OneSpan

Rethinking digital account opening and onboarding

A guide to minimize abandonment and drive growth

WHITEPAPER

Contents

The state of digital account opening

Rethinking digital onboarding at scale

Across banking, wealth management, lending, and insurance, the process of attracting and converting new customers is critically important for growth. Financial institutions invest heavily in sales and marketing to attract customers, establish relationships, and grow accounts. This focus on bringing in new customers shines a light on the customer onboarding experience. Seamless, easy, impactful experiences strengthen customer relationships and reinforce to prospective customers that they have made the right decision.

The experience customers have when they are onboarded can make or break a customer relationship. Get it right, and it's the perfect opportunity to win a customer's loyalty. Get it wrong, and it can cause them to get frustrated and walk away. Successfully onboarding a customer on their first attempt reduces the cost of customer acquisition, drives growth, and improves loyalty in the long term.

Despite the push for end-to-end digitization of account opening, many organizations still require new and existing customers to go through a mix of manual and online steps. Although organizations have taken steps to digitize, many do not offer a fully digital account opening process, whether online or through a mobile app. This is a result of addressing individual steps in the process, rather than digitizing the full process end-to-end. Some organizations have implemented eSignatures for example, but resort to manual steps for ID verification.

Manual steps, such as paper forms and in-person identity verification checks, add unnecessary friction. According to a Forrester survey, over 64% of banks experience lost revenue because of problems in the current onboarding process.[1] Technology now enables a fully digital account opening process, and customers have developed their own benchmark of what looks poor, good, and great when it comes to digital experiences.

This underscores the urgency to rethink digital onboarding at scale to make it fast, digital, and seamless, regardless of whether the applicant is in-branch or remote. Fully digitizing account opening using high-performing, secure, and reliable technologies can help financial institutions deliver convenient and effective customer onboarding. Although digital maturity is rising across the sector, some best-in-class organizations have utilized technology to widen their lead over the rest.[2]

In this report, we share insights and best practices for transforming account opening for multiple use cases, using advanced identity verification and document signing processes to improve the customer experience, facilitate compliance, and reduce the risk of fraud. Technologies covered include eSignature, smart digital forms, ID verification, video signing, co-browsing, and audit trail capture.

Digital account opening use cases

- Opening a checking or savings account
- Applying for a loan
- Applying for a credit card
- Applying for financing when buying a car or other large purchase
- Applying for a mortgage
- Opening a retirement account
- Opening an investing / trading account
- Opening a crypto account
- Applying for home insurance
- Applying for vehicle insurance
- Applying for health or life insurance
- Opening a pension or investment account

1. https://www.finextra.com/blogposting/10144/the-onboarding-challenge
2. Deloitte. Digital Banking Maturity 2022

Best practice 1: Go fully digital

Manual steps slow sales processes and frustrate customers

For some organizations, account opening and onboarding processes still involve cumbersome tasks such as form filling, manual data input, or visiting a branch. Many account opening processes involve a combination of digital and manual steps.

Consider this process for a new account application: The applicant fills out their details online and receives documents by email. But then, they're asked to go to a branch to show ID and sign paper documents in-person. Add customer due diligence checks, and the whole process can take several days. No wonder so many applicants abandon mid-way through the process.

Financial institutions with a hybrid workflow are increasingly falling short of customer expectations at a time when new challengers offer frictionless, and fully digital, experiences.

Applicants are less willing to accept slow, manual account opening experiences. They will not tolerate lengthy processes involving in-person appointments, manual identity verification checks, and paper forms. Today's applicant is looking for speed, ease, and convenience – whether online, mobile, face-to-face in the branch, through the call center, or through a virtual video conferencing session. Friction in their journey increases the risk of abandonment and decreases an institution's ability to compete.

If your account opening process includes a mix of manual and digital steps and you're losing customers, ask yourself:

- Are we offering the type of experience today's customers want?
- Are we losing customers due to friction? How can we reduce abandonment rates?
- How many manual steps are there in our processes? What can we remove?
- Are digitally enabled competitors gaining an advantage?
- How much time and money could we save by eliminating manual work?

