

AGREEMENT AUTOMATION: BEST PRACTICES TO REMOVE FRICTION, IMPROVE COMPLIANCE, & ACHIEVE GROWTH

A GUIDE TO DIGITAL TRANSFORMATION
FOR FINANCIAL AGREEMENT PROCESSES

WHITE PAPER





TABLE OF CONTENTS

Introduction	3
Best Practice 1: Go Digital	4
Best Practice 2: Strip Out Manual Checks	5
Best Practice 3: Digitize ID Checks	6
Best Practice 4: Fight Application Fraud with Digital Identity Verification	8
Best Practice 5: Future-proof Solution with Multiple Digital Identity Verification Methods	10
Best Practice 6: Create Legally Enforceable Agreements	11
Best Practice 7: Collect Digital Audit Trails	12
Best Practice 8: Provide Strong & Persuasive Evidence	13
Best Practice 9: Deploy Flexible Solution	14
Conclusion	15

This white paper is not intended as legal interpretation of relevant laws or regulations. The information presented here is for general purposes only and does not constitute legal advice.



INTRODUCTION

ACCOUNT OPENING AND FINANCIAL AGREEMENTS: THE FUTURE IS DIGITAL

The process of onboarding a new banking or finance customer 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 customers to get frustrated and walk away.

Despite customer demand for fast, convenient, and online services, account opening and financial agreement processes at many financial institutions remain slow and manual. In a recent study, Aite Group found that 60% of checking account applications were still handled in the branch, with a significantly lower amount submitted online (26%) and via mobile (4%).¹

Financial institutions (FIs) continue to rely on manual processes such as paper forms and in-person identity verification checks – not realizing that their manual processes carry risks. Manual or partially automated account opening processes expose FIs to operational, regulatory, fraud, and customer experience risks. Fully digitizing these processes using high-performing, secure, and reliable technologies mitigates these risks.

In this white paper, we recommend key areas to evaluate as you analyze the risk in your current processes. We also explain how technology helps address issues like customer abandonment, long sales cycles, and poor customer experience. Finally, we share insights and best practices for transforming identity verification and document signing processes to improve compliance, eliminate human error, and reduce the risk of fraud.

Technologies covered include e-signature, digital identity verification, fraud screening, agreement automation, and audit trail capture.



Client onboarding is a largely manual, error-prone, time-consuming, expensive, incomplete and ineffective process.

It often aggravates consumers and financial firms alike, and regulators have found it to be rife with ineffective controls that allow breaches of Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations, as well as a host of other global laws and rules aimed at protecting consumers and lowering the risk profile of financial services institutions.”²

Transforming Client Onboarding, KPMG



TYPE OF RISK:
POOR CUSTOMER
EXPERIENCE (CX)

4/5

Of the top 5 reasons why customers would use a nonbank provider, 4 relate to user experience

Ernst & Young

43%

Of those who experienced low satisfaction during onboarding indicated they will “definitely or probably” switch banks as a result

Digital Banking Reports³

1. Go Digital: Manual Steps Slow Sales Processes and Frustrate Customers

For some financial institutions, account opening and onboarding processes still involve cumbersome tasks such as form filling, manual data input, or visiting a branch. Financial agreement processes can also involve a mixture of digital and manual steps.

Consider this process for a loan application: The applicant fills out their details online (digital process) and receives documents by email (digital) – so far so good. But then, they're asked to go into a branch to show ID (manual) and complete and sign paper documents in-person (manual). Add customer due diligence (CDD) checks and the whole process can take several days due to these requirements.

No wonder so many applicants abandon mid-way.

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

Applicants are less willing to accept slow, manual processes. They will not tolerate lengthy account opening and agreement 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, through an intermediary, or face-to-face. Friction in their journey **increases the risk of lost sales and decreases an institution's ability to compete.**

When automating account opening and financial agreement processes, many financial institutions start with just one part of the process, such as adopting basic e-signature capabilities or digital application portals. These companies soon find semi-automated processes insufficient both from a customer experience and risk perspective because they drop to paper and/or require manual due diligence work during the application process.

If your account opening and financial agreement processes include a mix of manual and digital steps, ask yourself:



Are we offering the type of experience today's customers want?



How many manual steps are there in our processes? What can we remove?



Are we losing customers due to friction? How can we reduce abandonment rates?



How much time and money could we save by eliminating manual work?



Are digitally savvy competitors gaining an advantage?

How technology can address this issue:

Technology platforms allow financial institutions to digitize each stage of the process – from identity verification to document presentation, 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.

