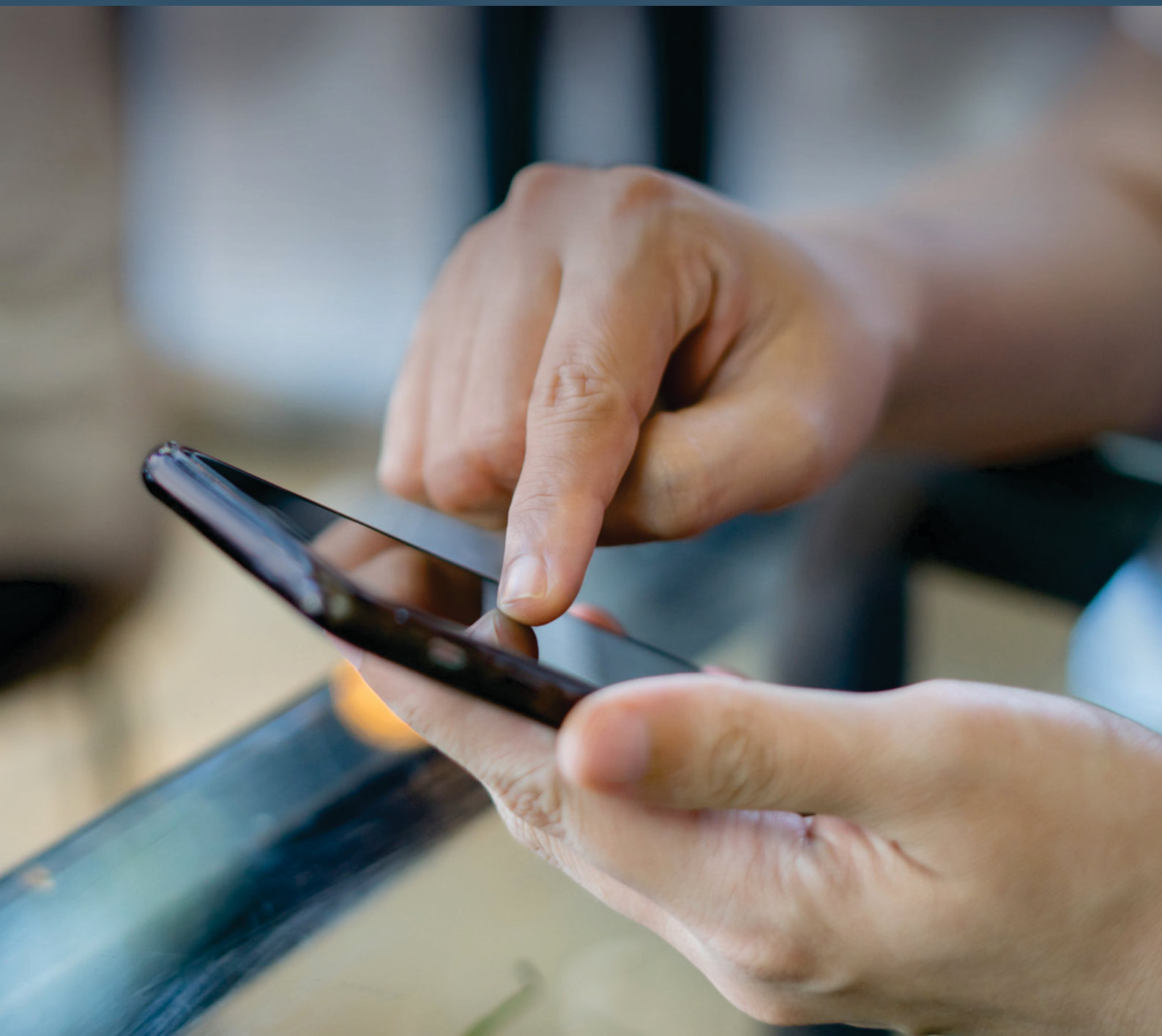
GEN KEY

# How do you know who your customers are online?

The future of ‘identity’ in financial services.

