Daon

7 Ways Next-Gen Digital Onboarding Enhances
Customer Acquisition

7 Ways Next-Gen Digital Onboarding Enhances Customer Acquisition

Behold the traditional account opening experience: awkward, time-consuming, and avoided by consumers whenever possible.

In fact, the latest research suggests new account openings have reached a frightening abandonment rate of **70-90%**, with one Forrester analyst placing the number as high as **97.5%**.

The problem is obvious. Visiting a bank branch for in-person registration likely means taking time off from work or sacrificing lunch—just to open an account. And the common digital alternative, known as Knowledge-Based Authentication (KBA), is neither safe nor user-friendly.

When typical financial institutions spend **$200-$400** to acquire a new customer, why on Earth would they tolerate an onboarding process that more than 70% of potential customers abandon even after making the decision to open an account?

The answer is that until now, there hasn't been a truly safe digital alternative that could reliably stop fraud and ensure compliance with AML/KYC regulations. And lacking those protections, global banks might lose billions of dollars each year to fraud and more than $15 billion to regulatory penalties and fines (according to a recent KPMG report).

But here's the good news: Thanks to next-generation biometrics and biometric liveness technology, digital onboarding isn't just more frictionless—it's more secure, too. In fact, it's been proven to reduce abandonment rates and operating costs while simultaneously stopping fraud and maximizing compliance.

Next, we'll share the top seven ways that next-generation digital onboarding is helping innovative financial institutions change the game:

1
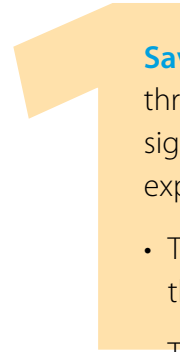
Saves Time. When account opening is done entirely through a mobile app or web browser, there's a significant enhancement to the overall customer experience:

- The customer doesn't need to visit a branch to have their photo ID validated.

- The customer doesn't need to type in their personal information, as this is extracted from the photo ID using optical character recognition (OCR).

- The customer doesn't need to answer annoying secret questions (otherwise known as KBA), since the biometric facial matching happens effortlessly.

New customers greatly appreciate the speed and simplicity of the improved process, which builds deeper trust and affinity for the financial institution's brand. Best of all, the faster, simpler customer experience leads to dramatically reduced abandonment.

BROWSER-BASED ONBOARDING

Modern digital onboarding solutions need not be confined to mobile apps. Rather, the entire onboarding process can now be browser-based, which removes the friction of having to download an app from the App Store. Furthermore, modern tools can deliver seamless cross-channel journeys from browser to app, or vice versa, so that customers can easily start in one channel and restart in another.

2

Improves Recordkeeping. Automatically capturing personal information from a photo ID (using OCR) is not only faster than manual entry, but also significantly more accurate. Without automation, manual typos and autocorrect anomalies will often lead to incorrect records and false rejections.

Moreover, next-generation onboarding tools now have a built-in "double check" process—wherein information extracted from a photo ID's barcode and/or machine-readable zone is compared to the data captured by OCR. The comparison detects inconsistencies that might be caused by a bad scan (low image quality, glare, etc.) or someone's attempt to falsify the ID. Regarding the latter, an underage student might be quite skilled at changing the birthdate on the face of his ID, but he'll find it next to impossible to alter the birthdate contained within the barcode. Better accuracy means fewer false rejections and less fraud. In other words: better acquisition of happier customers.

3

Better Experiences. Most online account opening processes start by verifying that the biographic information presented by a customer matches a unique known identity.

But while this proves an asserted identity is "real," it does not prove that the person asserting the identity is its rightful owner. To accomplish this aspect of the verification, organizations far too often rely on a flawed and hugely problematic technology called KBA.

KBA creates a short list of questions that, presumedly, only the true owner of an identity could answer correctly. Examples include:

- What is the monthly payment amount on your SunCraft boat loan?
- What year did you take out a mortgage on the home at 123 Maple Street?
- Which company do you have a current auto loan with—Ford, Chrysler, or Toyota?

Unfortunately, the answer to KBA questions can often be found on social media platforms and (as in the example above) any of your neighbors could see the new car parked proudly in your driveway or remember which year you moved into the neighborhood.

The other central problem with KBA is that it's a friction-filled experience, roundly disliked by consumers—many of whom will forget the answers to their secret questions on occasion and require a lengthy account reset process.

Organizations are well-advised to move away from KBA as quickly as possible, and to embrace next-generation digital technologies that can meet KYC requirements, strengthen security and privacy, and simultaneously enhance the customer experience.

✕ **Daon**®

4

Improves Inclusiveness. There's another, lesser-known problem with KBA—namely that it can disenfranchise certain classes of individuals, particularly those with smaller digital footprints or a limited history of meaningful financial transactions, which typically form the basis of KBA questions.
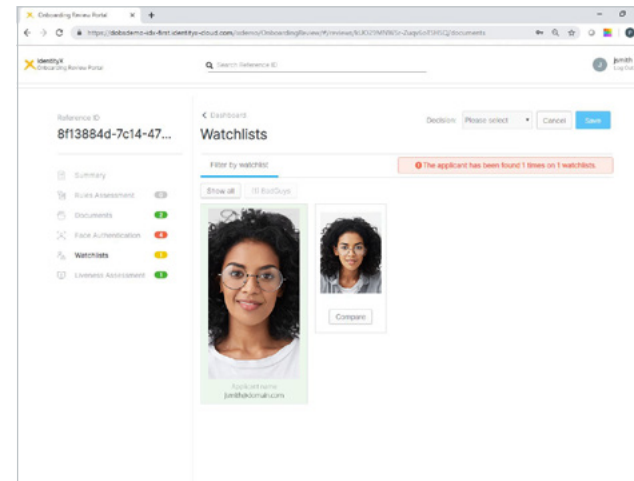
On the other hand, Pew Research notes that in 2019, 96% of Americans age 18-29 own a smartphone, including 71% of those making less than $30K per year. Hence, by abandoning KBA in favor of smartphone-based digital onboarding technologies that are more accessible to the masses, forward-thinking organizations can expand their customer base by appealing to these under-served consumer segments.