How technology can address this issue:

Technology allows financial institutions to digitize each stage of the process – from guided, two-way communication via smart digital forms, to identity verification, signing, and secure storage of all documents and audit trails. The ability to bring new customers onboard via a fully digital journey leads to a better customer experience, higher completion rates, and faster cycles. Navy Federal Credit Union was able to onboard new business clients in just 24 hours after implementing digital account opening for business lending – an increase of 10x over previous onboarding timelines. This meant they could process the same number of loans in 30 days that they had previously done in six months, leading to a rapid expansion in new business customers and company growth.[3]

Fully digital onboarding can also deliver huge time and cost savings. Bank of Montreal was able to save millions of dollars per year by eliminating manual processes from account opening, enabling accounts to be opened within 8 minutes.[4]

With the right technology, processes are completed in minutes – at a fraction of the cost.

3. https://www.onespan.com/blog/navy-federal-credit-union-truist-discuss-digital-innovation-business-banking
4. https://www.onespan.com/resources/celent-bmo-digital-transformation-personal-banking

Success story:
Clarien Bank goes 100% digital

Clarien Bank is one of Bermuda's largest independent integrated financial services organizations with assets of US$1.36 billion. The bank provides retail banking, corporate and private banking, as well as wealth management and investment services.

In 2021, Clarien Bank digitized their account opening processes with electronic signatures, smart forms, and digital identity verification technology to create a secure end-to-end online experience for retail banking. The success of the initiative has enabled Clarien Bank to deliver a more personalized experience for customers, as well as empowering the company to adopt a digital-first culture.

Read the full story

Strategic goal:

Digital bank of choice in Bermuda

15 mins

Mobile account opening

Recognition:

Mobile App of the Year

CLARIEN

Best practice 2: Streamline data capture

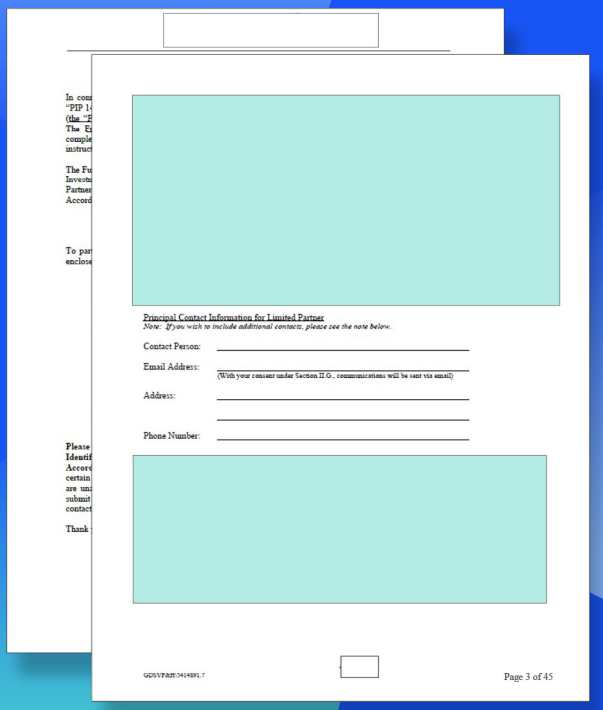
Turn static PDFs into dynamic, mobile-ready smart forms and agreements

The first step in the account opening process typically involves a data capture process.

Data capture is often a cumbersome process, whether conducted manually (where the customer shows up at a branch for a face-to-face questionnaire), or digitally through inflexible PDF forms.

Challenges of PDF forms:

- No ability to pre-fill with known information like identity verification, address, etc.
- No conditional logic so cannot validate critical information or notify of missing information during the process
- No ability to guide users through the workflow to help them better understand each question and prompt the next step
- Non-dynamic and non-intuitive, which results in printing, emailing, and rekeying to correct any missing or incorrect information
- Longer completion time increases risk of delays between initiation and submission of final, accurate form
- Non-mobile responsive restricts an organization's ability to make form updates quickly or efficiently
- Channel and signature limitations lead to high abandonment rates



Clunky and inflexible PDF forms add unnecessary friction to digital agreement processes, lowering completion rates and leading to customer abandonment. The lack of data interoperability leads to human error and documents with missing data and signatures, which results in inefficient and costly manual checks and reworks.