With the right technology, processes are completed in minutes - at a fraction of the cost. Consulting firm McKinsey has calculated that financial institutions can cut costs by up to 90% through deployment of workflow tools and digital account opening and onboarding capabilities.⁵



TYPE OF RISK:
POOR CUSTOMER
EXPERIENCE (CX)



TYPE OF RISK:
OPERATIONAL

2. Strip Out Manual Checks: Manual Checks are Inefficient and Increase Risk of Human Error

If your account opening and financial agreement processes include manual form-filling steps, then human error could expose you to **poor customer experiences and an increase in operational risks**, leading to lost sales and higher operating costs.

There are many things people do better than machines, such as building trust and establishing relationships. But people are also prone to errors and mistakes. The cost of fixing mistakes such as incorrectly signed agreements, inaccurate data on forms or documents, or missing pages can be substantial. Forms, applications, and agreements that contain mistakes will need to be re-submitted or re-keyed and the mistakes corrected. Where this isn't possible, sales are lost.

For one major European bank, 48% of all applications involving manual data capture were re-keyed due to human error, doubling acquisition costs.⁴



If your documents need to be checked for errors, ask yourself:



What is our document error rate?



What controls are in place to ensure not-in-good-order documents cannot progress?



How much do errors cost both directly and through lost business?



By automating this step, can time be freed up to focus on higher value tasks?



Why hasn't the document verification step been automated?

How technology can address this issue:

Technology can enforce workflow and business rules throughout the process, eliminating errors and saving millions in operational costs.



TYPE OF RISK:
POOR CUSTOMER
EXPERIENCE (CX)

3. Digitize ID Checks: Requiring Applicants to Bring Physical Copies of their ID Documents into a Branch Causes Friction and Increases Abandonment

The more hoops an applicant has to jump through when opening an account or applying for a financial product, the more likely they are to get frustrated and walk away. Each stage of the process that requires an applicant to complete a manual or inconvenient task (such as printing documents, scanning, or presenting identity documents in-person), is a point of friction that contributes to a poor experience.

Poor customer experiences lead to high abandonment rates as applicants look elsewhere.



“Application abandonment rates are still between 65% and 95%, depending on the product.”⁶

“Checking application abandonment rates are dependent on the banking channel, the number of steps required, and the overall user experience.”

Tiffani Montez,
Senior analyst, Aite Group

If your processes offer applicants a poor user experience or necessitate that applicants complete time-consuming manual steps, then you run the **risk of losing sales**. Not only that, but manual ID checks are slower and more costly than automated checks.

Automating applicant identity verification with digital checks gives financial institutions control over the identity verification process and the ability to prove an applicant's identity quickly and compliantly.



TYPE OF RISK:
POOR CUSTOMER
EXPERIENCE (CX)

If you are losing sales due to abandonment, ask yourself:

- Are we offering the type of identity verification experience that today's customers want?
- How many customers are we losing due to abandonment?
- Are we able to tailor the experience and choose an identity verification method (or methods) according to the level of risk in the process?
- What changes do we need to make to verify an applicant digitally while remaining compliant with all relevant regulations?
- Do we have full control over the identity verification process?

How technology can address this issue:

Financial institutions (FIs) should invest in technology to digitally verify an applicant's identity – whether that applicant is being verified remotely or in-person. There are many digital identity verification methods, from one-time passwords (OTP) to knowledge-based authentication (KBA), to biometric verification.

These methods are offered as point solutions through multiple technology providers, but FIs that want to use multiple verification methods (or optimize the verification method for risk profiles or agreement types) should consider investing in a single solution from a verification hub provider.

A verification hub integrates with multiple third-party identity and verification providers, so the FI doesn't have to. Through a verification hub, FIs can access a wide range of identity and verification check types, all through a single API integration and without contractual restrictions from multiple vendors. FIs can then design and adjust multi-check verification workflows over time to optimize for customer experience (CX), efficiency, and risk mitigation.

Point solutions typically offer a limited number of verification methods and require a separate integration for each solution. In addition, integrating multiple point solutions does not give FIs the ability to optimize check types and workflows for CX, efficiency, and risk, or enable FIs to change check types as requirements change or as new technologies come to market.



TYPE OF RISK:
FRAUD

4. Fight Application Fraud with Digital ID Checks: Achieve KYC Compliance Without Impacting the User Experience

Fighting application fraud is an uphill battle for financial institutions. As first-party fraud continues to grow, it is increasingly important for FIs to determine and prove who they are transacting with. To mitigate the **risk of application fraud**, many FIs are turning to technology to help them validate the identity of an applicant and prove the validated identity is genuinely the individual they are interacting with.



