aimbrain
simply smarter authentication

BIOMETRIC IDENTITY AS-A-SERVICE (BIDaaS): THE RISE AND RISE OF CLOUD BIOMETRICS

IN THE DIGITAL WORLD, HOW WELL DO YOU **REALLY** KNOW YOUR CUSTOMERS?

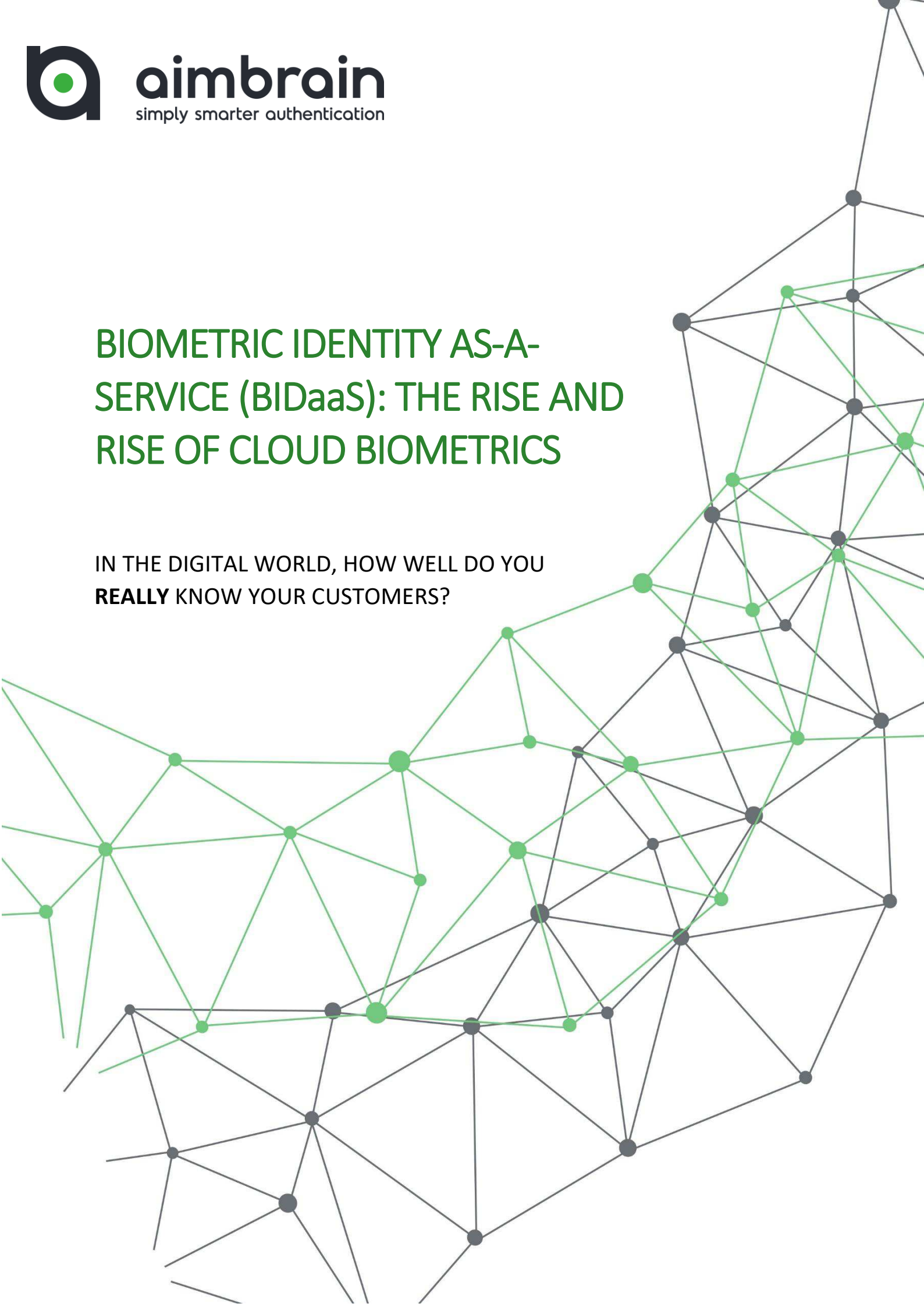


Table of Contents

Contents

Table of Contents 1

Introduction 2

Cloud-based authentication, not simply on-device 3

Step-up authentication, applying the “right” level of friction 3

Simplifying, enhancing and securing the customer journey 3

Omni-channel for fraud reduction and consistency 3

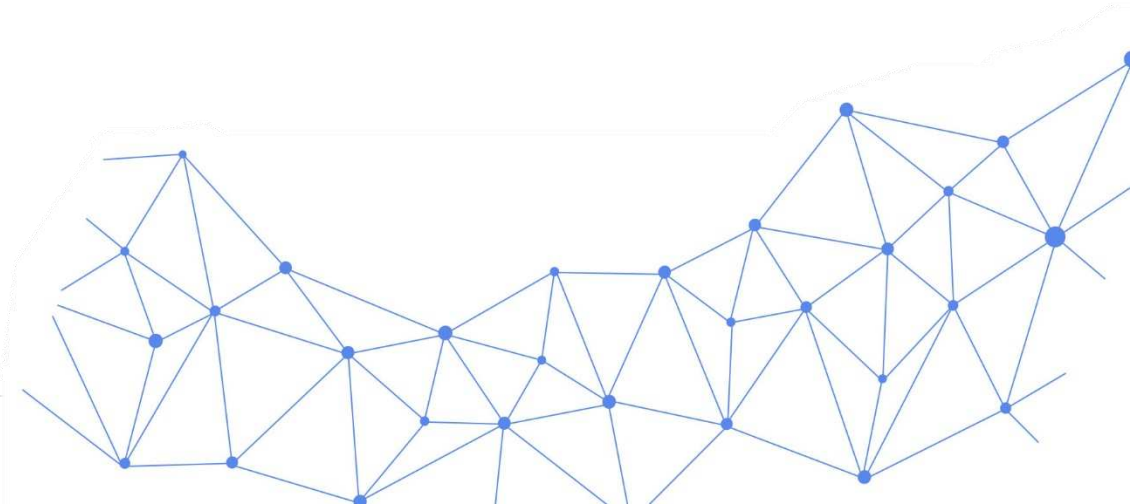
Regulation: PII and lessening the breach impact 3

Deep learning-based profile building 4

BIDaaS and business as usual 4

Conclusion 4

Considering authentication in the cloud? 5



Introduction

Biometric authentication is officially mainstream. Last week, the world watched as Apple unveiled the iPhone X's facial authentication technology, whilst research firm Acuity issued its Global Biometrics and Mobility Report[1], suggesting that within five years, biometric authentication could be enabling 1.37 trillion payment and non-payment transactions.

In both consumer and business worlds, we're seeing a new, voracious appetite for all things biometrics; from facial scans to vein pattern recognition, fingerprints to behavioural monitoring. Apprehension has moved through simple acceptance to something more exciting, as we embrace wearable technologies that measure and monitor us, talk to would-be intruders when we're miles from home, and even pay for our dinner by smiling at cameras[2].

But the true value of biometric authentication is stifled all the time that we restrict the authentication procedure to the devices we use. Using facial scanning technology or fingerprints that match to a biometric template stored **on the device** only serves to link the person to the device. The real value of using biometric authentication will be unleashed when organisations move the process away from the device, to the Cloud.

There are several terms currently in incubation stage for this process, a process that at AimBrain we refer to as Biometric Identity as-a-Service, or BIDaaS.

But why is moving the authentication process to the Cloud more beneficial to keeping it on-device? In this paper, we discuss the benefits of moving server-side.

First Things First: Differentiating between the Cloud and Server-side

An important distinction to make is clarifying what is true BIDaaS or biometrics server-side, and what is cloud-based biometrics. When we talk about BIDaaS, we are referring to when biometric information is acquired on a device, encrypted and sent to a server, where the authentication takes place.

