learning and other technologies enables banks to create an environment in which there is no requirement for a bank customer to do anything other than "show up" for his or her transaction on the mobile phone, at the bank, at the ATM or online.



Biometrics and the Promise **of a Fraud-Free Future**

Using biometrics to verify true identity is as easy as unlocking a phone. It delivers the utmost in customer experience and offers the potential to consign fraud to the pages of history.

Dig deeper into the topic of how financial services providers can use true identity to enable a secure and convenient customer banking experience across all touchpoints:

Website | Biometric Banking Revolution

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

Infographic | Here's Why Your Bank Needs Biometrics

HID

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

2021-12-02-eat-solving-fraud-in-banking-with-trusted-identities-eb-en PLT-06345

Part of ASSA ABLOY