



GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS



Daon[®]



WHITE PAPER

The Digital Onboarding Imperative

Why organizations must embrace digital onboarding solutions

Table of Contents

- 3 Introduction**
- 4 What is Digital Onboarding?**
- 5 Digital Transformation Driving Growing Adoption, Accelerated by COVID-19**
- 5 With Rising Levels of Digital Transformation, Comes Risk**
- 6 The Critical Importance of Liveness Detection**
- 7 The Critical Importance of User Experience**
- 8 Digital Onboarding for Verified Digital Identity**
- 8 Why Stop at Identity Verification? Connect Authentication for a Seamless User Experience**
- 9 Meet The Expert – An Interview with Clive Bourke from Daon**
- 10 CASE STUDY 1: Satisfying Compliance Mandates with Biometric e-KYC**
- 11 CASE STUDY 2: Innovating the Pensions Industry with Biometrically Secured mypensionID**
- 12 Summary**

Introduction

This white paper from Goode Intelligence is sponsored by Daon and details why organizations must embrace digital onboarding. It draws on material from the Goode Intelligence market analyst report “Identity Verification (IDV) Market and Technology Analysis and Forecasts 2021-2026 (second edition).”

In the report, Goode Intelligence identifies a number of key drivers for the adoption of digital onboarding services. These include:

- Rising numbers of digital transformation projects that need to conveniently and securely onboard users through digital channels, accelerated by COVID-19
- Compliance with regulation, in particular Anti-Money-Laundering (AML) and Know Your Customer (KYC) regulation
- Rising levels of fraud, in particular identity fraud and account take-overs (ATO)

Digital onboarding services must be introduced in a way that meets the needs of a modern user-centric solution. This means being easy to use, available across all major channels, resistant against all major biometric spoof attacks, aligned with all other stages of the customer identity journey (e.g. authentication and recovery) and compatible with third-party identity checks using trusted data sources.

It is worthwhile spending some time on explaining what digital onboarding is and what it typically comprises of.

What is Digital Onboarding?

Digital onboarding is an umbrella term that covers a number of business processes associated with a potential customer or citizen signing up for a service or opening an account.

Two major components of digital onboarding are **Identity Verification (IDV)** and **Document Verification (DV)**, and they play an important part in validating the identity of a new customer and, in regulated industries, meeting AML and KYC regulation.

As part of the digital onboarding process, IDV answers the following questions:

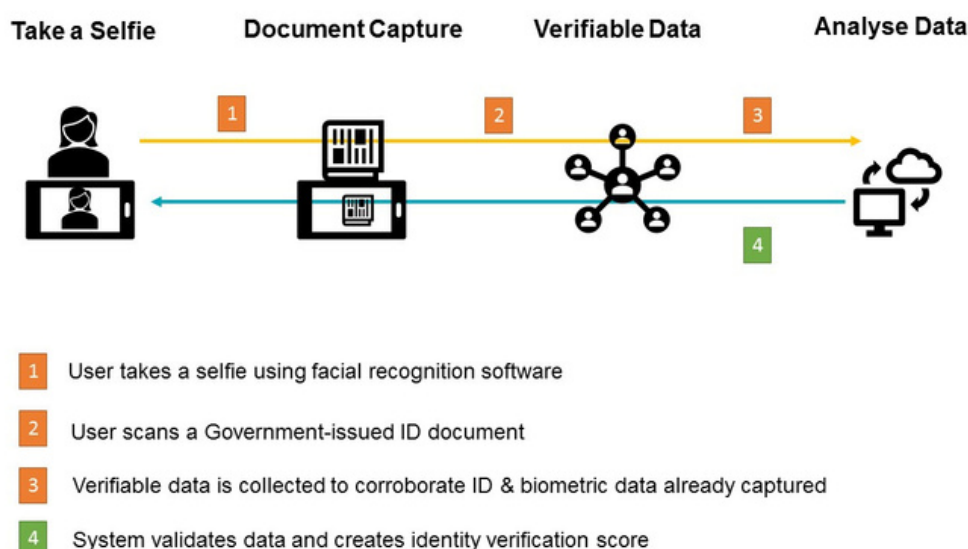
1. Is it a real user?
2. Is it authorised to use the data it presented?
3. Can you do business with the user?
4. What is the risk of doing business with the user?