**Michiel Loeff**
CEO GenKey



Knowing who your customer is has always been essential for most financial services. When I say ‘knowing’, I’m referring specifically in this article to the identification and verification of customers. This is at the center of many know-your-customer (KYC) services, from credit checks and bank transactions to new FinTech and microfinance ventures. KYC services are changing radically as many financial institutions move, with some urgency, towards more complex services online.

**What is online identification?**

Being able to identify who someone is online requires the user to have a digitial identity that can be accessed and verified by a provider of financial services. But what do we mean by digital identity? Broadly it relates to the information needed to authenticate someone’s identity, accessed online. This marks a radical shift in the way identity authentication is currently managed, being mainly in face to face interactions. As this becomes less the norm, the challenge for financial services is to put in place systems that no longer rely on the customer being physically present. This change is happening against the context of identity theft being the fastest growing crime in the world today.

The need for digital ID is fueled by the increasing volume and complexity of financial services online. Many financial services are under pressure to provide customers with online services that are seamless and omni-channel. Especially in the retail banking sector, where a banking app for example, sits alongside Amazon, Uber and Netflix as part of consumers daily interactions. The challenge in terms of identification is to provide the same levels of ease and, let's say, delight, whilst ensuring that the appropriate levels of authentication are in place. There is much progress to be made to improve these user experiences as identity authentication shifts from where it is today, a largely manual, paper based process.

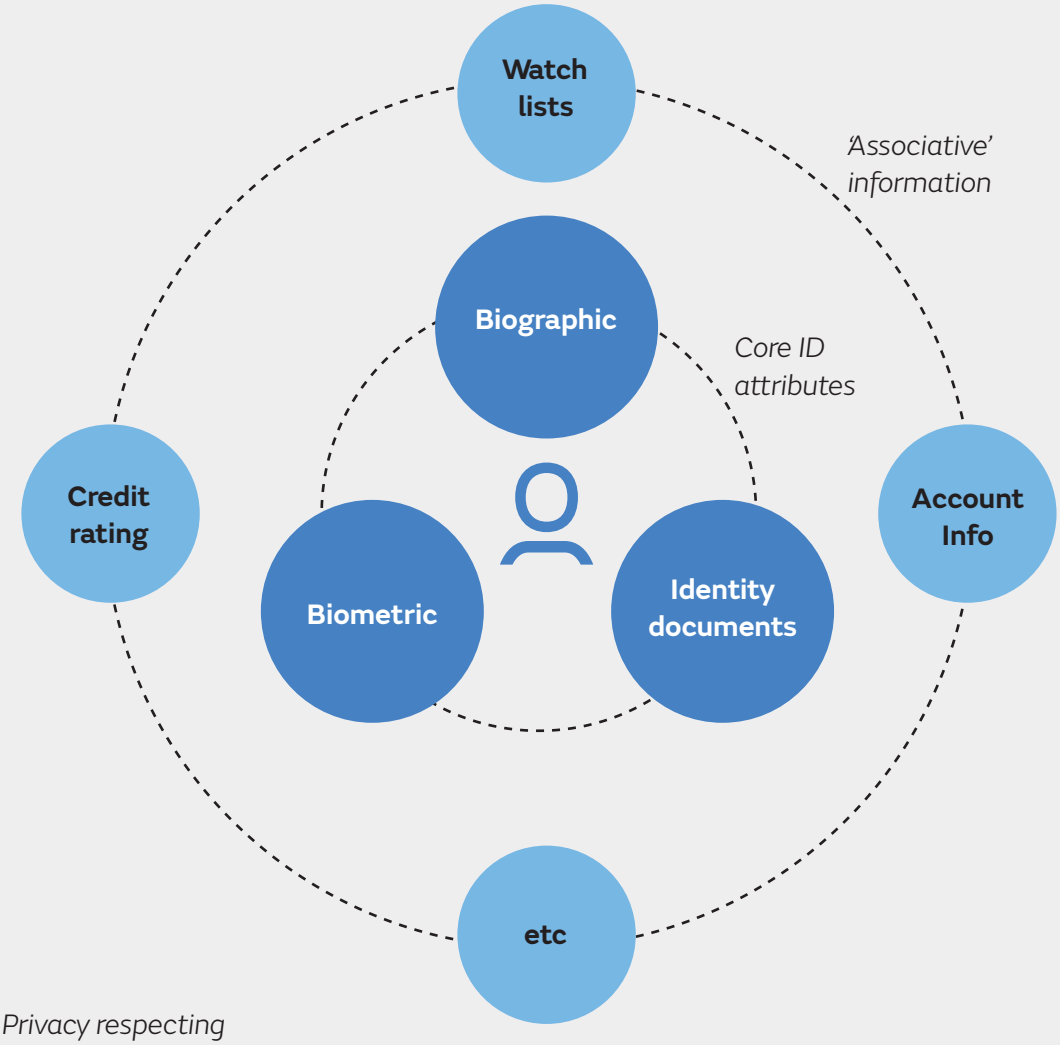
**" Many financial services are under pressure to provide customers with online services that are seamless and omni-channel."**

