IRTA International RegTech Association

protiviti® Face the Future with Confidence

# An Urgent Call for KYC Optimization

*A global market study calling for KYC innovation and collaboration*

# Foreword from the International RegTech Association (IRTA)

This global market study is an important milestone for the IRTA in delivering on our goal of demonstrating how better outcomes for consumers, businesses and society can be achieved by accelerating the adoption of regulatory technology (RegTech) globally. We are incredibly grateful to Protiviti for producing this report with us and for the input of IRTA members, partners and all contributors.

This study focuses on the optimization of anti-money laundering (AML) know your customer (KYC or AML/KYC) processes. It provides a blueprint for broader adoption of RegTech to enable better regulatory compliance and improve the efficiency and effectiveness of compliance processes.

We believe it is essential for policymakers, regulators, institutions and solution providers to align on their understanding of new digital technologies and how they can be used to redesign and transform current processes.

Developing a joint understanding of the effectiveness of these technologies on processes, controls and risks is one side of the coin. The other is having a shared knowledge of the significant risks of continuing to rely on legacy approaches. Legacy risk is recognized by organizations and institutions already engaged in the optimization of KYC, including many whose work we examined in this study.

Our recommendations lay out how existing policy frameworks and mechanisms can be leveraged to drive the understanding, testing and adoption of KYC optimization. We also suggest practical next steps for creating new mechanisms and digital assets that can help institutions overcome key challenges to KYC optimization within and across jurisdictions.

Richard Maton

Executive Board Member
& Strategic Initiatives Lead, IRTA

# Contents

*Protiviti and the IRTA do not make any warranties or representations regarding the content of this publication nor assume any responsibility for any errors that may appear in this publication. Protiviti and the IRTA specifically disclaim any implied warranties of merchantability or fitness for any particular purpose.*

# Current KYC controls are onerous and costly

Current anti-money laundering (AML) and know your customer (KYC) processes are ineffective and inefficient and result in poor customer experience. Complex KYC requirements also have the unintended consequence of adversely impacting financial inclusion in some jurisdictions.

## Ineffective

Organizations using technology to prevent financial crime are almost **twice as successful at performing KYC identity checks (47%), compared to those that don't use technology (28%),** according to more than 3000 respondents surveyed by Refinitiv in 2019.[1]

KYC remediation programs have become **repetitive check-the-box exercises** rather than a process that enables financial institutions (FIs) to understand and effectively mitigate financial crime risks.[2]

## Inefficient

In a survey of 250 C-suite executives, 54% reported that the **absence of a single client view of all data and documentation** was a challenge during onboarding of a new client or when migrating an existing client to a new product.[3]

Fenergo estimates that up to 80% of FIs' AML/KYC programs share commonalities, meaning that institutions perform the exact same compliance procedures and processes on the same customers, **delivering zero differentiation or competitive advantage**.[4]

## Poor Customer Experience

The KYC onboarding process for new corporate customers continues to worsen, with the length of onboarding taking an **average of 32 days, compared to 28 days just three years ago**, according to a 2017 report by Thomson Reuters.[5]

In an industry survey, 81% of FIs said ineffective data management lengthens onboarding and negatively affects customer experience. Poor customer experience relating to client onboarding and client lifecycle management costs banks **$10 billion in lost revenue per year**, according to the report.[6]

## Lacking Financial Inclusion

The Financial Action Task Force (FATF) points out that approximately **2.5 billion adults worldwide lack access to a formal bank account**, which amounts to 50% of the world's population.[7] Use of e-identity tools, can support financial inclusion while appropriately mitigating the money laundering and terrorist financing (ML/TF) risks.[8]

To receive formal financial services, customers must have a verifiable identity, which many are not able to provide. The Alliance for Financial Inclusion (AFI) suggests **building digital identification and eKYC systems** to simplify access to the financial system.[8]

# Stakeholder interviews echoed current state concerns

Based on qualitative interviews with more than 70 KYC leaders across 14 jurisdictions, many areas needing enhancements were identified.

**Regulatory requirements and expectations vary.**

“For customer identification, the U.S. requires four data points at a minimum compared to China, which requires only name and ID, or Australia, where no ID number is required. For identity verification, the U.S. does not enforce prescriptive mandates, though China requires face-to-face verification and consultation with the state, while Australia has the liberty to rely solely on digital resources.”

*— Senior Director, Global Financial Institution*

**KYC requirements impact financial inclusion.**

“Large swaths of the population are detached from mainstream finance because they lack formal ID documents.”

*— U.S.-Based Innovator and Thought Leader*

**KYC refresh is a huge burden.**

“Refreshing KYC information is a pain point, since we have tens of millions of customers in the U.K. and have to refresh KYC data across multiple lines of business that have many of their own systems and are relatively siloed. Despite a multiyear initiative we have undertaken to address this issue, we still only have a 25% KYC refresh success rate.”

*— Executive, Global Financial Institution*

**Poor quality of KYC data impacts the effectiveness of transaction monitoring.**

"There is no good ongoing mechanism to ensure quality KYC data. We receive many false positives in the transaction-monitoring system (an associated process) that become difficult to disposition because of this poor KYC data.”

*— Executive, U.S.-Based Financial Institution*

**Protracted onboarding adversely affects customer experience.**

“We lose 30% to 40% of our clients during onboarding because the process can take up to 12 weeks; half of those clients leave because they are bored of the process. Current data-collection methods are manual and siloed; this creates frustration with customers who expect a seamless process.”

*— Executive, Japan-Based Financial Institution*

**Difficulty selecting the right digital vendor has stymied innovation.**

"If you don’t trust the digital service vendors, you can’t test the solutions they are offering. Trust is integral to innovation. You need that to be able to try solutions in sandboxes.”

*— U.S.-Based Innovator & Thought Leader*

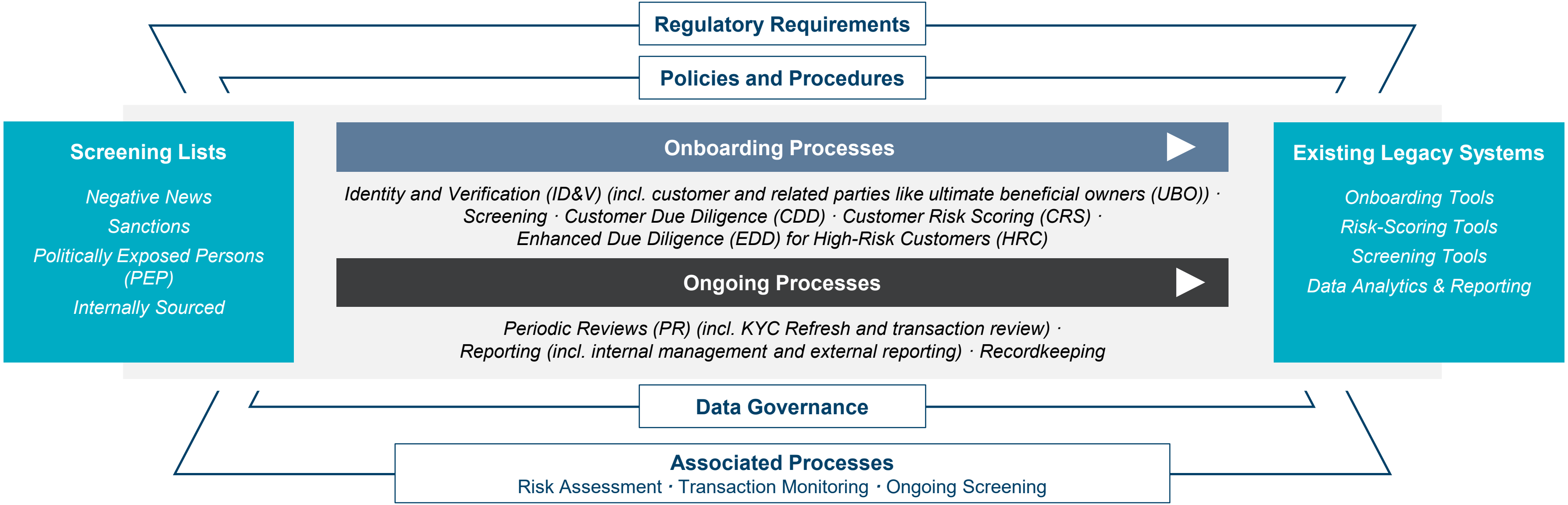
**KYC shared platforms are underutilized largely due to a lack of common data standards and concerns over privacy.**

“In many jurisdictions, corporate customers are reluctant to participate in a shared-platform model until common standards are defined and implemented. This problem can be resolved if national governments, regulators and financial institutions come together to create an agreeable set of data standards and regulations.”

*— European Union and United Nations AML Adviser*

# KYC includes complex interconnected processes

KYC includes several intertwined processes. The illustration below shows key KYC processes that the IRTA and Protiviti examined as part of this study, which provides recommendations on optimizing these processes.