Data capture automation and modernization are key to minimizing friction and reducing abandonment. Smart digital forms provide customers with a faster and friendlier experience that is less prone to errors.

If you are experiencing high application abandonment, ask yourself:

- How are forms used in the application process to capture data from the consumer?
- Are your forms mobile-ready?
- Are applicants abandoning the form-filling process before they get the opportunity to eSign the agreement?
- Are you able to deliver an adaptive interview-style questionnaire to make it easy for applicants to complete the application process?
- Do you offer guided forms and conditional logic to capture only the necessary data based on the applicant's responses?

How technology can address this issue:

Smart digital forms turn PDFs into mobile-ready, interview-style forms that are easy to complete before signing and help to deliver a more engaging, frictionless onboarding experience. Applicants can provide information on their own devices from almost anywhere, without the need for an in-person appointment or branch visit.

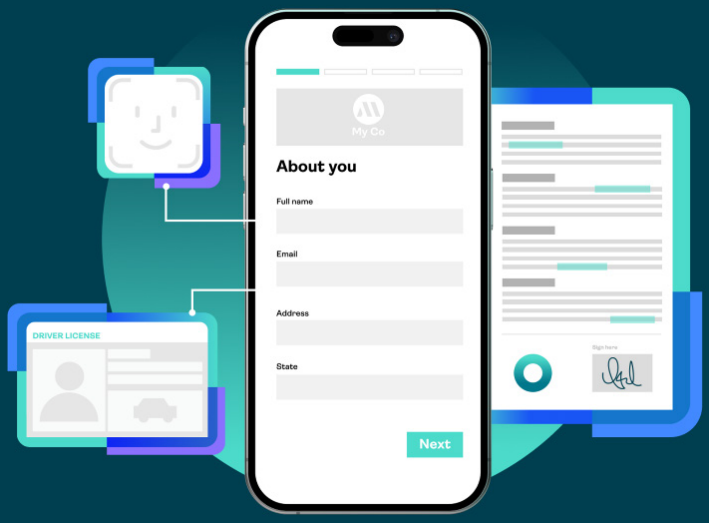
Smart forms can also reuse information when applicable and can automatically adapt to asking new questions based on previous answers. They also automatically generate a signature-ready agreement that can be signed instantly using eSignatures. This streamlined digital process is faster, more customer-friendly, and less prone to errors. Using smart digital forms enables organizations to reduce abandonment, increase efficiency, avoid unnecessary errors, and eliminate Not in Good Order (NIGO) documents.

A Forbes Global Top 500 leader in insurance and investment management digitized critical lines of business using smart forms and eSignatures, leading to a 40% reduction in paper and over 21,000 forms being converted to flexible smart forms in three years. The initiative led to a 300% increase in the use of eSignatures within the first 90 days of launching, and the company's investment business unit hit 60% of their sales quota in the first 60 days of the year due to the ability for customers to complete and sign contribution applications on their mobile phone.

Success story:
Top US bank transforms financing with smart forms and eSignatures

The financing arm of a large US bank leveraged smart forms and eSignatures to reduce account opening times from three months to just two weeks by improving the customer onboarding process. Prior to implementing these technologies, the company required potential customers to fill out a 14+ page static PDF form. The PDF was then emailed as an attachment back and forth between the customer and the bank, with errors and omissions extending the timeline to complete the onboarding application.

With smart forms and eSignatures, the company was able to create a guided, interview-style form with conditional logic that helped prospective customers through each step, all the way from application to signing. The customer satisfaction rating was 87% and the bank division employees felt the new process was flawless, allowing them to deliver an intuitive, error-free, faster customer onboarding process which helped their clients secure payment quickly and easily.



87%
Customer satisfaction rating

Best practice 3: Digitize account opening with ID verification

Poor user experience and lack of appropriate security measures can result in significant losses

Fighting new account fraud is an uphill battle for financial institutions. As identity fraud continues to grow, it is increasingly important for financial institutions to determine and prove who they are transacting with. In a 2024 State of Fraud Benchmark Report, researchers revealed that 33% of fraud is detected during customer onboarding.[5] By confirming the identity of applicants in real time, institutions can better detect identity fraud and mitigate the risk of new account and application fraud.