A typical IDV process will include these three parts, glued together by orchestration:

1. **ID Capture:** Secure capture of identity data from a government-issued trusted document (passport, driving license or national ID) that is being presented to the service provider and verification that this document is not a fake and has not been tampered with. This can be done optically, using a camera (typically a smartphone camera), or by reading the document's chip using NFC (ePassport or eID).
2. **Facial Capture:** Capture of facial image, typically using a smartphone camera. Liveness testing during capture ensures that it is a real person and not a spoof attack.
3. **Corroboration & Risk Mitigation:** Validation of captured images—face and document. Dependent on the risk appetite a range of other techniques, including collecting signals (device and network) and data, will be used to feed into the risk engine to verify the entity's identity and validity to perform a certain task, e.g., open an account.

Orchestration: The workflow that manages the processes and ties the disparate technologies and data sources together.

Figure X – Typical Identity Verification Process



Digital Transformation Driving Growing Adoption, Accelerated by COVID-19

There is a rise in the number of people using the digital channel (mobile and web) to discover and then apply for new services. The rise has been accelerated by the COVID-19 pandemic. COVID-19 has led to an acceleration of digital transformation projects that support remote digital onboarding. This has been at the expense of face-to-face onboarding as it has been not safe to support in-branch, in-retail, or in-office onboarding.

In just one year we've experienced 10 years' worth of digital transformation. This startling statistic shared by McKinsey highlights a monumental shift online during the COVID-19 pandemic.

COVID-19 has certainly accelerated digital onboarding considerably, and it will continue to accelerate as digital-first strategies are rolled out across all sectors.

To ensure that this demand is satisfied, organizations must meet the challenges of

managing customer onboarding and registration purely through the digital channel.

Organizations must meet the consumer demand for a fully digital customer experience to ensure that they stay relevant in a very competitive market and reduce costs associated with traditional face-to-face methods.

With Rising Levels of Digital Transformation, Comes Risk

The need to quickly stand-up digital services has proved to be challenging for many organizations. As businesses have taken their customer activities and conversations online, they need assurance that they are dealing with legitimate people, particularly with increased digital threats and attacks on digital platforms becoming commonplace. In the first half of 2020 alone, 22 percent of US citizens were targeted for digital fraud, there was a 43 percent increase in Account Takeover (ATO) fraud, and in the UK, there was a 400 percent increase in digital fraud reported.

Figure 1: Account Takeover (ATO) Increases During COVID-19



The Critical Importance of Liveness Detection

According to Clive Bourke, President EMEA & APAC at Daon, “effective and certified biometric liveness detection has become a critical and essential component of digital onboarding.”

Liveness detection and spoof detection, commonly called Presentation Attack Detection (PAD), determines whether the person is alive and not an artefact, e.g. a printed picture, an image displayed on a computer screen or a mask. A robust facial recognition system that is used for digital onboarding must be able to deter common spoof attacks and must be able to determine whether a person is real and present during the identity verification process. There are standards and guidelines that vendors can meet to ensure that they deter common spoof and liveness attacks that include:

1. NIST SOFA-B Presentation Attack Detection framework [1]
2. ISO/IEC 30107-1:2016 Biometric presentation attack detection Part 1: Framework [2]
3. ISO/IEC 30107-2: 2017 Biometric presentation attack detection — Part 2: Data formats [3]
4. ISO/IEC 30107-3: 2017 Biometric presentation attack detection part 3: Testing and reporting [4]
5. IDO Biometrics Requirements – Presentation Attack Detection Criteria [5]

Common spoof attacks for face biometric systems include:

- 2D replay attack using:
 - Printed photo
 - Image on computer screen
 - Video on computer screen
- 3D replay attack using:
 - Rigid mask (no eyeholes)
 - Rigid mask (eyeholes)
 - Silicone mask with eyeholes
 - Facial animation software

Machine learning and artificial intelligence, despite their essential value for training facial recognition systems, can also be used to attack these systems. The emergence of ‘deep fake’ facial recognition attacks is a worrying trend in the fight against spoof attacks, creating an arms race between attackers and biometric technology companies.

Organizations planning to deploy identity verification for digital onboarding must ensure that their suppliers offer passive liveness detection that, at the very least, has been certified by a registered independent certification authority to ISO/IEC 30107-3 standards.