Additionally, online identification is struggling to keep up with the growth of new FinTech businesses that are reimagining incumbent models and creating new opportunities that didn't previously exist. For example, the growth of new ventures offering microfinance to the world's unbanked, of which it's estimated there are over 2 billion people. Now there's an opportunity! When you consider that there are also 1.5 billion people in the world today with no legal identity, we have a situation where advances in finance depends as much on advances in identification. Both sectors are living through transformative times, reminding us that beyond the need for Netflix-style user experiences, there are many practical issues to overcome to ensure that online identification is inclusive, easily accessible, cost-effective and reliable.

These are big challenges, but online also brings new opportunities to strengthen customer authentication systems, something the financial services industry is particularly well placed to lead. For example, a person's identity can be more easily validated against a wide range of online data sets, such as their credit rating, transaction history and criminal watch lists. Perhaps even one day, a verified Facebook profile. The ability to reference external data in relation to a customer, can't be underestimated. This is especially true in terms of meeting new regulatory requirements and avoiding fines associated with missing or inaccurate customer information. Online identification is increasingly helping firms comply with legislation such as Anti-Money Laundering (AML), Counter Financing of Terrorism (CFT), the 9/11 Act, etc.

**" The ability to reference external data in relation to a customer, can't be underestimated."**

**Digital identity attributes**




**Note:** *Privacy respecting standards should be in place.*

*Source: GenKey, ©2020*

### What makes a digital ID?

A digital identity comprises of a range of core identity attributes, which can include basic biographic details (name, address, date of birth, etc), identity documents (visa, ID cards, ePassports, etc), and biometric data (fingerprints, face, eye, vein, etc). Because this information is held digitally, these attributes can be strengthened overtime as more information gets added, updated and validated, for example by adding a new document, like a visa or driving license.

The use of biometric authentication, such as fingerprint, face, eye, voice is becoming more present in financial services. It's one of the most reliable ways to identify who someone is, because unlike other

**" Biometrics is one of the most reliable ways to identify who someone is, because unlike other identity attributes, it is inherently linked to them and cannot be easily forged."**

*What makes a digital ID? Continued.*

identity attributes, it is inherently linked to a person and cannot be easily forged. The adoption of biometrics by financial services is driven by several factors such as the need to achieve higher levels of assurance for complex transactions taking place online, the convenience to customers during the authentication process, and in order to meet new regulatory requirements. Biometrics is also being adopted as a new standard in countries that currently have low identity coverage and where there is a lack of official documentation beyond 'tombstone' data, such as name, date of birth, etc.

