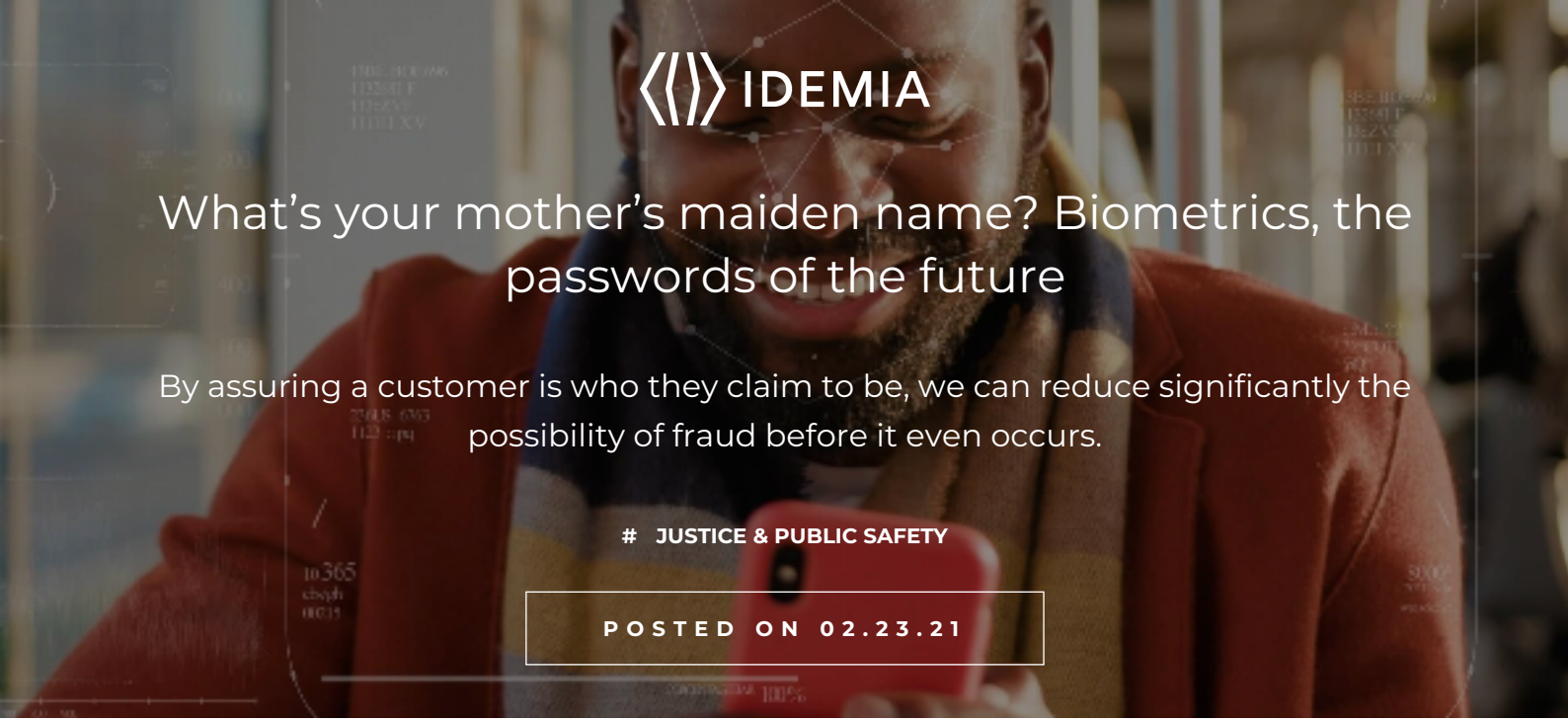
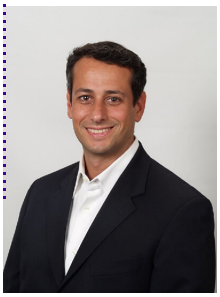


What's your mother's maiden name? Biometrics, the passwords of the future

By assuring a customer is who they claim to be, we can reduce significantly the possibility of fraud before it even occurs.

 # JUSTICE & PUBLIC SAFETY

POSTED ON 02.23.21



In a very near future, biometric-based identity will be the premium alternative to passwords, because it eliminates knowledge-based authentication. This is a major step towards reducing fraud risk.

Alejandro Lopresti, NORAM Regional Sales Director, IDEMIA

The growing acceptance for the use of biometrics on personal mobile devices is expected to create a market worth $68.6 billion by 2025[1] given that 81% of consumers are trusting fingerprint or facial recognition over traditional text-based passwords[2]. In 2023 alone, it's anticipated that 37.2 billion transactions, at a value of $2 trillion, will be authenticated by biometrics[3]. And most of those transactions will be remote – rather than face-to-face.

Today, API-first cloud architecture already enables forward-looking organizations to turn to biometrics use cases. In these cases, biometrics are deployed into the applications thanks to mobile or web SDKs which removes the need to use specific biometric hardware. The application is also connected to an API-based biometric verification service, which performs the matching. This enables enterprises to prepare for a password-less future without calling on significant technical resources or utilizing a lengthy integration process.

In the near future, customers will expect to use **biometric authentication** to access services, rather than typing out a password or entering a PIN. This type of authentication can be applied when accessing online and mobile applications, biometric identity proofing and verification during **digital onboarding**, as well as **physical access control**. In each of these cases, the use of biometrics provides a trusted and frictionless means of authentication that delivers on a stronger and easier security, without introducing any friction or additional security risks.

By assuring the customer is who they claim to be, service providers can reduce significantly the possibility of fraud before it even occurs.

If I know whom I'm dealing with, I'm less concerned about risk. This level of convenience delivers instant customer satisfaction, without sacrificing on security.

[1] Juniper Research: Mobile Payment authentication & Data Security" encryption, tokenization & biometrics 2019-2024: https://www.juniperresearch.com/researchstore/fintech-payments/mobile-payment-authentication-research-report

[2] Biometric System Market with COVID-19 Impact by Authentication Type (Single-Factor: Fingerprint, Iris, Face, Voice; Multi-Factor), Offering (Hardware, Software), Type (Contact-based, Contactless, Hybrid), Vertical, and Region – Global Forecast to 2025- https://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html

[3] Experian's 2020 Global Identity and Fraud Report – https://www.experian.com/blogs/insights/2020/02/experians-2020-global-identity-fraud-report/