In 2023, identity theft was the most common type of consumer complaint made to the US Federal Trade Commission (FTC), accounting for 29.4% of all reports received.[6] Identity theft, or synthetic fraud, involves fraudsters using stolen or fictitious identities to apply for new services or products. These identities may be entirely fabricated, or they may combine real and fake information to create convincing profiles. They may use a real Social Security number, for example, combined with fabricated names, addresses, and other personal data. Third-party fraudsters aim to secure loans, credit cards, BNPL (buy-now-pay-later) products, or other financial resources under these false identities, ultimately leaving financial organizations to suffer the losses when the fraudulent activity is uncovered.

Furthermore, the prevalence of deepfakes is on the rise. This advanced technology enables malicious actors to craft remarkably convincing impersonations of a person's voice or appearance. These deceptive creations are increasingly being employed to engage with organizations during the account opening phase, posing a significant challenge in distinguishing between legitimate applicants and imposters.

According to a survey conducted by Regula, approximately 80% of companies view counterfeit biometric artifacts such as deepfake voice or video as substantial threats. And approximately 46% of organizations worldwide encountered incidents of synthetic identity fraud in the past year.[7]

In these challenging times, financial institutions need to prove they know who the applicant is, and that the applicant is genuinely the person they are interacting with. They also need to comply with Know Your Customer (KYC) regulations, which mandate that financial institutions confirm the identity of a customer before providing them with financial services.

To help mitigate the risk of fraud and impersonation, ask yourself:

- Are we offering the type of digital identity verification experience today's customers want?
- Does our current identity verification process protect against identity fraud?
- Does our current identity verification process mitigate deep fakes?
- Does our process prove that the applicant exists?
- Does our process protect against account opening fraud?
- Are we using real time identity verification?
- What changes do we need to make to verify an applicant digitally while remaining compliant with all relevant regulations?

5. https://workweek.com/2024/02/28/fraud-management-id-verification
6. https://www.fool.com/the-ascent/research/identity-theft-credit-card-fraud-statistics/
7. https://www.securityinformed.com/news/businesses-hit-voice-video-deepfake-fraud-co-1663237705-ga.1682657700.html

How technology can address these issues:

To mitigate the risk of new account fraud, many financial institutions are turning to technology to digitally verify an applicant's identity. Technologies such as document verification and facial comparison help institutions validate the identity of an applicant and prove that the validated identity is genuinely the individual they are interacting with.

These technologies are seeing high adoption rates with consumers due to their ease of use and the high levels of trust they provide between an organization and an applicant. According to WORKWEEK, a recent study confirmed that 65% said they were happy to take a picture of their ID and a selfie to protect themselves from fraud when using a financial application, with 64% saying that they feel safer using a digital financial product when they're required to provide identifying information, like a photo of their driver's license.[8]

Document verification

Document verification is a digital identity verification method used to check whether an applicant's ID document such as a passport, ID card, or driver's license, is legitimate.

Using the in-built camera on a mobile or hand-held device, the technology captures an image of the applicant's ID document. Artificial intelligence and advanced authenticity algorithms are then used to analyze the image to produce an authenticity score to determine whether the ID document is fraudulent or genuine.

ID document verification enables a customer's ID documents to be authenticated digitally and in real-time. For the consumer, the experience is quick and simple. For financial institutions, automated ID document verification speeds up account opening, removes manual steps, eliminates the need to train staff to manually verify ID documents, and ensures that identity verification processes are consistent and compliant – all while protecting against identity fraud.

Benefits of ID document verification:

- Plays a crucial role in meeting AML and KYC requirements
- Enhances security through facial comparison, which establishes a match between the individual presenting the ID and the person depicted in the ID document
- Eliminates biases and human errors, thus enhancing accuracy and reducing fraud
- Delivers an excellent user experience
- Expedites the verification process because ID documents can be verified in seconds

Facial comparison

Facial comparison plays a key role in confirming the physical presence of an applicant during the remote account opening process. The ability to prove that a user is genuine and physically present during remote account opening is a critical component in the fight against application fraud.