**Regulatory Requirements**

**Policies and Procedures**

**Screening Lists**

*Negative News*

*Sanctions*

*Politically Exposed Persons (PEP)*

*Internally Sourced*

**Onboarding Processes**

*Identity and Verification (ID&V) (incl. customer and related parties like ultimate beneficial owners (UBO)) · Screening · Customer Due Diligence (CDD) · Customer Risk Scoring (CRS) · Enhanced Due Diligence (EDD) for High-Risk Customers (HRC)*

**Ongoing Processes**

*Periodic Reviews (PR) (incl. KYC Refresh and transaction review) · Reporting (incl. internal management and external reporting) · Recordkeeping*

**Existing Legacy Systems**

*Onboarding Tools*

*Risk-Scoring Tools*

*Screening Tools*

*Data Analytics & Reporting*

**Data Governance**

**Associated Processes**

Risk Assessment · Transaction Monitoring · Ongoing Screening

***Note:*** *While the KYC processes listed in the framework apply to both individual and corporate clients, the time to complete these activities is much longer for corporate clients than for individuals because of information-gathering requirements on related parties, which may include multiple individuals, entities and beneficial owners.*

# KYC optimization study: Scope and approach

Protiviti and the IRTA conducted a global study to investigate the effectiveness of existing KYC processes, their impact on customer experience across various jurisdictions and the efforts by financial institutions to innovate KYC controls. Information on the study is provided below.

## Methodology

- The study targeted leading financial centers and markets that are at various stages of KYC innovation efforts.
- Extensive interviews were conducted with stakeholders, including government and regulatory agencies, financial institutions, and KYC digital solution and shared platform providers, as well as innovators and thought leaders.
- In addition, the study relied on a wide range of official documents, such as corporate announcements, regulatory filings and reports on digital initiatives.

## Jurisdictions

Australia
The Baltics
Canada
China
Germany
Hong Kong
India
Japan
Netherlands
Scandinavia
Singapore
U.A.E.
U.K.
U.S.

## Stakeholders

| | |
|---|---|
| **8** | Government and Regulatory Agencies |
| **16** | Financial institutions |
| **14** | Digital solution and shared platform providers |
| **12** | Innovators and thought leaders |

Based on the study results, we developed strategic views on the following:

**Key enablers to optimize KYC · Potential future-state roadblocks · Recommendations for KYC optimization**

# KYC stakeholders recognize the need to work smarter

Current KYC controls and processes are manually intensive and time-consuming, frequently result in poor customer experience and can hinder financial inclusion. FIs can overcome these roadblocks by adopting digital solutions and digitally enabled shared platforms to optimize KYC processes. KYC optimization also requires the engagement of government and regulatory agencies to adapt existing regulatory frameworks and mechanisms and develop new ones as needed.

## Key Enablers

- Expanded use of **KYC digital solutions,** such as artificial intelligence, machine learning and distributed ledger technology (DLT), will reduce time and cost of KYC operations.
- Establishing and utilizing digitally enabled **KYC shared platforms** will eliminate redundancies in processes and improve customer experience.
- Use of both **KYC digital solutions and shared platforms** will dramatically enhance quality of data and make other interrelated processes, such as transaction monitoring, more effective.

## Key Roadblocks

Factors preventing wider adoption of digital solutions and shared platforms include:

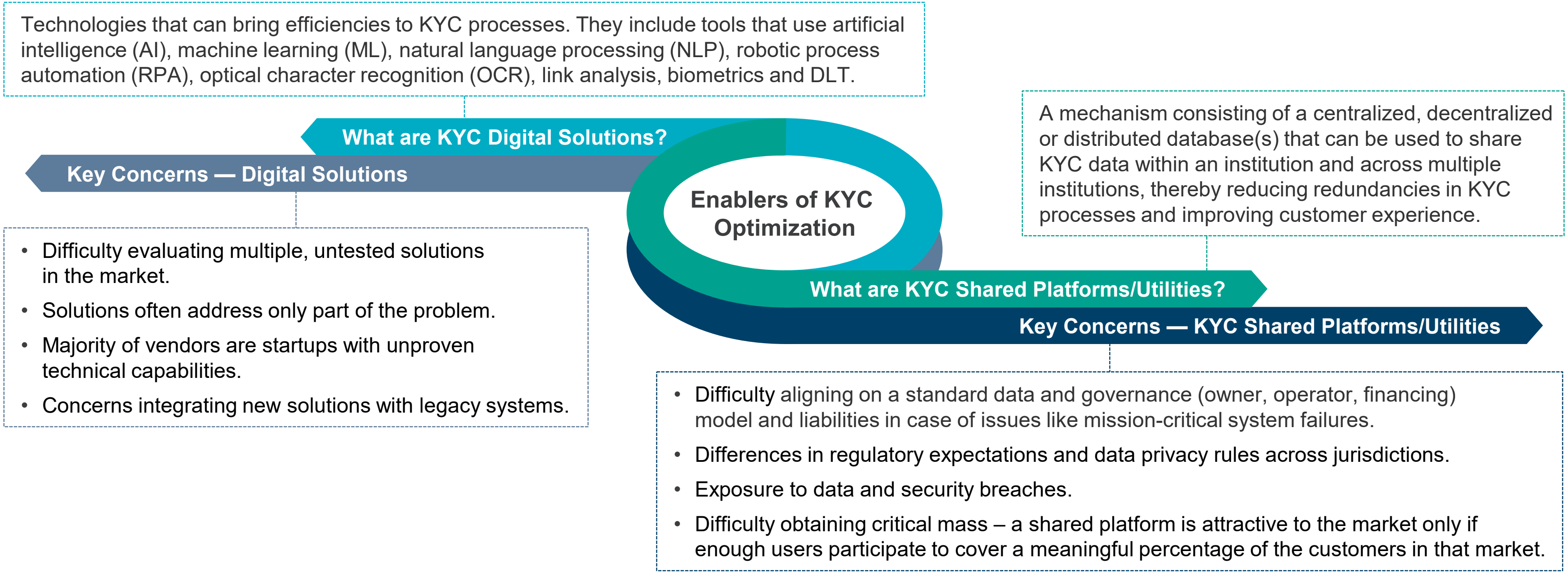
- Differing understanding and viewpoints among regulators and FIs over the impact of new digital technologies on regulatory outcomes and burdens.
- Lack of clarity around the responsibilities of stakeholders in mandating, adopting and developing standards and commercial models for public-private shared services.
- Concerns over data strategy and integrating legacy systems with new digital solutions and shared platforms.
- Difficulty on the part of FIs with evaluating the many unproven digital solutions in the marketplace.
- Conflict between KYC and data privacy requirements can prevent data sharing.

## Getting There

- Regulators need to clear the path for innovation by developing consistent regulatory standards and mandating the development of common data models to support KYC optimization, including enabling secure information sharing. Key activities include adapting existing regulatory frameworks and mechanisms and creating new shared industry assets to support KYC optimization.
- KYC stakeholders should form public-private partnerships to enable data sharing and operationalize KYC shared platforms. Clearly articulating best practices for the development of shared platforms and clarifying roles and responsibilities of stakeholders will enable and accelerate data sharing.
- FIs should design a KYC optimization strategy supported by their boards and senior management. This means prioritizing data integrity and data governance initiatives and committing to modernizing legacy systems that house KYC data.
- Digital solution vendors should deepen their understanding of KYC processes and increase stakeholders' understanding of KYC digital solutions. They should either broaden their solutions or partner with other vendors to address KYC challenges more holistically.
- Regulators should foster a culture of tech activism rather than one that is tech-agnostic. Tech activism requires regulators to be actively technology-informed, and to develop views on specific technologies without endorsing actual vendors.
- Regulators should support a competitive marketplace for continuing development of innovative digital solutions.

# Digital solutions and shared platforms hold great promise for KYC optimization

Greater adoption of digital solutions and digitally enabled shared platforms, jointly referred to as key enablers in this report, will transform the current KYC framework. KYC optimization, encompassing the use of both enablers, is also a key to increasing financial inclusion. While some FIs use certain digital technologies to enable KYC processes, myriad challenges have prevented optimization of KYC.



Technologies that can bring efficiencies to KYC processes. They include tools that use artificial intelligence (AI), machine learning (ML), natural language processing (NLP), robotic process automation (RPA), optical character recognition (OCR), link analysis, biometrics and DLT.

**What are KYC Digital Solutions?**

**Key Concerns — Digital Solutions**

- Difficulty evaluating multiple, untested solutions in the market.
- Solutions often address only part of the problem.
- Majority of vendors are startups with unproven technical capabilities.
- Concerns integrating new solutions with legacy systems.

**Enablers of KYC Optimization**

A mechanism consisting of a centralized, decentralized or distributed database(s) that can be used to share KYC data within an institution and across multiple institutions, thereby reducing redundancies in KYC processes and improving customer experience.

**What are KYC Shared Platforms/Utilities?**

**Key Concerns — KYC Shared Platforms/Utilities**

- Difficulty aligning on a standard data and governance (owner, operator, financing) model and liabilities in case of issues like mission-critical system failures.
- Differences in regulatory expectations and data privacy rules across jurisdictions.
- Exposure to data and security breaches.
- Difficulty obtaining critical mass – a shared platform is attractive to the market only if enough users participate to cover a meaningful percentage of the customers in that market.

# Cost-benefit analysis: What firms stand to gain through KYC optimization

The following are examples of estimated costs and benefits of using KYC enablers.