A person's digital ID can be further strengthened with associated (or contextual) information such as account history, transactional data, credit ratings (provided by credit bureaus) and criminal watch lists. Being able to integrate new records and data sets has the poten - tial to create a much richer and more nuanced view of the user. This offers higher levels of identity assurance during an authentication process (eg. onboarding), and also opens up better ways for financial services to tailor their services to customers.

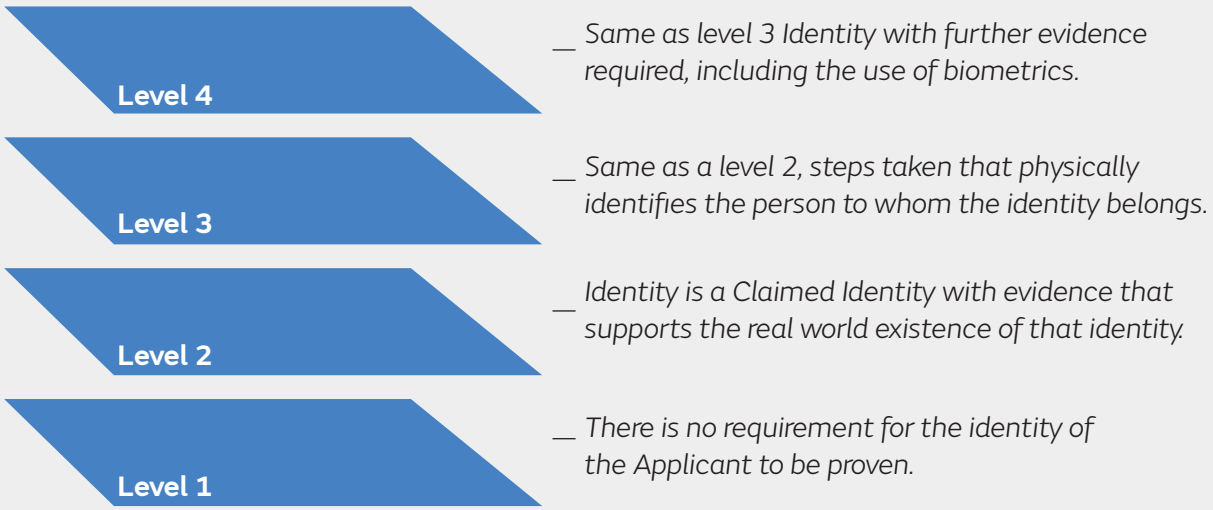
**The opportunity for financial services.**

With talk of biometrics and 'strength' it's worth also having in mind the 1.5 billion people that currently have no verifiable identity at all. The strength of a person's digital identity will very much depend on their circumstances. For example, very few of us need the level of assurance to board Air Force One. The size and strength of a person's digital identity will be needs driven. It will be based on the levels of assurance required to access a particular service online.

**" Very few of us need the level of assurance to board Air Force One. The size and strength of a person's digital identity will be needs driven."**

Assurance is a key factor in identity transactions for financial services and governments. The levels of assurance needed is proportionate to the degree of risk associated. The higher the risk, like using an online brokerage account or government service, the higher the level of assurance. For example, the UK government has defined 4 levels of assurance for iden - tification and verification to align across all its services, from tax to driving licences (led by Gov.UK Verify).

**Levels of Assurance**




*Source: Good Practice Guide No. 45 - Identity Proofing and Verification of an Individual, Gov.UK Verify*

As shown in the diagram above, level 4 requires the highest degree of assurance (including biometrics) and level 1 the lowest. It's possible to foresee levels of identity assurance being standardized by industry and governments. And, in turn for identity-providers to align standards by grading a person's digital ID, based on its strength (number of identity attributes, depth of information provided and associated). This is perhaps the biggest opportunity for financial services. With years of experience in cross-border operations, legal rights and protections, governmental and regulatory compliance, not to mention being more connected to their customers than most governments are to their citizens, financial services are best place to lead the way in the adoption of standardized practices for digital identity. These new systems have the potential to be go beyond institutions, sectors and countries.