In faceless delivery channels, such as online, mobile, and contact centers, using identity document capture and verification can enable a company to ensure that the identity document is legitimate and has not been tampered with, and comparing a selfie to the picture on the document can ensure that the owner of the document is on the other side of the device."

**Application Fraud: Fighting an Uphill Battle,
Aite Group, 2018**

Automated ID checks allow financial institutions to prove they know who the applicant is (referred to as Know Your Customer verification), and that the applicant is genuinely the person they are interacting with (referred to as Prove Your Customer verification).

- **Know Your Customer (KYC)** verification can be achieved digitally by matching application data (such as name, address, date of birth, and bank details) to trusted data sources such as voter lists and identity bureaus. This can mitigate the risk of first party, third party, and staff application fraud by screening applicant details against negative data to identify fraud and AML activity. IP geo-location, device verification, and corporate checks also contribute to building a strong verification profile for an applicant. Capturing data from an identity document enables an FI to use that data to prefill other documents, such as credit card or checking account applications. This also eliminates many keying errors that normally lead to additional back-office work, thus improving operational efficiency.⁷
- **Prove Your Customer (PYC)** verification can be achieved digitally via methods such as two-factor authentication, SMS verification, knowledge-based authentication, document verification, biometrics, or facial comparison. Behavioral biometrics, used by 7% of FIs, is another relatively new technology that can help in identifying human versus nonhuman or bot behavior, as well as normal applicant behavior versus fraudster behavior during the application process.⁸



TYPE OF RISK:
FRAUD



The law says you must have a true and proper approach to verifying your identity... the triangulation you end up doing between verifying someone's mobile number, their fingerprint, with another piece of data like their address, is actually far more solid than someone's signature."

Kirsty Roth,
Group Head of Operations, HSBC

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



Does our current identity verification process fully protect us and our customers against first party, third party, and staff application fraud?



Does our process prove that the applicant exists?



Does our process protect against application fraud?



Are we using the most appropriate identity and verification checks?



Are we able to conduct multiple checks from different providers without adding friction to the customer experience?



If one method of identity verification fails, can we conduct additional checks on a customer without adding risk?

How technology can address this issue:

Digital verification checks allow financial institutions to prove who their applicant is, and that they are in fact the person the FI is transacting with. Recent research from Aite Group found that 90% percent of FIs indicate plans to implement mobile identity document capture and verification solutions within the next two years.⁹

By offering a range of KYC and PYC check methods via a single integration, verification hubs equip financial institutions with future-proof solutions that allow them to add and manage check types as requirements change and as new check types come to market.

Look for a vendor that can provide you with access to multiple KYC and authentication methods such as:

- Mobile ID document capture
- Identity document check
- Biometrics verification
- OTP authentication
- Risk assessment
- Adaptive authentication
- And more



TYPE OF RISK:
POOR CUSTOMER
EXPERIENCE (CX)

5. Future-proof Your Solution with Multiple Digital Identity Verification Methods: A Single Inflexible Verification Method Can Lead to High Fail Rates & Security Vulnerabilities

If you have high fail rates for ID verification, then you could **be losing out on sales and offering a poor customer experience**. Some financial institutions that have integrated digital ID verification into their account opening and financial agreement processes encounter this problem as they are limited to one method of verification. By integrating multiple identity verification methods, providers can reduce fail rates and increase sales.

If you are experiencing high fail rates for digital ID verification, ask yourself:



Are multiple ID verification methods integrated into our solution?



Do we support checks against multiple bureaus?



If so, can we manage multiple identity verification providers through a single integration and contract, or do we have the added complexity of multiple suppliers, contracts, and integrations?



How resilient are our digital identity verification methods if a provider has an outage or cannot verify an applicant?

How technology can address this issue:

Verification hubs increase the chance an applicant can be verified, while also eliminating the risk of business interruption from bureau outages.

Integrating identity verification into digital account opening and financial agreement processes via a hub platform (which integrates with multiple ID & verification partners), helps financial institutions to:

- Reduce reliance on a single bureau or identification method
- Increase the chance that an applicant can be verified
- Minimize provider outage risks



TYPE OF RISK:
ENFORCEABILITY

6. Create Legally Enforceable Agreements: Collect Digital Audit Trails to Prove the Applicant Intended to Enter into the Agreement

Financial institutions looking to replace traditional manual steps such as ink signatures, paper forms, and in-person ID checks, should also consider whether their digital processes protect against legal disputes and the **risk of unenforceable agreements**.