## Using a KYC shared platform

According to a senior executive of a multinational FI: “Since all questionnaires are standardized to the same format, and with content that is already validated by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), our time savings for onboarding correspondent banks, using the SWIFT Registry, can be as high as 50%.”[1]

## Using RPA for gathering data

After implementing an RPA tool, a European bank reduced the time spent on gathering data for KYC verification across its retail and corporate sectors from 15 minutes to 90 seconds and from 10 minutes to 70 seconds, respectively.[2]

## Using a KYC CLM tool

According to a vendor offering a corporate and institutional banking KYC client lifecycle management (CLM) tool, clients that have implemented the solution have realized an average of 30% return on investment (ROI) on technology, an average 82% reduction in onboarding time, and an average savings of 34% in audit cost.[3]

## Using an ID verification system

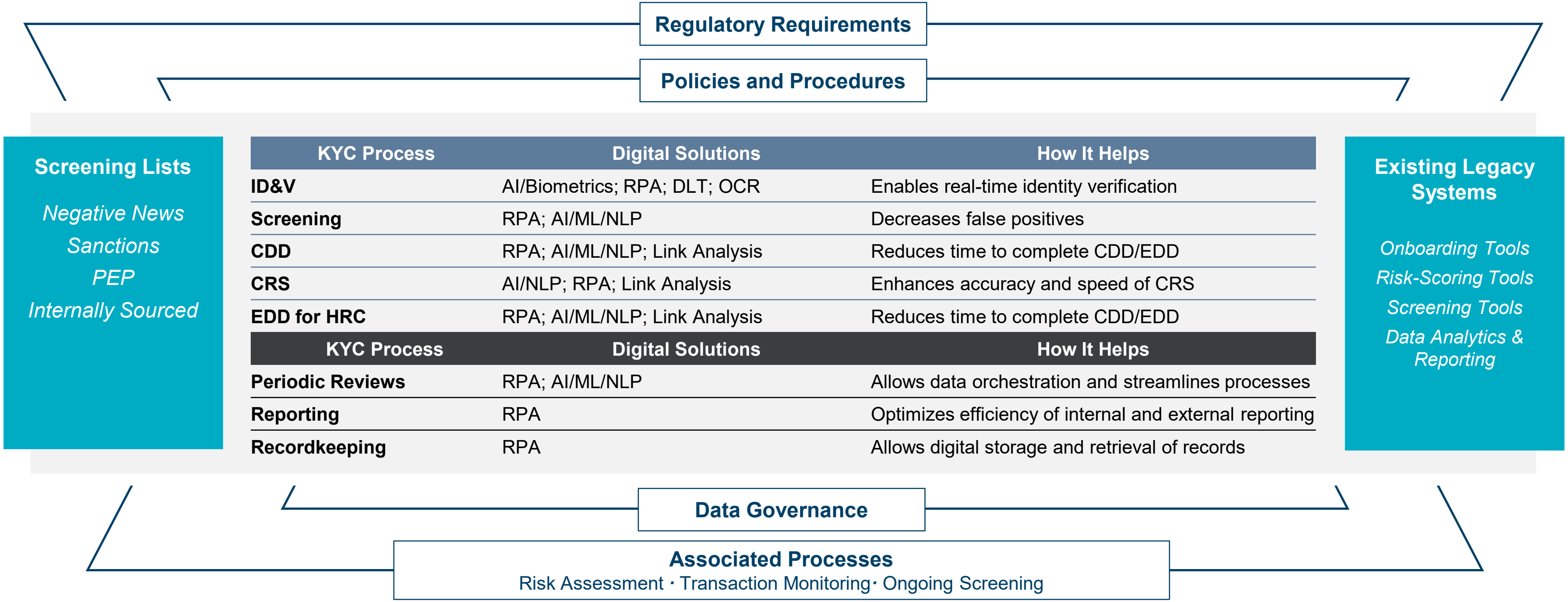
Based on research, the average time a consumer will wait before giving up on an online account-opening application is about 14 minutes. However, around one in three (29%) applications take more than 20 minutes to complete. Onboarding customers within 14 minutes is more achievable when using digital ID&V.[4]

> “The push for digitization, automation and overall change for banks, nonbanks and payment systems isn’t going to go away. Those of us on the ground trying to encourage best practices across the financial industry have a key role to play in pushing this digitization agenda.”
>
> — Official at U.S. Government Agency

# KYC Digital Solutions

# Digital solutions are increasingly impacting KYC processes

One or more digital solutions can be used to enhance KYC operational processes. However, the choice of solution will depend on many factors, including an FI's existing technology systems. The slide below is an overview of the digital solutions that can be used for various KYC processes within the framework we have established.



**Regulatory Requirements**

**Policies and Procedures**

**Screening Lists**

*Negative News*
*Sanctions*
*PEP*
*Internally Sourced*

| KYC Process | Digital Solutions | How It Helps |
|---|---|---|
| **ID&V** | AI/Biometrics; RPA; DLT; OCR | Enables real-time identity verification |
| **Screening** | RPA; AI/ML/NLP | Decreases false positives |
| **CDD** | RPA; AI/ML/NLP; Link Analysis | Reduces time to complete CDD/EDD |
| **CRS** | AI/NLP; RPA; Link Analysis | Enhances accuracy and speed of CRS |
| **EDD for HRC** | RPA; AI/ML/NLP; Link Analysis | Reduces time to complete CDD/EDD |
| **KYC Process** | **Digital Solutions** | **How It Helps** |
| **Periodic Reviews** | RPA; AI/ML/NLP | Allows data orchestration and streamlines processes |
| **Reporting** | RPA | Optimizes efficiency of internal and external reporting |
| **Recordkeeping** | RPA | Allows digital storage and retrieval of records |

**Existing Legacy Systems**

*Onboarding Tools*
*Risk-Scoring Tools*
*Screening Tools*
*Data Analytics & Reporting*

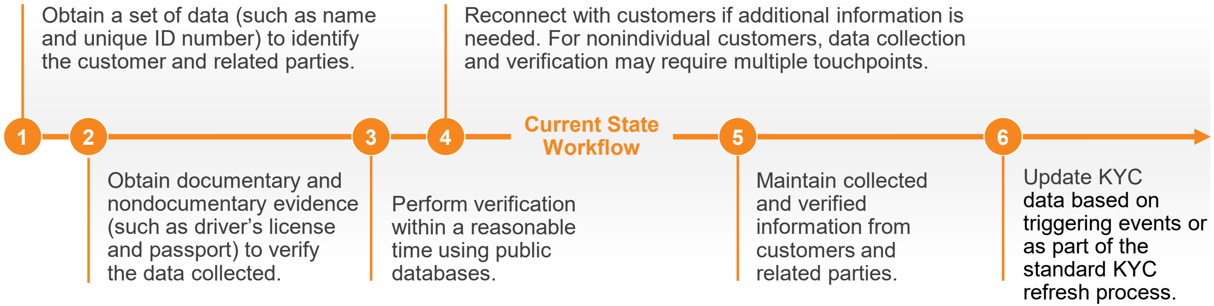
**Data Governance**

**Associated Processes**
Risk Assessment · Transaction Monitoring· Ongoing Screening

# Identity verification: AI and biometrics can dramatically streamline the ID&V process

Current ID&V requirements involve obtaining a set of data from customers, and related parties, including UBOs; verifying the information using a combination of documentary and nondocumentary methods; and storing the information collected. Employing the digital tools highlighted below will dramatically enhance this heavily manual process and allow near real-time verification. In addition, adoption and use of these digital tools will help to improve financial inclusion.

## Current State



**Current State Workflow**

1. Obtain a set of data (such as name and unique ID number) to identify the customer and related parties.
2. Obtain documentary and nondocumentary evidence (such as driver's license and passport) to verify the data collected.
3. Perform verification within a reasonable time using public databases.
4. Reconnect with customers if additional information is needed. For nonindividual customers, data collection and verification may require multiple touchpoints.
5. Maintain collected and verified information from customers and related parties.
6. Update KYC data based on triggering events or as part of the standard KYC refresh process.

**Challenges**

- A variety of inconsistent processes and a multitude of tools are used for ID verification, such as credit bureau checks and face-to-face validation.
- Manual procedures prolong the ID verification process.
- Multiple data systems maintain KYC data and adversely impact data quality.

## Digital Solutions

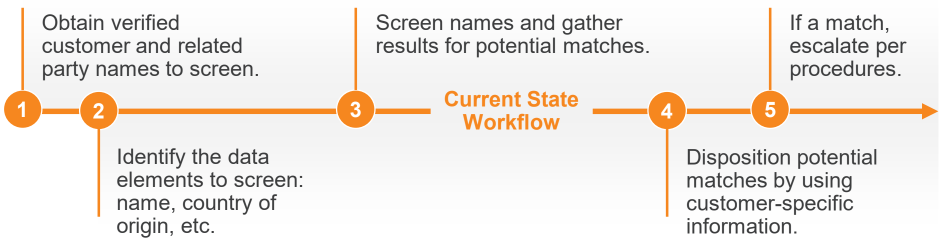
| Examples of Vendors* | What They Do | Getting to the Future State |
|---|---|---|
| • IdentityMind Global Inc.[1]<br>• Socure[2]<br>• Jumio[3]<br>• Know Your Customer[4]<br>• KYC-Chain[5] | • Use biometrics to compare facial features, captured through selfies or photos, to determine the identity of a customer.<br>• Compare the data extracts from ID documents with various online and offline data points to determine validity of the documents.<br>• Authenticate global identity documents.<br>• Share information with global registries. | • Identify KYC data required to be collected per policies and procedures of the FI.<br>• Identify KYC data being collected by each legacy system and any limitations such as field-length restriction.<br>• Standardize KYC data input requirements and streamline data fields across KYC tools at the back end, if multiple onboarding tools are being used.<br>• Use digital solutions like machine learning and biometrics, tailored to the onboarding channel, to ensure that customers and related parties are who they say they are. |

*Protiviti has and may continue to maintain business relationships with vendors listed in this study. However, the inclusion of the vendors in this study does not constitute an endorsement or recommendation by Protiviti or the IRTA.