Today, there are several models in place to deliver digital identity. Please read my follow up article on the subject. Overtime some might fail, others might consolidate, and some might continue in parallel. At the moment, it's too early to say. But, what I do fore - see is more standardized, 'open' protocols, relating to the grading (or rating) of a person's digital identity, and common levels of assurance set by financial services. And, in turn, the alignment of both (as shown in the diagram below). Even today, it's much needed.

**Levels of assurance aligned with customers digital ID**

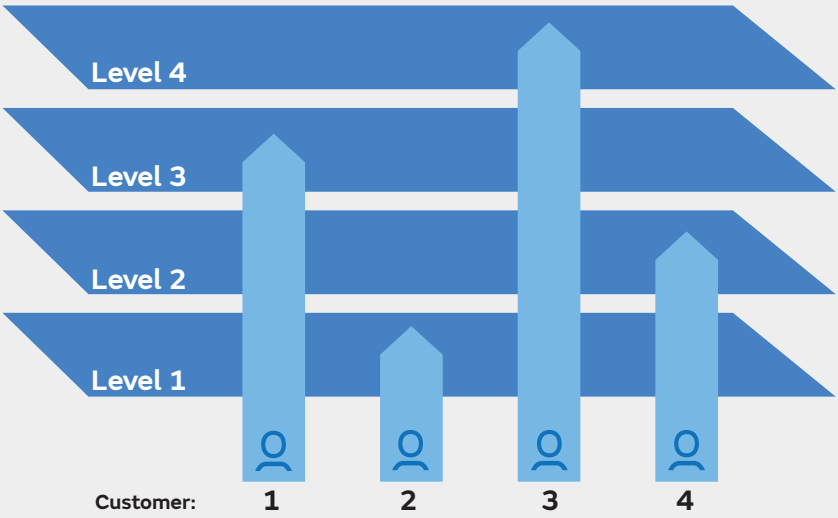



*Diagram shows 4 different customers with varying strengths of digital ID. For example, Customer 2 only meets level 1 of identity assurance and has a weaker digital identity than Customer 3.*

*Source: GenKey, ©2020*

**Concluding thought.**

I began this article talking about the challenges involved in indentifying customers online, but I end on an optimistic note. The urgent need for better online authentication is unargued. It's driven by the fact that customers are already there. They're waiting!

Identity providers and financial services have a lot to do to catch up with demand. But, the rewards go far beyond what's possible today, to meet the highest levels of assurance, to speed up transactions, to delight the customer, and to scale new ventures.

When it comes to identification and 'know(ing) your customer', the future is full of new opportunities. In many respects it's just the beginning, we've only just said 'hello'.

**CEO GenKey**

Michiel is CEO of GenKey, a leader in biometrics. With an engineering and business background, Michiel's role involves advising governments and private sector clients on the effectiveness of large-scale identity systems. For the past 10 years, he has been at the forefront of implementing ID systems for national elections, healthcare and eID, mostly in countries with no existing civil registry

**Contact:**
Michiel Loeff
CEO GenKey
Email: michiel.loeff@genkey.com

GenKey are experts in biometrics.

We work with partners to provide a full range of digital identity solutions, used by governments, public institutions and business.

Our mission is to work towards a world where everyone has a verifiable and trusted digital identity. We call it, **Identity for all, trusted by all.**

www.genkey.com

**GenKey's offices:**


GenKey HQ
High Tech Campus 69
5656 AG Eindhoven
The Netherlands

Email:
info@genkey.com

GenKey Ghana
5, 1st Asoyi Street
Bawaleshie,
East Legon, Accra
PMB 152 KA, Ghana

GenKey US
1834 Walden Office Sq
#220
Schaumburg, IL 60173