This is not to be confused with some "cloud biometrics" providers that simply authenticate on-device and then launch a cloud services passing on only the results of authentication, and almost always, only in binary form too. So for the purposes of this paper, when we say Cloud-based authentication, we mean biometric authentication that happens away from the device and in the Cloud.

[1] http://www.acuity-mi.com/GBMR_Report.php
[2] https://techcrunch.com/2017/09/03/alibaba-debuts-smile-to-pay/

BIDaaS enables Cloud-based authentication, not simply on-device

"*Device authentication is not identity authentication*", summarises an Acuity report just out[3]. Linking a mobile banking app to a device simply creates a link between the device and the account, and the authentication process reconfirms this link. A BIDaaS platform creates and stores a unique digital template for the genuine consumer which is held securely in the cloud, in the form of a mathematical construct, so that a bank can verify that it is the correct person, not just the correct device, performing a transaction. *Jump to the last page of this report for a quick reference guide of Cloud vs On-Device.*

BIDaaS enables step-up authentication, applying the "right" level of friction

BIDaaS allows the use of passive (behavioural) biometrics monitoring. By combining behavioural biometrics with deep learning, a richer understanding of the user is reinforced with every action, so that step-up authentication is only applied when strictly necessary. This 'appropriate' level of friction works for both the financial institution and the customer.

BIDaaS simplifies, enhances and secures the customer journey

Critical to the long-term viability of a financial institution is its commitment to improving the Digital Journey for its customers. By providing the mechanism to securely store a unique digital template for each of its customers, verified against a vetted identity document, a bank not only enables rapid onboarding and authentication for new customers or existing customers for new products, but can apply passive (behavioural) biometrics all the while a customer engages with the bank. This continual background monitoring ensures that the customer's transactions are safe, and the only time the customer is actively engaged is if abnormal behaviour is detected.

BIDaaS lets a user enrol across multiple channels once, reducing fraud and enhancing the customer journey

When a centralised template of an individual's profile is stored in the secure Cloud, a user can enrol using a single device and that template be used across multiple channels. As the Acuity paper states, "[biometrically-enabled smartphones] will create the opportunity to leverage [Unique Verifiable Identifier] as the basis of authentication for financial services across platforms, modalities, and borders." This both simplifies the customer's journey and eliminates the ability to create multiple identities on a single device; a key indicator of account fraud. Furthermore, the frustration of losing or damaging a device is somewhat mitigated, as the user would not need to re-enrol their biometric information on a new device.

BIDaaS stores biometrics away from personal information, eliminating the risk of total breaches

Acuity's report also refers to the myth of cloud-based security being lower than on-device or on-premise. "Concerns about biometric data storage and management in the Cloud being subject to loss, theft, and potential misuse have been sensationalized", it says. BIDaaS creates and stores a unique, irreversible digital template of an individual on its servers, away from the personal information held on a device or on-premise at an organisation. Performing the authentication server-side using an algorithmic construct rather than information, pictures, passwords or other vulnerable forms is far safer than authenticating on-device, as the template is encrypted, anonymous and impossible to reverse-engineer.

[3] http://www.acuity-mi.com/CloudFS.php

BIDaaS facilitates deep learning-based profile building

Acuity discusses the additional value of adding machine learning to the authentication process, referring to the process of being able to *"continuously improve the ability to recognize individuals and identify fraudsters"*.

Indeed, when authentication happens in the Cloud, it is possible to apply deep learning techniques using a backdrop of millions of records, to identify unique patterns and improve user recognition on a continual basis. The scale of learning potential is simply not possible, on the device or even on-premise.

BIDaaS lets an organisation get on with its core business

AimBrain is an expert in biometrics and server-side authentication. BIDaaS means that a bank, payments provider, corporate or other organisation can focus on its key strategies without the concern of data storage, hosting, maintenance or breaches. Financial institutions can now exploit the power and security of their own BIDaaS platform through easily-deployable SDKs and API plug-ins.