# Screening: False positives and negatives can be reduced with digital solutions

Current KYC regulations require FIs to screen customers and related parties against relevant money laundering, terrorism financing and sanctions sources to determine if they are part of a blacklist or sanctioned-persons/entities lists, thereby posing additional risk to the institution.

## Current State



Current State Workflow

1 Obtain verified customer and related party names to screen.

2 Identify the data elements to screen: name, country of origin, etc.

3 Screen names and gather results for potential matches.

4 Disposition potential matches by using customer-specific information.

5 If a match, escalate per procedures.

### Challenges

- Current processes produce a high number of false positives and false negatives.
- Use of multiple lists results in a potential match being identified multiple times across the lists, requiring disposition of the potential match identified in each list.
- Disposition of potential matches is a manual, time-consuming process.
- Lack of real-time refreshes on internal lists creates a gap in the screening process.

## Digital Solutions

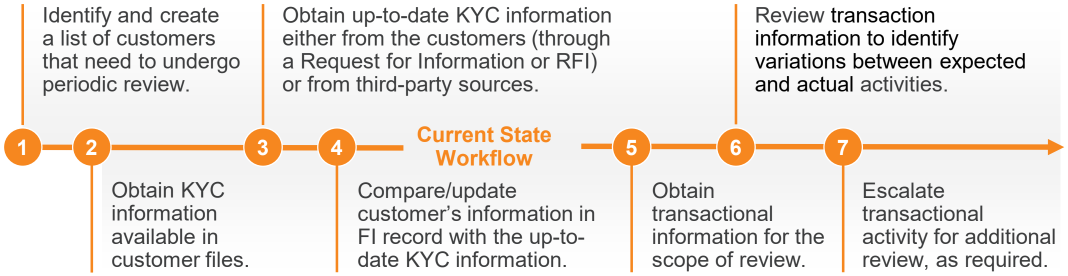
| Examples of Vendors* | What They Do | Getting to the Future State |
|---|---|---|
| • IdentityMind Global Inc.[1]<br>• Napier[2]<br>• iComply[3]<br>• Comply Advantage[4] | • Reduce false positives and negatives by verifying digital identities against a large set of data from the public domain, social networks, the deep web, the dark web and other private data sources.<br>• Machine learning-based tools can consider different dimensions within a match, such as average length of words, average similarity score and maximum similarity score and improve scoring results.<br>• AI/machine learning, coupled with RPA, enables faster, more accurate screening results. | • Establish a screening standard to define the required data fields for screening.<br>• Perform proofs of concept (POCs), with a sample of customer data, with tools that:<br>– Utilize public and private databases, including social media feeds.<br>– Use matching algorithms that account for different cases (for example, higher importance is often placed on the first name of a business, in comparison to the other names it may contain).<br>– Consolidate potential matches from various lists.<br>– Identify same entities across lists, reducing time to disposition.<br>• Compare the number of false positives and negatives resulting from the POC with those from the business as usual (BAU) processes to determine overall benefit of using these technologies.<br>• Modify algorithms as required and pilot screening on a larger sample of customer data. |

*Protiviti has and may continue to maintain business relationships with vendors listed in this study. However, the inclusion of the vendors in this study does not constitute an endorsement or recommendation by Protiviti or the IRTA.

# Periodic reviews: Data orchestration with RPA minimizes process challenges and improves accuracy

Periodic review (PR) of customer information includes refreshing KYC data and obtaining a holistic view of the transactional activity for the review period, using a risk-based approach. Currently, this activity is largely a manual process that creates a challenge for all FIs.

## Current State



**Current State Workflow**

1. Identify and create a list of customers that need to undergo periodic review.
2. Obtain KYC information available in customer files.
3. Obtain up-to-date KYC information either from the customers (through a Request for Information or RFI) or from third-party sources.
4. Compare/update customer’s information in FI record with the up-to-date KYC information.
5. Obtain transactional information for the scope of review.
6. Review transaction information to identify variations between expected and actual activities.
7. Escalate transactional activity for additional review, as required.

### Challenges

- Customers are often unresponsive to RFIs due to a lack of understanding of KYC requirements and a desire to avoid clickbait scams.
- Outdated manual processes and static data, which is often stale, create multiple customer touchpoints and make performing holistic transactional reviews difficult.
- Siloed KYC refresh approaches across business lines may result in collecting unnecessary data from customers or result in the same information being requested by different individuals within the same FI.

## Digital Solutions

| Examples of Vendors* | What They Do | Getting to the Future State |
|---|---|---|
| • Appway[1]<br>• Fenergo[2] | • Data orchestration platforms eliminate the need to manually gather information from various source systems; instead, data is extracted, formatted and loaded into a platform that can be used by analysts to compare/update KYC data.<br>• Automated searches: RPA-enabled tools allow name searches to be performed across various internal and external databases to identify potential matches that can be reviewed/dispositioned using an interface.<br>• Holistic transaction reviews: RPA and ML-enabled tools can identify variations between actual and expected activity and generate reports after extracting large data sets and grouping them by transaction type. | • Develop procedures for PR of customers (e.g., event-driven, based on risk-scoring results) and educate customers about the need for PR.<br>• Identify data fields and KYC data sources that need to be accessed to refresh data.<br>• Develop a POC using an orchestration platform, RPA bots and a workflow tool or an integrated solution of a set of customer and transaction data. Key steps include:<br>– Establish a workflow tool to streamline PR review alerts for analysts and RFIs with customers.<br>– Use a data orchestration platform/tool to review data.<br>– Establish RPA bots to extract, collate and analyze data from transaction systems.<br>• Analyze results and modify workflows/bots as required and develop a pilot starting with high-risk customers. |

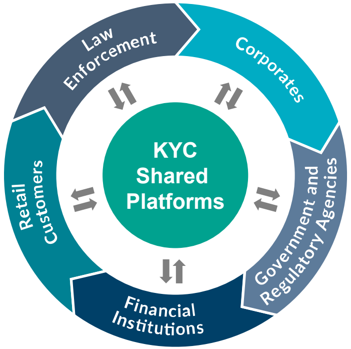
*Protiviti has and may continue to maintain business relationships with vendors listed in this study. However, the inclusion of the vendors in this study does not constitute an endorsement or recommendation by Protiviti or the IRTA.

> “Enabling more information sharing is key. Ideally, we need to get to that future nirvana state, where there is a centralized utility that maintains data on all types of customers that are using the information. At a very minimum, we need to make it easier for banks to share and use KYC data in a standard format.”
>
> — Executive, Global Financial Institution

# KYC Shared Platforms

# The shared platform model presents many key benefits

A KYC shared platform, often referred to as a KYC utility, is a standardized KYC service that allows multiple FIs to complete KYC processes such as identity verification and screening of customers and related parties in a more efficient and effective manner by using pooled KYC data.



## Key Aspects

- Currently, KYC shared platforms do not cover processes other than identity verification and screening of customers and related parties. However, there are shared platforms that can facilitate the process of obtaining additional information for CDD and EDD.
- Establishing a KYC shared platform appears to be more difficult for corporate customers than for retail customers. The need to identify UBOs and the lack of common due diligence standards for corporate customers, among participating FIs, add to this difficulty.
- Within a KYC shared platform, FIs can be providers and/or users of customer information (i.e., relying parties).
- Various reasons have hampered the widespread adoption of shared platforms. The reasons include the lack of a common data model; concerns about the security and privacy of customer data; the unwillingness of participating FIs to share customer data with competitors; the lack of clarification around the responsibilities for validating customer data; and challenges related to the interoperability of utilities.
- Multiple operating models of KYC utilities exist (see below). The choice of operating model impacts the usability of the platforms.

## KYC Operating Model Spectrum

**Decentralized Model** → **Fully Centralized Model**

| FI not using a KYC utility | Third-party managed utility | Consortium/multi-FI managed utility | Government-mandated standards/models | Government-mandated/managed utility |
|---|---|---|---|---|
| Every institution for itself. No sharing of information across FIs. | A third-party vendor establishes a KYC utility that can then be used by other participants. FIs may have some ownership of the utility.<br>**Example:** SWIFT's KYC Register | Multiple FIs collaborate to establish a KYC utility. Participation may be open or restricted to other FIs.<br>**Example:** Nordic KYC Utility | **Recommended Model:** Government mandates the development of common KYC standards and data models, allowing FIs/third parties to manage shared platforms. Multiple utilities may exist in the market. | The government or a regulatory body establishes a shared database that is then used by all FIs in the jurisdiction.<br>**Examples:** India eKYC and U.A.E. eKYC |

# Shared platforms are most useful when built with digital technologies

Shared platforms are most effective when enabled with digital technologies. Examples of these digital technologies are highlighted below.

## Digital Identity

Some shared platforms use biometrics and machine learning tools to establish, maintain and share digital identities of individuals or entities, while reducing friction for end users (e.g., India's Aadhaar).[1]

## Privacy Enhancing Technologies (PETs)

The market recently began exploring the use of PETs in KYC (e.g., FCA's July 2019 AML and Financial Crime TechSprint in London focused on applying examples of PETs to AML/KYC).[2] [3]

**Homomorphic encryption (HE):** Enables the processing of machine-to-machine encrypted data without the need to decrypt the data. Basically, HE allows data to remain encrypted while it is analyzed and processed.

**Zero-knowledge proof (ZKP):** Enables data to be verified without revealing the data itself. The technology can transform the way data is collected, used and transacted. ZKP uses the concept of a verifier and a prover. In each transaction, the prover can use the data without revealing the input or the computational process to the verifier.