5

Lowers Costs. Saving time and eliminating complexity has the added bonus of dramatically reducing your total cost of operations. First, think of all the human capital needed for in-person onboarding at hundreds or thousands of physical branches across the globe. Next, consider the cost of scanning, printing, mailing, returning, and filing physical paperwork—a number Deloitte recently estimated at $25 million per year for a market-leading retail bank. Finally, consider the cost of handling an unending flow of KBA-related requests (most often from customers who forget the answers to their secret questions).

All these resources are much better spent on acquisition activities—enhancing the omni-channel customer onboarding experience—or going directly to the organization's bottom-line.

BIOMETRIC WATCHLISTS

A fraudster can easily change his name, but not so easily his face. That's why next-generation biometric watchlists use facial matching to compare an applicant's face to a database of those who were previously rejected (in the last day, week, month, or year). Repeated attempts at opening an account often indicate a fraudster trying to get through an organization's defenses with different forged IDs (all using the same face). Organizations might also choose to compare a new applicant's face to a register of known fraudsters (like a no-fly list) or a list of recently successful account openings, where a match might indicate a fraudster trying to open several accounts with multiple assumed identities.

![Daon logo]

6

Reduces Fraud. As noted previously, KBA is considered by most experts to be a fatally flawed security technology, while biometric-based authentication with advanced liveness detection is viewed as exponentially more effective and inclusive. Moreover, there are exciting new opportunities for fraud reduction within the realm of biometrics, most notably the use of facial biometric watchlists.

No matter how it's done, reducing fraudulent account access deepens trust, which boosts both customer satisfaction and new customer acquisition. Best of all, your fraud savings (just like your operational savings) can go directly to the organization's bottom-line.

INTEGRATED THIRD-PARTY IDENTITY CHECKS
Several firms, such as LexisNexis, Experian, Equifax, and TransUnion, provide critical identity proofing services that can verify that biographic information presented by a new customer matches a unique known identity. It's essential that your modern digital onboarding tool be able to integrate seamlessly with these identity check services, so you can be sure each new customer has a real identity and not a fraudulent, synthetic one.

7

Reduces Identity Theft. The account opening process isn't just about KYC and AML. Fraudsters who are successful in opening an account with a synthetic identity (i.e., a combination of name, address, and date-of-birth that doesn't actually exist in the real world) will use these accounts to build false digital footprints that can later be leveraged for more malicious and costly fraud activities.

Over time, fraudsters can build a digital footprint robust enough to convince a KBA system that it's real. (Since the KBA system draws on data from accounts associated with the synthetic identity, the fraudster knows all the secret answers.) Now, with a KBA-certified identity and financial history, the fraudster can potentially take out thousands of dollars in loans, from multiple institutions, with no intention of ever paying them back.

The good news is that modern digital onboarding tools with integrated third-party identity checks can stop these popular synthetic identity frauds before they start, which preserves customer trust and prevents potentially huge future losses for the financial institution.

7 Ways Next-Gen Digital Onboarding Enhances Customer Acquisition

ONBOARD AND ONWARD

As financial institutions struggle to meet KYC/AML regulations without driving away potential customers, the truth is becoming clear: In-person and KBA-based onboarding processes are simply obsolete in today's highly competitive marketplace.

Fully remote, digital onboarding processes are faster, more accurate, more secure and overwhelmingly preferred by consumers. Better onboarding means better customer acquisition. And when customers feel positively about their account opening experience, they're more likely to fund the account and begin using it for daily transactions—generating faster time-to-revenue for the organization.

Better yet, with modern technologies, onboarding a new customer is just the start of their journey. With a "two-in-one" platform for Digital Onboarding and Omnichannel Authentication like Daon's IdentityX®, your customers can use their onboarding credentials to authenticate—quickly and easily—at any time going forward, and through any channel they choose.

	STEP 1	**STEP 2**	**STEP 3**	**GOING FORWARD**
WHAT THE **USER** DOES:	• Takes a selfie	• Scans ID document	• Reviews & confirms details	• Enjoys easy ongoing access
WHAT THE **SYSTEM** DOES:	• Captures biometric faceprint • Performs both passive and active liveness checks to prevent spoofing • Compares faceprint to biometric watchlists to spot known fraudsters and repeat applicants	• Compares image to live biometric faceprint • Extracts customer information using optical character recognition (OCR) • Integrates with 3rd party data sources to help perform AML/KYC checks	• Delivers prompt customer decision in accordance with fully configurable rules and workflows	• Compares live biometric faceprint to registered identity credential for simple, immediate access

Come see how IdentityX boosts customer acquisition through simple, seamless customer onboarding and omnichannel authentication here.