Due to data breaches and SMS security vulnerabilities, traditional methods of identity verification such as KBA (knowledge-based authentication) and two-factor SMS authentication alone can no longer be relied on to verify users during remote account opening.

As a result, financial institutions are shifting their focus towards robust alternatives like facial comparison, which can be used with document verification to prove that a prospective customer is genuine. Facial comparison takes place after document verification is used to verify the authenticity of an applicant's passport, ID card, or driver's license. It compares a selfie with the image from the applicant's verified ID document to prove that the person is present during the account opening process.

Liveness detection

Before a captured image or selfie is used for facial recognition, liveness detection can be applied to the image to prove that a person is genuinely present, and that a static image of the person has not been fraudulently used. This technology helps ascertain that the image hasn't been fabricated using methods such as high-resolution printouts or pre-recorded videos.

8. https://workweek.com/2024/02/06/digital-identity-paradigm-shift

Importance of security in identity verification

When addressing the realm of AI-driven presentation attacks, it is essential to distinguish between two significant categories: presentation attacks and deepfakes.

AI-driven presentation attacks

Presentation attacks occur when malicious individuals employ someone else's physical characteristics or biometric data to deceive systems and impersonate others. ISO/IEC 30107-3:2017 provides a regulatory framework to safeguard against such attacks, allowing for the classification and evaluation of detection mechanisms. Advanced AI algorithms can be implemented to detect diverse types of presentation attacks.

Deepfakes

In contrast to presentation attacks, deepfakes involve the artificial creation of images, audio, or videos using AI to replace one person's likeness with another's. Dedicated algorithms can be employed to combat this threat. A vital aspect is the synergy between capture (client-side) and analysis (back-end) capabilities in processing and analysis of evidence such as documents, selfies, and audio. Maintaining control over both fronts makes it difficult for deepfake attacks to infiltrate the authentication process.

What to look for in a vendor

Digital verification checks allow financial institutions to prove who their applicant is and that they are in fact the person the financial institution thinks they are transacting with.

Look for a vendor that can provide you with access to advanced identity verification and authentication capabilities, including:

- Mobile ID document capture
- Identity document verification
- Facial comparison
- Liveness detection
- Biometric verification
- Strong authentication methods
- Risk assessment
- Adaptive authentication

Best practice 4: Sign documents with secure and convenient eSignatures

Lack of an efficient and secure eSigning process can result in financial losses and a poor user experience

eSignatures have become the new norm for organizations of different sizes and industries looking to digitize processes, improve the customer experience, and reduce costs. By leveraging secure eSignature, documents can be signed digitally in an easy and secure manner as part of a seamless digital account opening process.

However, despite the high adoption of eSignature, not all solutions are created equal. Common challenges that financial services and insurance companies experience with traditional solutions include:

- **Multiple eSignature tools deployed:** Some eSignature solutions deliver limited digital agreement and integration capabilities. When this happens, organizations find themselves using multiple eSignature applications to service all use cases across the enterprise. This in turn drives up the total cost of ownership and results in inconsistent customer experiences, from account opening onwards.
- **Poor user experience:** Some eSignature solutions offer limited customization capabilities, which can lead to poor experiences. A good example of a necessary customization capability is white-labeling, or custom branding, to ensure that the person applying for a new account recognizes and trusts the eSignature notification emails sent to them. Otherwise, this will negatively impact completion rates and the ROI of the digital process.
- **Increased risk:** Sensitive data shared during the account opening process makes security a top consideration. Some eSignature solutions lack bank-grade security, which in turn exposes organizations to phishing and data security risks.

Implementing an eSignature solution is essential for optimizing costs and streamlining processes. With greater scrutiny over technology spending, enterprises should evaluate opportunities across their entire business rather than limiting it to a single use case or department, and periodically reassess the solution's alignment with requirements to ensure it is supporting all use cases.

To improve the document signing experience, ask yourself:

- How do applicants currently sign documents as part of account opening?
- Is it a good customer experience?
- What security controls do you have in place for secure document signing?
- Does your eSignature solution offer white-labeling capabilities to protect your brand and reduce phishing risks?
- What is the abandonment rate? Are enough applicants completing the process?
- Does your eSignature solution enable your organization to scale?
- Have you integrated eSignature with smart digital forms?
- Is eSignature integrated with your mobile app experiences?