## Data Sharing Technologies

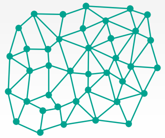
DLT, such as blockchain, underpins a secure ledger of digital events that is shared among all the parties participating in the events. Blockchain is bonded in nature, as each block can contain several transactions and has a unique proof of work attached. Together with the unique proof of work from the previous block, a chain effect is created, making it impossible to alter the information.[4]

DLT allows a high degree of data privacy and security while maintaining transparency through an audit trail of data changes. DLT uses smart contracts to help streamline roles and responsibilities in a shared platform.

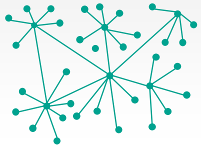
Some challenges to consider when exploring the use of DLT in KYC shared platforms include:[5]

- Agreeing on who is responsible for maintenance, especially mission critical system failures. Unlike centralized and decentralized technology, DLT has a more democratic ownership structure (see figures A, B and C).
- The permanence of personally identifiable information data added to the ledger may conflict with data privacy regulations (e.g., The General Data Protection Regulation or GDPR) which provide the "right to be forgotten."
- Lack of knowledge and education about DLT beyond its use in cryptocurrency (e.g., Bitcoin) impacts its use for KYC purposes.

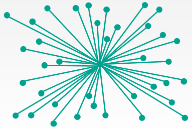
(A) Distributed



(B) Decentralized



(C) Centralized



# Learning from India's eKYC utility

In 2009, the Unique Identification Authority of India (UIDAI) was established to issue unique identification numbers, also known as Aadhaar, to residents of India and to develop and operate a database for storing the information. Since its inception, the Aadhaar program has been used to collect the unique identifiers (such as name, photo, addresses, fingerprints and iris scans) of more than 90% of India's population. More recently, FIs have been using Aadhaar for electronic KYC (eKYC) authentication, significantly enhancing the ease of performing KYC processes. Below we highlight some key benefits and challenges.

## Benefits

- **Fostered financial inclusion:** The Aadhaar ID program has allowed more people who were previously unable to overcome paperwork requirements and participate in government welfare programs to access financial services.[1]
- **Eased accessing available information:** Any agency or institution that partners with the Aadhaar program can quickly access participants' information, making the identity-verification process seamless and efficient for both the agency and the individual.[2]
- **Improved mechanisms for fighting crime and corruption:** With a centralized database, the government can track the activities of suspicious people and businesses, as well as monitor corruption in welfare programs.[1]

## Challenges

- **Multiple data breaches:** Aadhaar data has been hacked and leaked to the public multiple times, putting millions of users at risk for identity theft. In 2018, for example, 200 official government websites made Aadhaar data public via Google. There have been reports that Aadhaar information can be purchased on the black market.[1]
- **Data privacy concerns:** The use of the IDs has raised huge privacy concerns. In 2018, the Supreme Court of India ruled that private entities cannot compel customers to provide their Aadhaar number as a condition of service to verify their identity. Aadhaar is, at present, being used for eKYC; however, concerns remain over who has access to participants' data.[3]

***Recent news and observations:*** *In 2019, the Indian government amended the Prevention of Money Laundering Act of 2002 to clarify the various modes of capturing customer details electronically, paving the way for banks and other regulated entities to fully utilize Aadhaar eKYC. The success of the Aadhaar program shows the importance of having government backing for the development and sustainability of shared platforms.*[4]

# Why Singapore's KYC utility pilot initially struggled

An industry utility steering committee (IUSC), consisting of Singapore's local and large international banks, embarked on a two-year project to pilot a centralized KYC utility designed to perform end-to-end KYC tasks for corporate customers. The utility mutualized each customer record to reduce duplication and prevent criminals from exploiting the information gap among institutions. Below are some targeted benefits, as well as challenges that resulted in the initiative's failure.[1]

## Benefits

+

- **Public-private collaboration:** The project brought together operation and technology experts from both the private and public sectors to identify and authenticate reliable sources of data, harmonize KYC policy and reduce the turnaround time for completing KYC.
- **Developed a liability model:** The project established a liability model that was agreeable to all stakeholders, including upstream banks that contributed data to the utility and downstream banks that relied upon the data. The model allowed enforcement actions against banks that performed KYC poorly despite using the utility output.
- **Defined pro forma solutions for many other issues:** Pro forma solutions were developed to address relevant risk management issues, including banking secrecy, data privacy, data ownership, outsourcing risk management, technology risk management and regulation of the utility.
- **Modernized screening capabilities:** Several next-generation screening capabilities were evaluated, and a proof of concept was conducted. In a blind test, one screening engine was sufficiently differentiated in terms of higher matches and lower false positives.

## Challenges

!

- **Costs outweighed benefits**: The proposed solution was going to cost some FIs more than it would ultimately save them. Specifically costs, such as bank integration, assessed against estimated fees that could be charged by the utility weakened margins, rendering the business case inadequate.[2]
- **Data migration challenges**: The process of migrating clean and mutualized KYC data into the utility was operationally intensive and costly, as the data had to be transferred, processed and returned to the banks.
- **Overly ambitious design**: The utility underwent multiple design iterations without clarity around cost implications, leaving some FIs with an unclear path to profitability.
- **Operational risk issues**: The utility faced risks associated with data quality such as the challenge of validating data from a variety of sources, including customers, FI databases and other public sources.
- **Divergent stakeholder needs**: Participants, including the banks, regulators and other stakeholders, had different positions on certain issues. For example, FIs often had to accommodate a lengthy process of gathering requirements and aligning on a common view to achieve consensus.

***Recent news and observations:** The Singapore KYC utility pilot is reportedly being revitalized, though minimal information has been made public. Based on our discussions with industry experts, we believe the success of this shared platform hinges on the government's ability to delineate roles, responsibilities and liability for the participants. It is also important for the shared platform to be designed in a way that makes it cost-effective for FIs to participate. KYC shared platforms for corporate entities are being designed in several other jurisdictions, including in the Nordic region by a consortium of bank.*

# A digital identity project in the UK aims to put the consumer in control

The Investing and Saving Alliance (TISA), a U.K.-based nonprofit organization, is leading the development of a digital ID project for U.K. financial services consumers. TISA's goal is to create a single digital ID that meets all relevant KYC and AML regulatory requirements and is interoperable with the government's digital service (GDS) Verify scheme. The project is expected to be completed by April 2020. Highlighted below are some of its key benefits and challenges.

## Benefits

- **Broad participant engagement:** A wide range of participants, including experts with deep technical knowledge of digital ID systems in financial services, is engaged in the development of the technology. The participants' goal is to develop technology that is capable of being migrated to more complex technologies such as DLT, can interact with other digital ID systems and is cost effective.
- **Strong governance and trust framework**: Key strategic decisions, including budgetary and communication actions, are made by a steering committee consisting of participating firms. The governance structure also includes working groups tasked with delivering individual workstreams, research and third-party commissioning.
- **Enhanced consumer experience**: A single digital ID that is owned and controlled by the consumer, and is reusable across various financial services, would dramatically encourage adoption and enhance the consumer experience. The initiative will allow FIs to open new accounts at a lower cost while increasing protection of customers' personal data.
- **Design compatibility:** The digital ID technology is designed to be compatible with other digital ID programs such as Verify and the EU's Electronic Identification, Authentication and Trust Services (eIDAS). A compatible design would deliver additional benefits, including speed and convenience in accessing broader services for customers.
- **Compliance with regulations**: The digital ID technology is designed to meet all current and future AML/KYC requirements associated with GDPR, the Payment Services Directive II (PSD II) and other regulations.

## Challenges

- **Potential resource constraints**: The development of digital ID standards and technology that is interoperable with Verify and other systems will require significant investment in technical expertise and resources.
- **Commercial model challenges**: Current ID&V providers generate revenue through existing identity schemes and services. If ID&V activity is consolidated within the TISA-led consortium, it could threaten these revenue streams and prevent some ID&V providers from participating in the project.
- **Cultural barriers**: The public's distrust over the failure of an earlier U.K. initiative to develop a national ID card may impede widespread adoption of this project. Growing social concerns over data privacy and security could also impede its progress.
- **Difficulty harmonizing standards**: The different ID&V requirements for each use case, such as access to different financial services, government services and healthcare, could make it harder to establish a single digital ID standard across multiple services.