[1] <https://www.nist.gov/itl/tig/projects/strength-function-authenticators>

[2] <https://www.iso.org/standard/53227.html>

[3] <https://www.iso.org/standard/67380.html>

[4] <https://www.iso.org/standard/67381.html>

[5] <https://fidoalliance.org/specs/biometric/Biometrics-Requirements-v1.0-wd-20180830.pdf>



The Critical Importance of User Experience

This shift to digital presents significant challenges for organizations. In its report “Customer service trends and predictions 2021” [6], the UK’s Institute of Customer Service states that:

“In 2021 and beyond, online channels and applications will become even more important competitive environments for customer experience. Online customer engagement has intensified, including amongst many customers who did not previously buy from or interact with companies through online channels. As the COVID-19 environment evolves and forms of new normal take shape, some of this shift to online will become habitual. For organisations, success will depend on delivering intuitive, straightforward customer journeys.”

Our own research at Goode Intelligence shows that while user experience was certainly important before the pandemic, it is now of critical importance in a COVID-19 world. The high abandonment rates for onboarding and for eCommerce highlight consumer frustration with clunky, complicated onboarding and authentication methods that can lead to lost customers and sales.

Digital onboarding can be one of the first touchpoints for new users, and if an organization does not get this right, then they will simply go elsewhere. Relying parties and service providers must design and deploy digital onboarding solutions that are easy to use and do not add any needless friction.

Great user experience for digital onboarding can be achieved through:

1. Speedy and accurate capture of identity document information either through optical (smartphone camera) or NFC.
2. Accurate identity document verification ideally performed using machine learning and artificial intelligence or with the assistance of trained document analysts if exemptions occur.
3. Passive liveness detection that doesn’t put the onus on the user through clunky biometric capture.
4. Third-party identity data checks delivered within the app and in a timely way, ideally with pre-integrated third-party data connections to trusted providers like Experian, Datazoo and AAMVA.
5. Support for cross-channel interactions that can flow from desktop to mobile, browser to app, and back again.
6. Smooth orchestration, or workflow, that glues together the disparate processes that make up a digital onboarding solution.

[6] <https://www.instituteofcustomerservice.com/product/customer-service-trends-predictions-2021/>



Digital Onboarding for Verified Digital Identity

Alongside the rise in remote digital onboarding is the verified digital identity movement; a trusted, assured, digital identity that is portable and reusable.

The market for digital onboarding and IDV services has exploded in the last three years, and GI expects a similar stratospheric trajectory for verified digital identity schemes.

In many regions of the world, including the Nordic countries, Belgium and Canada, a consortium of trust providers that typically include the government, banks and telecommunications providers are deploying verified digital identities that can be used for digital onboarding purposes. Before these digital identities can be issued, identity verification takes place to ensure that the identity credentials are being issued to the authorized owner. Many digital identity schemes are leveraging the remote digital onboarding techniques described in this white paper, and this has become an important market for vendors and service providers.

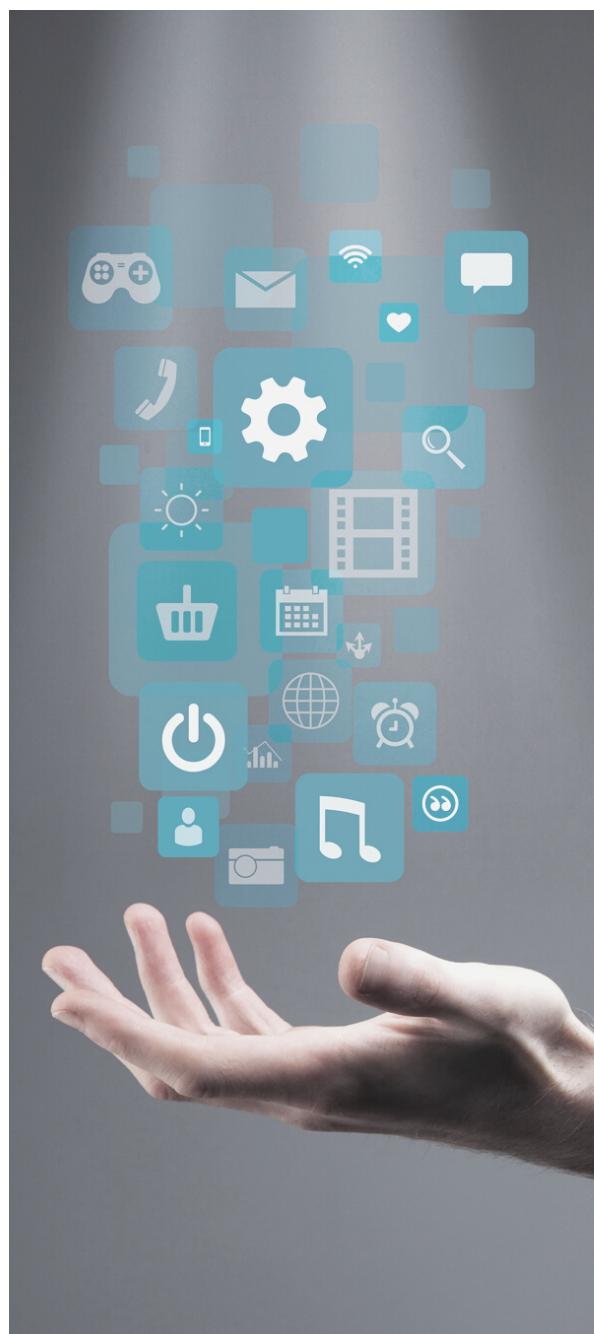
Why Stop at Identity Verification? Connect Authentication for a Seamless User Experience