How technology can address these issues:
Implementing eSignatures ensures the best user experience for remote account opening. Electronic signing can take place on any device, via an app or browser, and can be fully integrated for an automated hand-off between back-end systems.

For the highest completion rates and ROI, industry leaders focus on three best practices:

1. Develop an organization-wide center of excellence for eSignature: By standardizing on an enterprise-grade solution, organizations can customize workflows to match the requirements of any use case, such as deposit account openings – and then rapidly scale to other use cases or lines of business (e.g., account opening in another business unit such as insurance, wealth management, commercial lending, or mortgage). This creates a consistent user experience across business units, standardizes compliance, lowers the total cost of ownership, and accelerates time to market.
2. Maximize adoption through an excellent user experience that builds on features such as white-labeling: White-labeling enables an organization to put their brand front and center throughout the entire eSign experience. This has proven to boost adoption and completion rates. For example, a leading direct-to-consumer auto insurer experienced a 23% increase in completion rates in the first 30 days of implementing a white-labeled eSignature experience.[9]
3. Safeguard the organization with bank-grade security: The right eSignature solution will help protect from financial losses and reputational damage caused by phishing attacks. Phishing attacks are often automated and executed in bulk, which makes eSignature vendors with extensive databases an appealing target. Not only does white labeling improve the user experience, it also provides an extra layer of security, reducing the chances of phishing attacks being sent to an organization's customers.

These essential practices will take eSignature investments to the next level with higher completion rates, great cost savings, and the ability to scale faster and more efficiently.

Success story:
BMO's eSignature center of excellence

Bank of Montreal (BMO) implemented eSignatures to simplify and streamline the remote onboarding and account opening process for 100 use cases across four business units, including banking, wealth, and capital markets. For the Personal Banking business unit, the adoption of eSignatures resulted in a 40% increase in overall operational efficiency, and the ability for prospective customers to open an account remotely in under 8 minutes.

Leveraging an innovative enterprise-wide shared service approach, BMO extended the use of eForms and eSignatures across multiple departments, including talent/HR, procurement, IT, risk management, and equipment financing.

The adoption of eSignatures at BMO is projected to deliver annual cost savings of $98.2M due to the eliminated costs of inefficient manual processes and duplicative systems.

8 mins
To open an account on a phone

30 mins
Saved per day, per bank representative

40%
Increase in process efficiency

$98m
Projected annual cost savings

BMO

9. https://www.onespan.com/resources/direct-to-consumer/case-study

What to look for in a vendor

Look for vendors that offer:

- The ability to craft custom workflows for front and back-office use
- Scalable, efficient, and secure APIs and SDKs
- Ready-to-use web and mobile applications to meet workflow needs
- A strong integration framework to tie workflows to existing business applications
- White-label branding capabilities to boost adoption and completion rates, and reduce the risk of phishing attacks
- Specialized onboarding and training to guarantee that the team receives comprehensive guidance, facilitating swift adoption and effective utilization
- A solution that enables in-person and remote, online and offline, mobile and web experiences to cover clients' needs securely and conveniently
- Strong evidence capture; providing a thorough overview of the entire agreement process, covering identity verification, authentication, eSignature, and storage
- Access to prompt and responsive support around the clock
- Multi-language support, and compliance with international regulations

Best practice 5: Humanize the agreement process

Recreate the power of a face-to-face meeting in a virtual environment

As financial activities get more complex, consumers tend to turn to channels where they can get human help and assistance. Despite a surge in all things digital, customers still value the human connection. That's why a human-digital hybrid approach in the financial services industry is an important combination.

> **"...customers will continue to use digital, but when that moment is there, when they need a human, we'll be able to connect them to a human being. That's our approach in terms of how we're thinking about digital and that human connection."**
>
> **Ankit Bhatt**
> EVP and Consumer Chief Digital Officer, US Bank

If your process is complex and requires a virtual meeting, ask yourself:

- Are the agreements normally mediated by a human (e.g., advisor, agent, contact center representative)?
- Are the agreements high-value or high-risk and would benefit from human assistance to drive higher completion rates?
- Am I able to infuse human help into our current digital agreement processes?