***Recent news and observations:*** *The successful adoption of a digital ID that has uniform standards and is interoperable with other digital ID programs would create immense value for both U.K. consumers and the financial services sector. While there are major challenges, there are considerable benefits to be gained in the form of quicker account opening and transfers, enhanced online security and a more competitive market.*[1] [2]

# Spotlight: Global AML & Financial Crime TechSprint

## Collaborating to develop data sharing solutions – Financial Conduct Authority (FCA) TechSprint

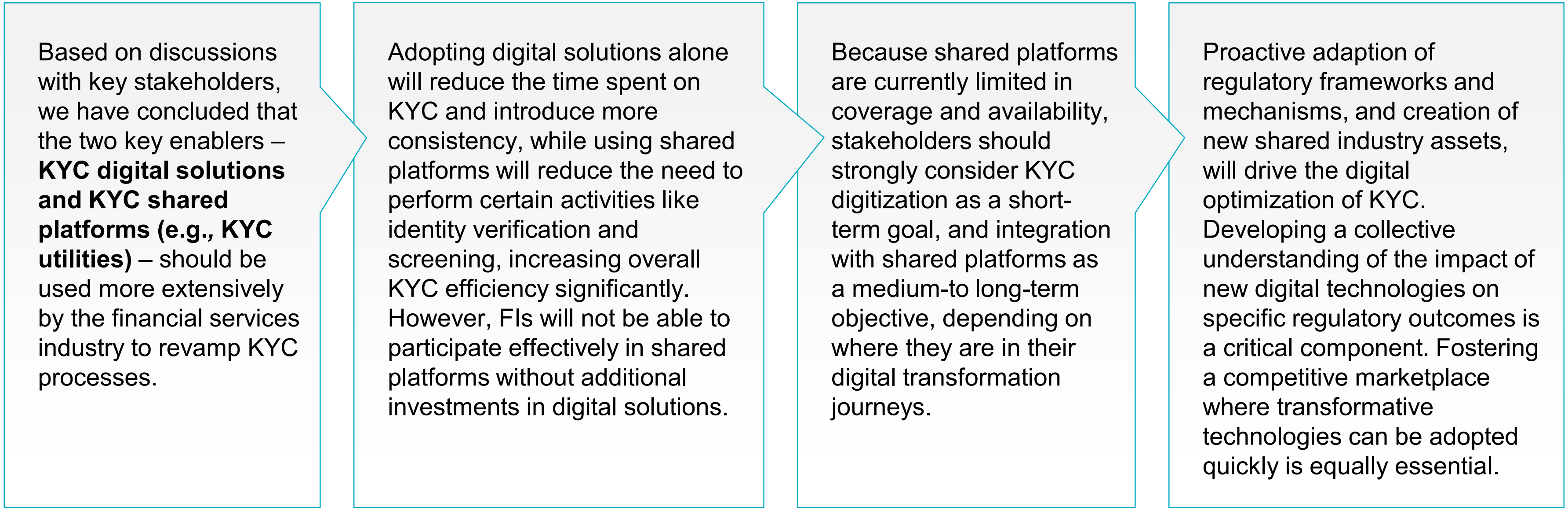
- In July of 2019, a Global AML & Financial Crime TechSprint was held in London, with a satellite event organized in Washington, D.C. The events were hosted by the FCA and the Alliance for Innovative Regulation (AIR) respectively. More than 500 participants and observers from government and regulatory agencies, FIs, digital technology vendors and consulting firms participated.
- The ability to share data while balancing data privacy and AML compliance is one of the biggest constraints in applying digital solutions to achieve better AML/KYC outcomes. For this reason, the London edition of the TechSprint explored how PETs could enable sharing capabilities in legally compliant ways to fight financial crime.
- Multidisciplinary teams from FIs, technology companies and advisory firms developed POCs to solve these problems, with guidance from regulators that oversee both AML and data privacy requirements.
- During the events, several POCs were unveiled and demonstrated how PETs could be applied legally to enable effective data sharing and enhance the use of KYC and AML solutions across networks to identify bad actors and patterns of criminal activity.
- The TechSprint POCs also provided financial services and data privacy regulators an opportunity to improve their understanding of the practical implications and risks associated with balancing the needs of data protection and fighting financial crime.

TechSprints are a means for regulators to encourage regulatory innovation and collaborate with stakeholders to develop viable solutions to compliance challenges. The events can also facilitate the development of tools such as PETs and data cleanup, which are critical to the successful development and design of KYC shared platforms.[1] [2] [3] [4]

> “The things that will keep us standing in good stead are attitude and appetite, a willingness to learn through experimentation and being curious about what is next on the horizon.”
>
> — U.K. Financial Regulatory Authority

# Recommendations

# Use of digital solutions and shared platforms will dramatically improve the future state of KYC



Based on discussions with key stakeholders, we have concluded that the two key enablers – **KYC digital solutions and KYC shared platforms (e.g., KYC utilities)** – should be used more extensively by the financial services industry to revamp KYC processes.

Adopting digital solutions alone will reduce the time spent on KYC and introduce more consistency, while using shared platforms will reduce the need to perform certain activities like identity verification and screening, increasing overall KYC efficiency significantly. However, FIs will not be able to participate effectively in shared platforms without additional investments in digital solutions.

Because shared platforms are currently limited in coverage and availability, stakeholders should strongly consider KYC digitization as a short-term goal, and integration with shared platforms as a medium-to long-term objective, depending on where they are in their digital transformation journeys.

Proactive adaption of regulatory frameworks and mechanisms, and creation of new shared industry assets, will drive the digital optimization of KYC. Developing a collective understanding of the impact of new digital technologies on specific regulatory outcomes is a critical component. Fostering a competitive marketplace where transformative technologies can be adopted quickly is equally essential.

**In the subsequent slides, we list specific recommendations for each of the key stakeholders: (i) regulators and policymakers; (ii) financial institutions; (iii) KYC digital solution providers; and (iv) KYC shared platform providers. Our final recommendation centers on the development of a co-creation framework.**

# Regulators and policymakers should develop policy and regulatory frameworks for KYC

Although AML/KYC regulatory frameworks exist in many jurisdictions, there is a need for regulators and policymakers to update and/or expand existing regulatory frameworks to specifically address KYC innovation. The proposed regulatory policy framework on digitally enabled KYC would allow regulators to keep abreast of technological advancements and support initiatives that drive KYC optimization. The need to implement certain elements of the regulatory framework will vary depending on the level of KYC maturity and the availability of KYC enablers (i.e., KYC digital solutions and shared platforms) within the jurisdiction. Regulators and policymakers should consider the following recommendations.

## Advance KYC optimization through supranational entities

- Existing supranational entities such as the Financial Action Task Force (FATF) should provide guidance on KYC optimization that would serve as a blueprint for regulators in different jurisdictions to develop a common KYC standard and data model. FATF should also help to coordinate the provision and delivery of technical support to developing markets from regulators and development organizations.
- Organizations such as the International Organization of Securities Commissions (IOSCO), the Financial Stability Board (FSB) and the Bank for International Settlements (BIS) should also have a seat at the table during the development and adoption of KYC guidance across jurisdictions.
- Industry bodies such as the Wolfsberg Group and the International Institute of Finance should develop digital enablement policies and standards as part of their digital identity and RegTech programs.

## Develop jurisdictional KYC optimization frameworks

- Jurisdictional KYC optimization frameworks should incorporate a risk-based outcomes approach rather than a rules-based prescriptive approach, which makes it harder to evaluate new data and digital sources that are needed to achieve better KYC outcomes.
- Regulators should assemble a mix of professionals, such as policy, supervision, innovation and technology experts to create the frameworks and devise strategies for testing and developing KYC digital solutions and shared platforms. The experts may include data scientists and software engineers, behavioral economists and psychologists. It is important that regulators utilize agile methodologies to engage with the industry on innovative projects.[1]
- The jurisdictional frameworks should include standardized: 1) requirements and terminology around digital identity attributes; 2) requirements for digital verification of customers and related parties (e.g., eIDs); and 3) data models to enable information transferring.[2]
- In financial crime risk assessments, regulators should include the role of digital technology as a crime-fighting tool.[3]
- The KYC optimization framework should foster a culture of tech activism rather than taking a tech-agnostic approach. According to Nick Cook of the FCA, tech activism requires regulators to be technology-informed and active and to develop views and opinions on specific technologies without endorsing actual vendors.[1]
- Regulators should train examiners on the use of technology in assessing KYC programs.[4]

# Regulators should build on existing mechanisms to enable KYC optimization

Regulators should use various mechanisms to support testing and market adoption of KYC digital technologies, as well as to increase the collective understanding of how these technologies can be used to enhance KYC processes. The following are regulatory mechanisms that regulators and policyholders should consider to enable KYC optimization.

## Regulatory mechanisms

- Create technology demonstrations and events that bring financial institutions and digital solution vendors together to explore new KYC technologies and solutions.
- Spearhead the development of TechSprints, sandboxes and POCs to build the market's confidence in KYC digital tools and improve understanding of the technology.
- Leverage existing public-private vehicles, such as the Joint Money Laundering Intelligence Taskforce (JMLIT), to coordinate the development of effective digital KYC solutions and shared platforms. A potential area for coordination involves integrating shared typologies of crime developed by JMLIT into machine learning testing facilities. The JMLIT is a partnership between U.K. law enforcement and the financial sector that provides a platform for public and private agencies to exchange and analyze information related to financial crimes and economic threats.
- Develop regional and multijurisdictional regulatory mechanisms such as the Global Financial Innovation Network (GFIN).
- Replicate and adopt the GFIN model in jurisdictions with complex regulatory frameworks, such as the United States, to help solve the challenges around policy coordination and adoption of digital-enabled KYC.
- Promote KYC optimization in jurisdictions where KYC requirements have hampered financial inclusion by evolving beyond traditional documentary and non-documentary forms of ID&V to verification methods such as digital IDs, which can be used more extensively. Government agencies, regulatory bodies, development agencies, and supranational organizations such as the FATF can partner on initiatives that will improve financial inclusion.[1] [2]
- Partner with organizations such as the Alliance for Financial Inclusion, development banks and foundations to utilize digital solutions to increase financial inclusion. For example, for ID&V, financial institutions can use GPS locations to overcome the challenge of obtaining proof of address for KYC in developing markets. New types of ID&V attributes can provide customers with tiered access to financial services.[3]

# FIs should accelerate KYC optimization

FIs can reduce cost, enhance customer experience and improve compliance through KYC optimization, which encompasses the use of digital solutions and shared platforms. KYC optimization also increases the efficiency and effectiveness of associated AML processes, such as transaction monitoring. Below are key recommendations for FIs.