Replacing a traditional ink signature with an e-signature is a legal method of capturing an applicant's consent in many countries (for a full review of global e-signature legislation see *Electronic Signature and the Law: Global Legislation Review*). When evaluating e-signatures, look for technology that is able to provide a **complete audit trail** of exactly what the applicant saw and did during the verification, authentication, and signing process. Audit trails can protect financial institutions from legal disputes.

Leading e-signature lawyer Lorna Brazell advises financial institutions that electronically signed agreements, although legal, may not be enforceable in the event of a challenge if the financial institution cannot also provide an audit trail of the applicant's interactions (including an audit trail of how the applicant's identity was digitally verified).¹⁰ Unenforceable agreements are a huge risk to financial institutions. If FIs can't enforce their portfolio of loans then the whole portfolio is at risk of being worthless.

David Whitaker, a lawyer at DLA Piper, adds that banks must be able to demonstrate that electronically signed documents are protected, and that they can't be changed after they're signed. They also need to be able to demonstrate the process, down to the specific screenshots the applicant sees, for putting an electronic signature on a document. "You want to be able to show at the courthouse what the customer experienced," he says.¹¹

If your financial agreements risk being challenged in a legal dispute, ask yourself:



Does our agreement process provide strong evidence of identity, intent, and consent, in order to prove compliance?



Does our agreement process provide an audit trail of the applicant's interactions before, during, and after signing the agreement?

How technology can address this issue:

Financial institutions should consider technology solutions that capture a full audit trail of exactly what the applicant saw and did during an account opening or financial agreement process.

This evidence (whether proving the identity of the applicant or their intention to enter into the agreement) protects financial institutions against enforceability challenges.



TYPE OF RISK:
ENFORCEABILITY



TYPE OF RISK:
COMPLIANCE

Since 2008, financial institutions around the world have paid over \$321 billion in fines.¹² These fines are largely due to financial and regulatory misconduct, or an inability to provide evidence to prove that compliant processes were followed.

7. Collect Digital Audit Trails: Prove Compliance and Avoid Regulatory Fines

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. FIs should look to capture as much detail as possible about the transactions that take place with customers and partners, so that they are able to prove compliance when required to do so.

Compliance and enforceability are major concerns for financial services companies. 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 from regulating bodies. Technology can help FIs deal with different regulations and capture 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 and customer agreement process fair and compliant?



Do we capture an audit trail throughout the process?



If so, how do we collect evidence to prove it?



Does the audit trail prove the identity of the applicant as well as what the applicant saw and did during the agreement process?

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 trail 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 a financial institution's ability to enforce an agreement if challenged.



TYPE OF RISK:
ENFORCEABILITY

8. Provide Strong & Persuasive Evidence: Ensure Audit Trails are Complete and Tamper-Proof

As well as capturing audit trails to prove compliance, financial institutions should consider whether those audit trails are strong and persuasive enough to be legally defensible.










Strong and persuasive audit trails need to have integrity and be easy to understand. If audit trails do not meet these criteria, then financial institutions **risk unenforceable agreements**. Audit trails that are incomplete or that have not been tamper-sealed may be considered unenforceable if challenged by an applicant, customer, judge, regulator, or auditor.

E-Signature lawyer Lorna Brazell advises that audit trails should:

- Be a derivative of a specific transaction and that transaction only
- Be stored in one location only (not stored in bits and bytes across multiple folders and systems)
- Not have changed by accident or design
- Not have been lost or deleted (wholly or partially)
- Be easy to find and retrieve
- Be easily intelligible by non-technical individuals

Audit trails that meet these criteria contribute to a stronger position with regards to compliance, fair conduct, and agreement enforceability.

If you are unsure whether your audit trails are strong and persuasive, ask yourself:

- | | |
|--|--|
|  Is each audit trail linked solely to its corresponding transaction? |  How easy is it to find and access our audit trails? |
|  Are our audit trails spread across different file storage systems or archived with third-party vendors? |  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? |
|  Are our audit trails tamper sealed? |  Is it possible to store and move our audit trails without compromising their integrity? |
|  Could our audit trails be lost or deleted? |  Are our audit trails easy for non-technical people to understand? |
|  Do our audit trails cover every step in the agreement/sign-up process, including identity verification and authentication? | |

How technology can address this issue:

Technology platforms that digitize account opening and financial agreement processes can capture an audit trail of exactly what the applicant saw and did during a transaction, and store that audit trail in a secure and tamper-proof way.