Most identity verification systems waste the personal information they collect. Typically, an onboarding system will use identity information and biometric data to verify a user, and then discard it, forcing the user to resubmit their personal information to a second system for ongoing authentication of the now-verified user. Needless to say, this is far from a seamless experience.

But there are indications that this is changing. Goode Intelligence's research for its Identity Verification Market Analyst report has uncovered an emerging trend where forward-thinking organizations are choosing

a single platform for both onboarding and authentication—allowing the re-use of identity information captured during onboarding in subsequent interactions with that customer, typically for authentication but also for fraud management.

This approach enhances security, improves the customer experience, and puts the information a business spent money collecting to good use.



Meet The Expert – An Interview with Clive Bourke from Daon

Alan Goode, CEO and Chief Analyst, Goode Intelligence, caught up with Clive Bourke, President EMEA & APAC, Daon, to get his views on digital onboarding and to discuss some of the important trends that are shaping this service.

What activity are you seeing for digital onboarding?

“Before the start of the COVID-19 pandemic digital transformation was accelerating and within that, digital onboarding of end customers was a red-hot trend. Due to the impact of the COVID-19 pandemic on global face-to-face interactions, we observed an enormous push from a wide range of sectors. To support the delivery of government services to citizens in the COVID era, governments are increasingly turning to digital onboarding to support seamless digital registration with strong identity proofing. In addition to financial services markets where e-KYC is growing and growing, we are also seeing increasing demand from a wide range of sectors that previously have not prioritised digital e-KYC/digital onboarding such as education, telecoms, travel, sports betting and more. We are also seeing new customers across all continents, some of whom would previously have been slower adopters of

digital transformation and identity proofing initiatives.”

What use cases for financial services are popular for digital onboarding?

“The major use cases that Daon see at the moment include 1) remote customer account opening, 2) existing customer identity re-assurance, 3) lending authorization, 4) migrating existing customers to new digital use cases and 5) account recovery. A new use case enabled by these solutions is step-up authentication for high-risk transactions (such as high-value transfers or changes of address) using facial recognition. In this use case, a new server-based facial authenticator is established during the onboarding journey, linked to the customer identity and used as a new trusted element of that user’s credentials.”

What is the demand for liveness detection from customers?

“There is definitely better awareness of fraud risks and the role of liveness detection to detect presentation attacks. There is also greater awareness of the importance of having a certified solution, and customers are asking whether the solution has been certified against ISO/IEC 30107-3. The most discerning customers appreciate the difference between laboratory certifications and real-world operations, and they’re demanding greater vendor transparency. They also appreciate the trade-off between security and convenience and finding working thresholds that best address their customer base.”



“We are seeing increasing demand from a wide range of sectors that traditionally have not paid much attention to digital onboarding including those sectors that are not as highly regulated as traditional adopters of digital onboarding services”

Clive Bourke, President EMEA & APAC, Daon

Satisfying Compliance Mandates with Biometric e-KYC

Vendor:

Daon in joint venture with Sumitomo Mitsui Financial Group/Sumitomo Mitsui Banking Corporation and NTT Data.

Client:

PayPay – User of Polarify.

Business Objective:

Replace existing methods with more secure and convenient paperless KYC process for streamlined digital onboarding.

Solution:

Easy Check, an e-KYC service that lets users verify their identities by snapping smartphone photos of their face and identity documents.

About PayPay:

PayPay is a cashless payment system founded by SoftBank and Yahoo Japan in collaboration with India's largest payment company PayTM. PayPay uses a barcode linked to the user's bank account. To pay in-store, the user can scan the QR code installed in the store with the camera of the smartphone and enter the amount, or show the barcode displayed on the smartphone to be scanned by the store clerk. PayPay has over 10 million users and one million merchant partners, and is the second largest mobile payments company in Japan.