## Design a KYC optimization strategy that is supported by the board

- Adopt a KYC optimization strategy that is promoted by the board across the organization. Modify KYC operating models by incorporating KYC innovations and working in consultation with digital solution providers.
- Adopt challenger banks' best practices, such as the use of real-time identity verification solutions to enhance KYC processes.
- Work with regulators and industry associations such as the IRTA to understand, build and test digital solutions. Share lessons learned from KYC optimization efforts with these stakeholders.
- Get buy-in from the business lines, and the compliance, legal, IT, marketing and audit departments to develop a holistic strategy that enhances the KYC controls.

## Tackle technical and operational requirements for adopting KYC digital solutions

- Map out end-to-end KYC processes to identify points of inefficiencies and estimate the potential benefits to customers by making these processes more efficient.
- Develop data integrity and governance initiatives and commit to modernizing legacy systems used in KYC processes.
- Work with KYC digital solution vendors to obtain POCs for digitizing specific KYC processes, and conduct pilots using the POCs to estimate the costs and benefits and the impact on associated processes. The solutions should consider the use of both structured and unstructured data, as well as agile methodologies.
- Maintain evidence of all decisions made and use built-in interpretable algorithms to explain those decisions.[1]

## Pursue the advantages of shared platforms

- Actively participate in the development of regional and global KYC shared platforms as a member of a consortium or as part of a larger initiative, like a TechSprint.
- Update internal client data and workflow systems so they can effectively provide and receive data from the shared platform. The source of truth for jurisdictional KYC data standards would ideally come from federal regulators.

# KYC digital solution providers should educate stakeholders to help close the knowledge gap

KYC digital solution vendors need to better understand how their solutions fit into the broader KYC challenges that organizations face. By expanding their solutions and educating peers and other market participants, vendors can go to market with solutions that address KYC challenges more holistically. The following are recommendations for digital solution providers.

## Increase stakeholder understanding of the impact of KYC digital solutions

- Demonstrate POCs of digital solutions and participate in TechSprints to educate regulators and FIs on the underlying technology.
- Participate in sandboxes to increase regulators’ confidence in technology offerings and increase investor interest. For example, startups in the first cohort of the FCA sandbox received £135 million in equity funding and 80% are still operating today.[1]
- Address concerns over implementation costs by working with FIs to compare and benchmark various costs and future savings from efficiency and effectiveness gains (e.g., reduced headcount for ID&V process by requiring fewer applications to be populated while KYC information is collected).
- Form a strategic partnership with FIs at the technical level to ensure that the new digital technology solutions can interact with existing legacy systems, meet security concerns and improve customer experience.[2]

## Design holistic end-to-end solutions

- A key challenge that FIs have identified is being faced with the availability of a plethora of point solutions that may then need to be combined to fully digitize the customer lifecycle management process. Digital service providers should align with FIs and work with other vendors to create or structure end-to-end customer onboarding and lifecycle management tools that enhance customer experience.
- Use the IRTA’s Principles for RegTech Firms to adequately address requirements that FIs will be looking for during their procurement process (e.g., governance, legal and cyber).[3]

# Best practices: Operating KYC shared platforms successfully

Certain principles and factors contribute to the success of KYC shared platforms. The best practices listed below are based on interviews with industry stakeholders and are recommended to shared platform providers.

## Best practices for KYC shared platform providers

- **Building a trust and governance framework** – When establishing the KYC shared platform’s governance and trust framework and operational model, public and private sector participants should be aligned on the expected outcomes and goals so they can appropriately define roles and responsibilities, influence the engagement process, design features and manage the risks of the shared platforms.
- **Enhancing user experience** – To provide optimal customer experience, shared platform providers should deliver convenience, privacy and control for users (e.g., assigning single digital identities), with the ability to extend coverage beyond financial services to sectors such as government and healthcare.
- **Establishing common standards and models** – One way to achieve interoperability is for governments to mandate the development of a common data model for KYC shared platforms within a given market to enhance the efficiency of data normalization efforts. Additional common standards for collecting and verifying KYC data, performing KYC refresh, digital identity attributes and digital verification requirements at a minimum should be developed.
- **Defining a liability model** – An ideal KYC shared platform should have a defined liability model that is agreeable to participants, includes regulator input, and provides clarity on liability for failings. For example, the liability model should clarify who is responsible for verifying customer identity within the utility. Similarly, if DLT is being used for the shared platform, it is important to clarify who is responsible for mission-critical system failures.
- **Providing scalability and cost-effective technology** – The shared platform should be designed in a way that is cost-effective for participants, incorporating design features such as DLT and privacy enhancing technology. In addition, the design should allow for scalability and flexibility in order to adapt to frequently evolving regulatory requirements and user preferences.
- **Commercial model** – Participating financial institutions stand to gain clear efficiencies by sharing services. However, there may be potential conflicts of commercial interest related to revenue streams generated from ongoing activities, such as ID&V services, that are provided within the utility. If these conflicts cannot be solved by the market, the government needs to mandate the development of a utility approach.

# Develop a co-creation model to accelerate KYC optimization

Public-private partnerships are being developed to understand and test the effectiveness of digitally enabled KYC. To accelerate the pace of KYC optimization, we recommend that stakeholders create a model incorporating the elements below.

## Adopt the following key elements of the co-creation model

- Provide clear roles and responsibilities for government, regulators, industry and solution providers throughout the ideation to market-adoption phases. For example, regulators can focus on developing standards and taxonomies; while the digital solution providers and FIs can focus on developing tools for data sharing and PETs.
- Facilitate public-private funding mechanisms to seed and scale establishment of shared platforms and industry assets, such as data lakes and typology banks. These industry assets would provide synthetic or real privacy-enhanced data sources that could be used for designing, testing and calibration, including sharing of evolving typologies of crime.
- Create open intellectual property on standards and models developed through regulatory TechSprints and pilot programs. Develop independent third-party testing of digital solutions. This will help validate vendor claims, support more effective audits and foster faster procurement of vendor solutions.
- Build frameworks and digital technology tools to accelerate adoption of artificial intelligence at scale and better explain the technology and potential unintended consequences, such as data bias and lack of financial inclusion.
- Provide resources to support the specific needs of developing markets for industry assets such as biometric SIM card identity databases to reduce fraud and terrorism risks in jurisdictions where mobile money agents are involved in onboarding customers for money transfers and related mobile-based transactions.[1] [2]

# Appendix

# Bibliography (1/3)

| Slide | Section | Link Sources |
|---|---|---|
| 4 | **Current KYC controls are onerous and costly** | [1] Innovation and the Fight Against Financial Crime<br>[2] Breaking the KYC Remediation Cycle<br>[3] The Cost of Poor CX, Part 2 Collaboration in the Digital Age<br>[4] KYC Utilities: The Promised Silver Bullet for Nordic Banks?<br>[5] Thomson Reuters 2017 Global KYC Surveys Attest to Even Greater Compliance Pain Points<br>[6] The Cost of Poor CX, Part 1 The Cost of Poor CX<br>[7] FATF Guidance on AML/CFT Measures and Financial Inclusion, with a Supplement on Customer Due Diligence<br>[8] Fintech for Financial Inclusion: A Framework for Digital Financial Transformation |
| 10 | **Cost Benefit: What firms stand to gain through KYC optimization** | [1] Bank of America Merrill Lynch Sees Significant KYC Time Savings Using SWIFT's KYC Registry<br>[2] Robotic Process Automation (RPA) in Finance – Current Applications<br>[3] Fenergo Corporate and Institutional Banking<br>[4] The Battle to Onboard III |
| 13 | **Identity verification: AI and biometrics can dramatically streamline the ID&V process** | [1] IdentityMind Global Inc.<br>[2] Socure<br>[3] Jumio<br>[4] Know Your Customer<br>[5] KYC-Chain |
| 14 | **Screening: Reduce false positives and negatives with digital solutions** | [1] IdentityMind Global Inc.<br>[2] Napier<br>[3] iComply<br>[4] Comply Advantage |
| 15 | **Periodic reviews: Data orchestration with RPA minimizes process challenges, improves accuracy** | [1] Appway<br>[2] Fenergo |

# Bibliography (2/3)

| Slide | Section | Link Sources |
|---|---|---|
| 18 | **Shared platforms are most useful when built with digital technologies** | [1] Digital's Next Frontier<br>[2] FCA's 2019 Global AML and Financial Crime TechSprint<br>[3] From Innovation Hub to Innovation Culture<br>[4] Blockchain Disruptive Technology<br>[5] Blockchain Opportunities for Private Enterprises in Emerging Markets |
| 19 | **Learning from India's eKYC utility** | [1] The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment<br>[2] Aadhaar Paperless Offline e-KYC<br>[3] In a Year of Data Breaches, India's Massive Biometric Programme Finally Found Legitimacy<br>[4] Finance Ministry Amends PMLA Act to Offer Clarity on Digital KYC |
| 20 | **Why Singapore's KYC utility pilot initially struggled** | [1] Industry Banking KYC Utility Project After-Action Report – Knowledge Sharing<br>[2] MAS to Shelve 'Know-Your Customer' Project Due to High Costs, Work on SME Innovation Platform |
| 21 | **A digital identity project in the U.K. aims to put the consumer in control** | [1] TISA Encourages Firms to Join the Digital ID Following Success of Pilot<br>[2] Digital Identity Market Welcomes Plan to Hand Gov.uk Verify to Private Sector |
| 22 | **Spotlight: Global AML & Financial Crime TechSprint** | [1] Bureau of Consumer Financial Protection TechSprint RFI<br>[2] FCA's 2019 Global AML & Financial Crime TechSprint<br>[3] Citadel transcript<br>[4] Demo 8 – Citadel |