Conclusion

Biometrics will become ever more prevalent, and not just within the financial services sector. As we move towards an increasingly mobile society and business transactions take place without face-to-face meetings, biometric identity authentication will become more and more commonplace. Organisations that use biometric authentication server-side will be able to onboard quickly and securely, minimise unnecessary friction, comply with anti-money laundering best practices and at the same time delivering a kick-ass experience.

Given the growing appetite that the general public now has for biometric authentication, BIDaaS will add the much-needed authentication of an identity alongside the existing authentication of a device. It provides that much needed inherence factor to the current factors of knowledge and possession, adding to **something I have** and **something I know** with the crucial irreplaceable factor; **something I am.**

When a bank truly knows who its user is, they can provide the optimum experience for that person; a safer, more personalised experience across any channel, with just the right amount of friction to keep their customer's data and assets secure.

Cut Out & Keep: Your Guide To Being An Authentication Rock Star

1. **CLOUD-BASED BIOMETRIC AUTHENTICATION FACILITATES CROSS-CHANNEL, CROSS-DEVICE ACCESS.** Customers can enrol voice, facial and behavioural biometric information from a single device, applicable across multiple channels, devices and applications.

2. **CLOUD-BASED BIOMETRIC AUTHENTICATION DECOUPLES AUTHENTICATION FROM THE DEVICE, FOR ENHANCED SECURITY.** Using device based biometrics to unlock a device, then using the same device to receive an additional code is little more than an approximation of identity, not a true link between the user and their individual biometric profile.

3. **CLOUD-BASED BIOMETRIC AUTHENTICATION BENEFITS FROM SECURITY-SPECIALIST BEST PRACTICES.** By using identity security specialists, banks reap the benefits of the vendor's focused expertise of industry-leading security practices.

4. **ON-DEVICE BIOMETRICS DO NOT WORK TO ACCEPTABLE ACCURACY WITH MAJORITY OF DEVICES.** Most of them are way too weak computationally, energy-wise and memory-wise, to run the required algorithms.