The Challenge:

In 2008, The Financial Agency Task Force (FATF) warned Japan that its remote account opening requirements were not sufficient to meet compliance with AML obligations. A decade later in November 2018, the Japan Financial Services Agency (FSA) enacted legislation that mandated stricter e-KYC processes for all remote



account openings of financial products, with old methods to be deprecated in April 2020. The legislation provided the following requirements, two of which involve digital onboarding with biometrics:

- Liveness checking of the person being onboarded
- Authenticity checking of the document they are using
- Japanese market-specific security checks of the document
- Tough criteria for biometric matching performance (False Acceptance Rate (FAR) $\leq 0.001\%$ with False Rejection Rate (FRR) $\leq 1\%$)

The Solution:

With Daon's technology, users can start using PayPay Money without having to go through troublesome procedures and instead utilize Easy Check (e-KYC) for identity verification by simply taking a photo of their face and capturing the identity documents with the cameras of their smartphones.

Over 750,000 users were successfully onboarded in the first week that PayPay Money was launched, proving the scalability and robustness of the onboarding platform. There are currently over 2.5 million users in the system with new users continuing to be onboarded at the rate of 20,000 per day.

SUMMARY

In this white paper, we have identified key drivers for the adoption of digital onboarding services. These include:

- Rising numbers of digital transformation projects that need to conveniently and securely onboard users through digital channels, accelerated by COVID-19
- Compliance with regulation, in particular Anti-Money-Laundering (AML) and Know Your Customer (KYC) regulation
- Rising levels of fraud, in particular identity fraud and account take-overs (ATO)

Organizations considering deploying digital onboarding services or seeking to upgrade existing ones must ensure that they are introduced in a way that meets the needs of a modern user-centric solution. This means being:

- Easy to use;
- Available across all major channels;
- Resistant against all major biometric spoof attacks;
- Aligned with all other stages of the customer identity journey (e.g., authentication and recovery);
- Compatible with third-party identity checks using trusted data sources

For more information, contact info@daon.com or visit www.daon.com





ABOUT GOODE INTELLIGENCE

Goode Intelligence is the leading digital trust research, consulting and events organisation covering Authentication, Biometrics, Fraud & Security, and Identity - founded in 2007 and based in London.

For more information on this or any other research please visit www.goodeintelligence.com. Follow us on **Twitter**.



ABOUT DAON

Daon is an innovator in developing and deploying biometric authentication and identity assurance solutions worldwide and operates across six continents. Daon has pioneered methods for securely and conveniently combining biometric and identity capabilities across multiple channels with large-scale deployments that span payments verification, digital banking, wealth, insurance, telcos, and securing borders and seamless travel. The Daon IdentityX® platform provides an inclusive, trusted digital security experience, enabling the creation, authentication and recovery of a user's identity, and allowing businesses to conduct transactions with any consumer through any medium with total confidence.

Daon's award-winning identity assurance technology successfully performs 250M+ authentications each day for iconic companies around the world, protecting life savings, personal information, and myriad consequential transactions. The company's design philosophy emphasizes inclusion, privacy, and ease of use, empowering Daon customers and their end users to meet precise needs and to customize identity experiences according to their preferences. It was Daon's pioneering methods of deploying digital identity solutions for border security agencies and high street banks that led to the creation of VeriFLY.

Many of the most iconic and innovative brands across the world, such as NatWest Group, Sumitomo Mitsui Financial Group, Standard Chartered Bank, Softbank, Experian, Australia Post, the New Zealand Government, Capitec, and Atom Bank use Daon products for mission-critical areas of their business, such as customer authentication.

Daon maintains a comprehensive Information Security Management System (ISMS) and Privacy Information Management System (PIMS) which are independently audited for compliance with the AICPA SOC 2 Trust Principle for Security, plus the international standard for information security management (ISO27001:2013) and extensions for privacy management (27701:2019) and management of PII in the public cloud (27018:2019). The company is subject to rigorous security tests and privacy audits by some of the largest organizations globally on a regular basis.

Get to know Daon on **Twitter** and **LinkedIn**.

This document is the copyright of Goode Intelligence and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Goode Intelligence.

This white paper contains extracts from the Goode Intelligence Market Analyst Report; Identity Verification (IDV) Market and Technology Analysis and Forecasts 2021-2026.