# Bibliography (3/3)

| Slide | Section | Link Sources |
|---|---|---|
| **25** | **Regulators and policymakers should develop policy and regulatory frameworks for KYC** | [1] From Innovation Hub to Innovation Culture<br>[2] Nordic KYC Utility Takes Shape<br>[3] 2018 US National Money Laundering Risk Assessment<br>[4] Keynote Remarks by Jelena McWilliams, Chairman, FDIC |
| **26** | **Regulators should build upon existing mechanisms to enable KYC optimization** | [1] How a Know-Your-Customer Utility Could Increase Access to Financial Services in Emerging Markets<br>[2] KYC Utilities and Beyond: Solutions for an AML/CFT Paradox?<br>[3] KYC Innovations, Financial Inclusion and Integrity |
| **27** | **FIs should accelerate KYC optimization** | [1] The Future of Regulation: AI for Consumer Good |
| **28** | **KYC digital solution providers should educate stakeholders to help close the knowledge gap** | [1] Taking the Next Step in Sandbox Evolution<br>[2] Digital ID Verification for Customer Onboarding<br>[3] IRTA Principles for RegTech Firms |
| **30** | **Develop a co-creation model to accelerate KYC optimization** | [1] US State Dept Thinks Africa's Leading Mobile Money Platform is Vulnerable to Money Laundering<br>[2] KYC Innovations, Financial Inclusion and Integrity |

# Index of key acronyms and abbreviations

| | |
|---|---|
| **AFI** | Alliance for Financial Inclusion |
| **AI** | Artificial intelligence |
| **AIR** | Alliance for Innovative Regulation |
| **AI/ML** | Artificial intelligence/machine learning |
| **AML** | Anti-money laundering |
| **BAU** | Business as usual |
| **BIS** | Bank for International Settlements |
| **CDD** | Customer due diligence |
| **CLM** | Client lifecycle management |
| **CRS** | Customer risk scoring |
| **DLT** | Distributed ledger technology |
| **EDD** | Enhanced due diligence |
| **eKYC** | Electronic KYC |
| **FATF** | Financial Action Task Force |
| **FCA** | Financial Conduct Authority |
| **FPR** | False positive rate |
| **FSB** | Financial Stability Board |
| **GDPR** | General Data Protection Regulation |
| **GFIN** | Global Financial Innovation Network |
| **HE** | Homomorphic encryption |
| **HRC** | High-risk customers |
| **ID&V** | Identity and verification |
| **IOSCO** | International Organization of Securities Commissions |
| **IUSC** | Industry Utility Steering Committee |
| **IRTA** | International RegTech Association |
| **JMLIT** | Joint Money Laundering Intelligence Taskforce |
| **KYC** | Know your customer |
| **ML/TF** | Money laundering and terrorist financing |
| **ML** | Machine learning |
| **NLP** | Natural language processing |
| **OCR** | Optical character recognition |
| **PEP** | Politically exposed persons |
| **PET** | Privacy-enhancing technology |
| **POC** | Proof of concept |
| **PR** | Periodic reviews |
| **RPA** | Robotic process automation |
| **RFI** | Requests for information |
| **SWIFT** | Society for Worldwide Interbank Financial Telecommunication |
| **UBO(s)** | Ultimate beneficial owner |
| **UIDAI** | Unique Identification Authority of India or Aadhaar |
| **ZKP** | Zero knowledge proof |

# Examples of digital solution providers

Extensive research on digital solution providers (vendors) offering one or more KYC functionalities revealed that digital capabilities, such as AI and robotics, are often bundled together to enhance the KYC process. Using multiple digital solutions or an integrated solution can be particularly effective because it allows FIs to address the full spectrum of KYC functions.

| Digital Solution | Examples of Vendors* |
|---|---|
| **Artificial Intelligence (AI)** | Ayasdi, Socure, Jumio, ComplyAdvantage, Trulioo Information Services Inc., Quantexa, Pitney Bowes, IdentityMindGlobal Inc, KYC-Chain |
| **AI – Natural Language Processing** | smartKYC, Finantix, IBM, Salesforce, IdentityMindGlobal Inc, Napier, ComplyKYC, Comply Advantage |
| **Robotic Process Automation** | UiPath, Blue Prism, Automation Anywhere, Kofax Kapow, AuthomationEdge, AntWorks, Contextor |
| **Blockchain/ DLT** | Tradle |
| **Link Analysis/ Graph Networking** | Pitney Bowes, Quantexa, Quantaverse, Threat Matrix, ACA Compliance Group, DataWalk |
| **Homomorphic Encryption** | Enveil, Symphony, Duality |
| **Data Orchestration Tools** | Appway, Fenergo |

*Protiviti has and may continue to maintain business relationships with vendors listed in this study. However, the inclusion of the vendors in this study does not constitute an endorsement or recommendation by Protiviti or the IRTA.

# Examples of KYC shared platforms

| KYC Utility Name* | Target Market/Client | Key Participants | Geography |
|---|---|---|---|
| SWIFT KYC Registry | Banks and corporations | Over 5,000 FIs from 200 countries, including Citi, J.P. Morgan, Deutsche Bank, HSBC, Morgan Stanley, and Standard Chartered | Global |
| Clarient Entity Hub by Thomson Reuters | Asset managers, hedge funds, corporations | BNY Mellon, Barclays, Goldman Sachs, Credit Suisse, J.P. Morgan, State Street, Depository Trust and Clearing Corp (DTCC), and TandemSeven among others | Global |
| Accelus Org ID by Thomson Reuters | Asset managers, hedge funds, banks, corporations | Thomson Reuters, Tradeweb Markets | U.S., Europe, Asia |
| KYC Exchange Net | All bank clients | Standard Chartered, Commerzbank, Soc Gen, AdNovum, and the Bank of London | Global |
| Markit \| Genpact KYC Services | Asset managers, hedge funds, banks, corporates | Citi, Deutsche Bank, HSBC, and Morgan Stanley | U.S., U.K. |
| Nordic KYC Utility | Corporations doing business in Scandinavia | DNB Bank, Danske Bank, Nordea Bank, Svenska Handelsbanken, Skandinaviska Enskilda Banken, and Swedbank | Nordics |
| UAE eKYC Utility | All bank clients | Abu Dhabi Commercial Bank, Abu Dhabi Islamic Bank, First Abu Dhabi Bank, Al Ansari Exchange, Al Fardan Exchange, U.A.E. Exchange, ADGM | U.A.E. |
| Netherlands PoC KYC Utility | Corporations | ABN Amro, ING, and Rabobank | The Netherlands |
| Fenergo Utility | All bank clients | Bahrain’s Electronic Network for Financial Transactions (BENEFIT) | Bahrain |
| DIFC Utility | All bank clients in Dubai | Founding members: Dubai International Financial Centre and Mashreq Bank; open to all qualified FIs | Dubai |
| Ernst & Young KYC Utility | FIs | FIs | Specific jurisdiction or globally |
| PWC KYC Utility | FIs | FIs | Channel Islands |
| Mansa | FIs | Spearheaded by African Export-Import Bank | Africa |

*Protiviti has and may continue to maintain business relationships with vendors listed in this study. However, the inclusion of the vendors in this study does not constitute an endorsement or recommendation by Protiviti or the IRTA.

Thank you to our
authors and contributors

# Authors and contributors

**Richard Maton**
Executive Board Member & Strategic Initiatives Lead, IRTA
+44 238 097 0791
richard@richardmaton.com

**Jo Ann Barefoot**, Founder & President, Alliance for Innovative Regulation

**Bruno Abrioux**, CEO, Encognize G.K.

**David Ehrich**, Executive Director, Alliance for Innovative Regulation

**Michael Juenemann**, Partner, Bird & Bird LLP

**Makoto Koinuma**, Counsel, Greenberg Traurig Tokyo Law Offices

**Michael Meyers**, CEO, RegTech Lab

**Ben Richmond**, CEO, IRTA & CEO, Cube

**Richard Rosenholtz**, Chairman, Nordic RegTech Association

**Samantha Jane Sheen**, Director, Ex Ante Advisory Ltd.

**Mona Zoet**, Founder & CEO, RegPac Revolution Pte. Ltd.

**Mike O’Keeffe**, Head of Corlytics UK

# Authors and contributors

**Michael Brauneis**
Managing Director and North America
Financial Services Industry Leader
+1 312-476-6327
michael.brauneis@protiviti.com

**Carol Beaumier**
Senior Managing Director and
Asia-Pacific Financial Services Leader
+1 212-603-8337
carol.beaumier@protiviti.com

**Shaun Creegan**
Managing Director, Risk and Compliance
+1 212-708-6336
shaun.creegan@protiviti.com

**Shelley Metz-Galloway**
Managing Director, Risk and Compliance
+1 571-382-7279
shelley.metz-galloway@protiviti.com

**Bernadine Reese**
Managing Director, Risk and Compliance
+44 20-7930-8808
bernadine.reese@protiviti.co.uk

**Shubhendu Mukherjee**
Director, Risk and Compliance
+1 212-479-0734
shubhendu.mukherjee@protiviti.com

**Saverio Mirarchi**
Director, Risk and Compliance
+1 212-399-8663
saverio.mirarchi@protiviti.com

**Susan Moran**
Manager, Risk and Compliance
+1 312-551-8387
susan.moran@protiviti.com

IRTA
International RegTech Association

protiviti®