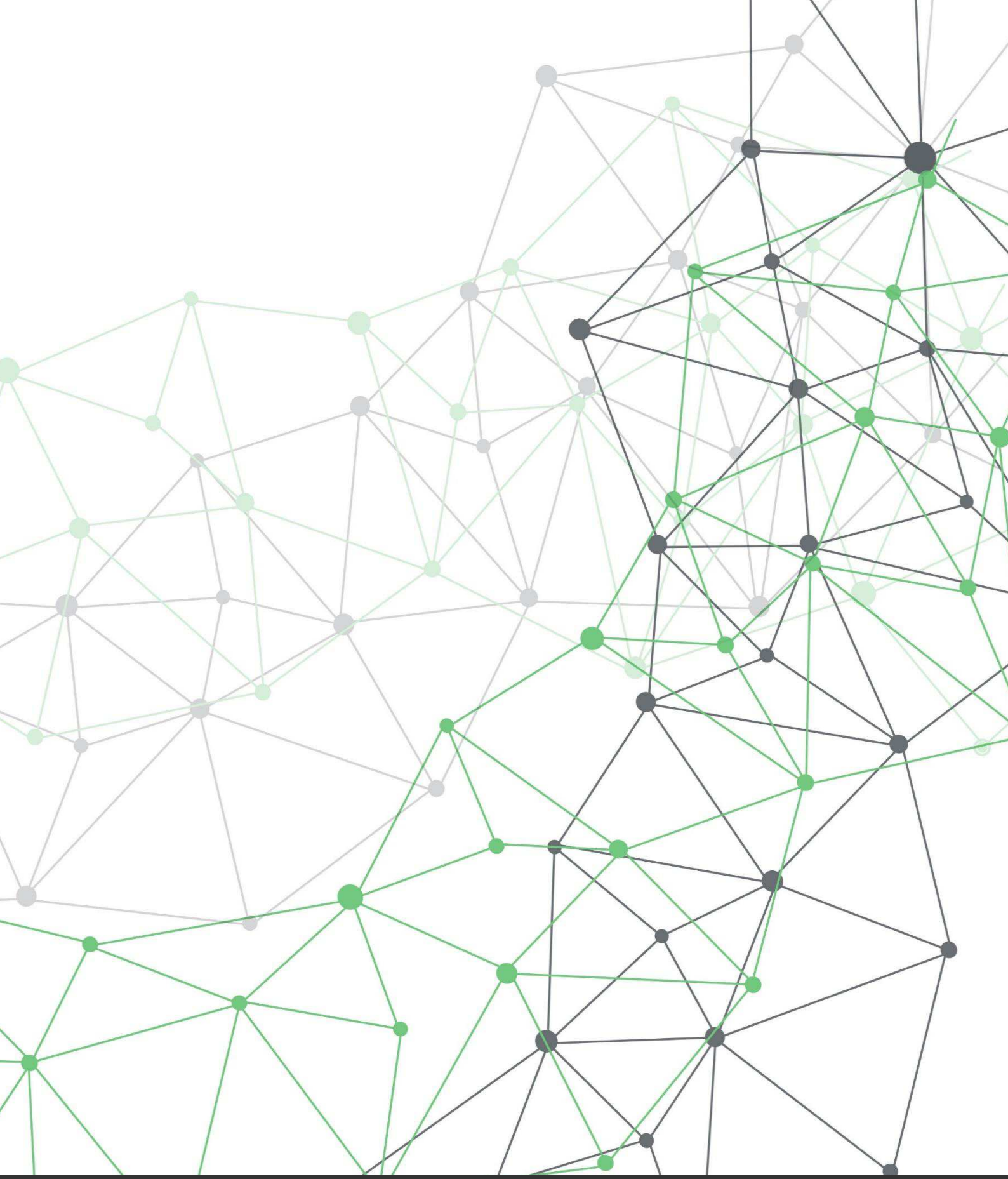
5. **UPDATING THE ALGORITHMS BEHIND CLOUD-BASED AUTHENTICATION IMPROVES ACCURACY, QUICKLY AND EASILY.** On-device, this would be an extremely long and painful process.

6. **CLOUD-BASED BIOMETRIC PLATFORMS BENEFIT FROM ECONOMIES OF SCALE;** each and every new client improves accuracy for everyone else.

7. **CLOUD-BASED BIOMETRIC AUTHENTICATION FACILITATES NEW FEATURES, FASTER.** Features such as liveliness detection, or improved accuracy under extreme lighting conditions, can be rolled out instantly, and customers can immediately reap the benefits.

8. **CLOUD-BASED BIOMETRIC AUTHENTICATION ALLOWS THE SAFE AND RAPID ONBOARDING OF "UNSEEN" CUSTOMERS** by leveraging KYC documents, national identity documents or governmental data.

9. **CLOUD-BASED AUTHENTICATION OFFERS EXCEPTIONAL DATA SECURITY BY STORING DATA IN NON-REVERSIBLE, FULLY REVOCABLE TEMPLATES**. This means that even if a vendor or service provider experiences a full systems breach, sensitive data could not be accessed or leaked, as digital templates are non-reversible and allow for instant invalidation or revocation.



- **news@aimbrain.com**
- **aimbrain.com**
- **AimBrain, Level39, One Canada Square, E14 5AB**

aimbrain
simply smarter authentication

AimBrain is a BIDaaS (Biometric Identity as-a-Service) platform for global financial institutions. Our approach to BIDaaS uniquely combines voice, facial and behavioural biometrics with cloud-based authentication to verify an identity, unlike traditional implementations of PINs, tokens and even fingerprints that simply confirm the link between the individual and the device.

We have the industry's only cloud-based, multi-module identity authentication solution that combines both passive and active biometrics, using voice, facial and behavioural. Our technology is underpinned by a proprietary deep learning engine, designed to build an increasingly accurate profile of a user over time.