How technology can address this issue:

- Video-enabled communications help mimic a face-to-face environment where you can add a human touch and develop a relationship with customers.
- Strong identity verification and authentication options ensure you know exactly who you're transacting with and that all participants in the agreement process are who they claim to be.
- Co-browsing facilitates real-time collaboration, the ability to review the terms and conditions, and reduces missing and incorrect information in account applications and forms.
- Comprehensive audit trails help to satisfy the legal and compliance requirements for a legally binding agreement.

Best practice 6: Collect digital audit trails

Prove compliance and avoid regulatory fines

Audit trails protect both the customer and the organization. They also help reduce customer disputes as the audit trail captures the entire process leading up to the final agreement between the parties. This is especially important for transactions where the customer is not accepting a waiver or industry specific recommendation.

In addition, audit trails also help prove compliance with industry and local regulations. Financial institutions are being audited more frequently than ever, and senior executives are being held both legally and financially responsible for the decisions they make. Organizations should look to capture as much detail as possible about the transactions that take place with customers and partners, so they are able to prove compliance when required to do so.

Organizations need to ensure that signed documents are not just secure, but also compliant with laws like UETA, ESIGN, and eIDAS. Failure to carry out each step in the agreement process according to the regulations of a particular jurisdiction could lead to fines for non-compliance. Technology can help by capturing digital audit trails to prove that fair and compliant practices were followed, and that applicants were fully aware of what they were signing up for at the time of opening an account or applying for a financial product.

To determine if you could be at risk of non-compliance, ask yourself:

- Is our account opening process fair and compliant?
- If so, how do we collect evidence to prove it?
- Do we capture an audit trail throughout the process?
- Does the audit trail prove the identity of the applicant?
- Does the audit trail confirm what the applicant saw and did during the agreement process?
- Is each audit trail linked solely to its corresponding transaction?
- Is each audit trail tamper-sealed?
- Could audit trails be lost or deleted?
- Do the audit trails cover every step in the account opening process, including identity verification and authentication?
- How can we access our audit trails?
- Are we dependent on internal IT or third parties to retrieve, explain, or verify our audit trails? If so, are our audit trails accessible in perpetuity?
- Is it possible to store and move our audit trails without compromising their integrity?

How technology can address this issue:

Technology can directly address the issue of legal enforceability by capturing an audit trail of the entire agreement process. This audit should include:

- Evidence of the identity of the applicant
- Evidence of exactly what the applicant saw throughout the transaction (such as terms and conditions)
- Evidence of exactly what the applicant did during the transaction (such as confirming that they read and agreed to the terms and conditions of the agreement)

The audit trail should also be stored in a tamper-proof and secure digital file. This strengthens an institution's ability to enforce an agreement if challenged.

Summary

In a world where new clients expect convenience and speed, it is essential to offer a user experience built around digital channels. Forcing a prospective customer to carry out manual steps during customer onboarding amounts to a poor and frustrating experience. What's more, weaknesses in your tech stack expose your organization to fraudulent activity, which then requires time and resources to prevent further fraudulent applications and accounts.

The good news is there are modern and effective approaches to digital account opening available in the market today that address gaps in partially digitized processes. These approaches help prevent application fraud and reduce unnecessary friction in the customer journey.

Whether looking at account opening, insurance applications, loan applications, or other forms of first-day processes and customer acquisition, it is time to embrace the next step in your digital transformation. Innovative technology such as smart forms, ID document verification, eSignatures, and secure virtual environments deliver an exceptional digital onboarding experience, from beginning to end.

Speak to one of our experts to understand how to implement these technologies in your environment today.

About OneSpan

OneSpan, the digital agreements security company™, helps organizations accelerate digital transformations by enabling secure, compliant, and refreshingly easy customer agreements and transaction experiences. Organizations requiring high assurance security, including the integrity of end-users and the fidelity of transaction records behind every agreement, choose OneSpan to simplify and secure business processes with their partners and customers. Trusted by global blue-chip enterprises, including more than 60% of the world's largest 100 banks, OneSpan processes millions of digital agreements and billions of transactions in 100+ countries annually.

Learn more at
OneSpan.com

Contact us at
OneSpan.com/contact-us

OneSpan