The right platform will also provide the flexibility for the audit trails to be stored in the financial institution's system of record without compromising their integrity.



TYPE OF RISK:
COMPLIANCE

9. Deploy a Flexible Solution: Future-proof Against Market, Legal, and Regulatory Changes

Change is an inevitable part of the financial services industry. It comes in many forms and can be caused by factors from within the business or outside of your control.

Adapting to these changes requires processes and technology that can be easily updated. If technologies cannot be updated, digital account opening and financial agreement processes **risk becoming non-compliant, obsolete, or operationally expensive.**

If you require the flexibility to adapt to future changes, ask yourself:



Is it likely that new regulations will impact our account opening and agreement processes?



Is it possible to update our processes as changes occur? Can this be done without multiple integrations and prohibitive cost?



Are we likely to expand into new geographies or product areas?

How technology can address this issue:

Financial institutions should look for technology providers with digital solutions that are future proofed against both internal and external change factors.

Future-proofed solutions will include factors such as the flexibility to add additional steps to a workflow or otherwise adapt a workflow. These additional steps could include the requirement for an applicant to read an extra document, check an extra box, consent to new terms, or verify their identity using a new method.



Conclusion

Financial institutions face an increasingly competitive market. In a recent survey, researchers found that four out of five reasons applicants would use a non-traditional finance provider relate to user experience.¹³ In this competitive environment, FIs with the best customer experience will win new customers and secure the ongoing customer loyalty needed to drive growth. To achieve this goal, FIs must fully digitize services such as account opening and agreement processes.

Financial institutions that embrace change must do so with two goals in mind:

1. Improve the customer experience with a seamless digital process.
2. Remove the risks inherent in their existing, paper-based account opening and financial agreement processes and mitigate ongoing risk.

Financial institutions looking to achieve both goals should start by identifying areas of hidden risk in their existing processes – whether operational, compliance, CX, fraud or enforceability risks. They should then look to adopt processes and purpose-built technologies that mitigate these areas of risk.

By 2020, FI executives project that less than half (47%) of DDA [Demand Deposit Account / Checking Account] applications will be submitted in branches, and submissions through online and mobile channels will grow to 45%, with contact center volume changing only slightly.”¹⁴

Application Fraud: Fighting an Uphill Battle, Aite Group, 2018

The benefits for those that achieve these two goals are huge – a better customer experience due to low friction, as well as increased sales, reduced operational costs, and enforceable agreements. For those that don't, the costs are significant. Financial institutions looking to avoid non-compliance, regulatory fines, lost sales, and legal disputes should act today.

¹ Aite Group, Application Fraud: Fighting an Uphill Battle, 2018

² KPMG, Transforming Client Onboarding, 2018, <https://assets.kpmg.com/content/dam/kpmg/pdf/2015/03/kpmg-client-onboarding.pdf>

³ Digital Banking Report Media, 2017 Account Opening and Onboarding Benchmarking Study

⁴ McKinsey, 2014, www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-rise-of-the-digital-bank

⁵ Anonymous client survey

⁶ Aite Group, Transforming the Digital Account-Opening and Onboarding Experience, 2018

⁷⁻⁸⁻⁹ Aite Group, Application Fraud: Fighting an Uphill Battle, 2018

¹⁰ Osborne Clarke, E-Signature best practice for UK financial services companies, 2016

¹¹ American Banker The Circuit: An E-Signature Event, www.americanbanker.com/news/the-circuit-an-e-signature-event

¹² Reuters, www.reuters.com/article/us-banks-fines-idUSKBN1692Y2

¹³ EY, Global Consumer Banking Survey, 2016

¹⁴ Aite Group, Application Fraud: Fighting an Uphill Battle, 2018



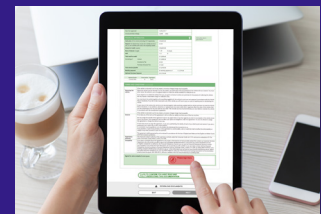
OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.



Copyright© 2019 OneSpan North America Inc., all rights reserved. OneSpan™, the "O" logo, "BE BOLD. BE SECURE.™", DEALFLO™, V-HUB™, DIGIPASS® and CRONTO® are registered or unregistered trademarks of OneSpan North America Inc. or its affiliates in the U.S. and other countries. Any other trademarks cited herein are the property of their respective owners.

Last Update March 2019.

FIND OUT MORE
ABOUT AGREEMENT
AUTOMATION



CONTACT US
info@OneSpan.com
OneSpan.com