



# A Next-Generation Approach to KYC:

## 3 Essentials for Safe, Seamless Digital Onboarding

### Introduction

Introduced in 2001 as part of the U.S. Patriot Act, Know Your Customer (KYC) compliance is essential for conducting digital business today. These guidelines were established to address the risks of financial crime and to help financial institutions (FIs) fight identity fraud and money laundering activities.

With the introduction of the more recent Title III, FIs must also deliver on two requirements to comply with stricter KYC: the Customer Identification Program (CIP) and Customer Due Diligence (CDD). These regulations allow FIs to accurately verify the identities of their applicants, make sure they're real, confirm they're not on any prohibited lists, and effectively assess their risk factors to mitigate money laundering, terrorism financing, and other financial fraud risks.

Although crucial to the success and safety of customer onboarding, implementing and maintaining a successful KYC program can sometimes create an overwhelming administrative burden. Additionally, navigating manual verification methods is costly and prone to inaccuracy, creating greater risk of customer turnover and lost revenue.

**The good news? With the right KYC solution, businesses (including FIs) can overcome these challenges and provide a safe, seamless onboarding experience that mitigates risk while enabling top-line revenue growth.**

This paper will explain the three essential elements required for a successful KYC solution that enables a next-generation approach to onboarding, growth and compliance.



### 3 KYC Essentials for Safe, Seamless Digital Onboarding

The ideal KYC solution will ensure that businesses and FIs get identity verification right every time and will provide feedback that allows the institution to proceed knowing that the applicant doesn't present a risk and is someone with whom they are able to conduct business.

#### The Ideal KYC solution should include:

1. Advanced analytics-driven identity verification
2. Intelligent, automated global watchlist screening
3. Continual watchlist monitoring

### Requirement 1: Advanced Analytics-Driven Identity Verification

As the top requirement for the ideal KYC solution, businesses should be autonomously examining data using sophisticated techniques and tools, typically beyond those of traditional business intelligence (BI), to discover insights, make predictions and generate recommendations on how they are coming to a resolution on the identity.

#### Why is this so important?

The ultimate goal of KYC compliance is to verify identities quickly and accurately, allowing businesses to gain high auto-approval rates and minimize manual reviews.

### BUSINESS ISSUE

## Identity Verification **MUST** Be Fast and Accurate

The ideal solution should include advanced analytics techniques including data mining, machine learning, pattern matching, forecasting, cluster analysis and more to ensure high match rates and fast response within seconds.

Using advanced analytics enables institutions to experience and benefit from accurate, automated identity verification with over 90% auto-approval rates.

In contrast, solutions that only apply simple, binary-based matching with little to no intelligence will produce lower-than-desired auto-acceptance rates in the 60-70% range.

This is why implementing advanced analytics for identity matching is key. Incorporating a broad range of advanced analytics techniques increases accuracy, maximizes auto-acceptance rates, alleviates customer friction and improves the onboarding experience.





## DIVERSE DATA COVERAGE AND PROPRIETARY SEARCH ANALYTICS EQUATE TO A BEST-IN-CLASS SOLUTION

We are well past a time when credit and KBA checks alone are enough to keep bad actors at bay. Achieving the best identity verification outcomes from a KYC solution requires large and diverse data sources with billions of records. Such a database holistically reflects the population, including mainstream and underbanked or thin-file consumers.

When evaluating KYC solutions, businesses will want to look for the following data sources:

1. Ingested data feeds
  - Credit bureaus
  - Telecom records
  - Utility records
  - Verified identities
  - Social Security records for deceased individuals
  - Marketing records that include addresses and phone numbers
  - Student data
  - Military data
  - NIST 800-63 Authoritative Sources
2. Techniques to standardize, validate, correct, deduplicate, and resolve multiple entities
3. Continuous data updates to maintain quality and avoid degradation

## ADVANCED DATA ANALYSIS AND RESOLUTION

With a breadth of data sources, businesses require a KYC solution that applies advanced analytics techniques to intelligently analyze the data and deliver accurate results. The solution must go well beyond a simple binary, text-based matching approach, which is inadequate to manage analysis on the billions of records or to yield accurate results.

Basic, rules-based KYC solutions have been available for years. They walk through the multiple characteristics of a person's profile, weigh them and deduce if any number of them signal risk. However, bad actors have a number of ways to circumvent these simple techniques.

In contrast, a solution with intelligent analytics techniques like machine learning algorithms can provide the foundation for the best path forward to accurately ensure a provided identity is real.

### Why advanced analytics?

In terms of innovation and applying AI to big data, advanced analytics and machine learning can often be misunderstood. When considering their merits in identity verification solutions, it's important to understand some of the specific capabilities they should provide.

## BUSINESS VALUE

Intelligent Data  
Analysis Delivers **90%+**  
Auto-Approval Rates



## Scale

First, there's serious scalability. Rules-based systems are not capable of analyzing the dynamic data needed to recognize the nuanced and emerging patterns of identity and synthetic fraud. However, a KYC solution that uses advanced analytics can automate this effort at scale to clean and normalize the data while providing rigorous quality assurance scrutiny.

## Correlation

Then, there's the value of data correlation that advanced analytics provides with the ability to combine data sources into the idea of an "identity cluster." This provides greater detail with a longer history on an identity and allows the solution to accurately determine whether the identity, as a whole, represents a real individual.

For example, checking against a single source like a Social Security number provides limited identity matches. However, when searching that identity's data records further, across sources, a KYC solution can use fuzzy approximation to uncover name derivatives, misspellings, variations in identifier form, and phonetic variations to find identities and paint a broader and more accurate picture.

## Resolution

A KYC solution that is capable of drilling down not only on individual attributes but also the relationships between them, can better "learn" and understand the data in the repositories. The ideal solution should then dynamically apply risk weightings to the attributes to come to a resolution on the validity of the identity. This intelligent risk analysis approach provides the business with an accurate assessment on whether that identity is valid.

The importance of advanced analytics in the ideal KYC solution cannot be understated. It provides organizations with greater precision in detecting authentic identities and deflecting identity fraud attempts—automatically. The gains that FIs and other organizations will experience with 90%+ auto-approval rates will turn the KYC process from a check-box compliance solution into a growth-focused, revenue-generating endeavor.

## Requirement 2: Intelligent, Automated Global Watchlist Screening

The risk of inadvertently doing business with criminals and enabling money laundering has led many organizations to experience the sting of lost revenue and regulatory fines—not to mention the long-term impact it has on an organization's brand reputation.

As part of the U.S. Patriot Act's Customer Due Diligence (CDD) Rule, requirements for anti-money laundering were placed on FIs to mitigate this risk by conducting ongoing due diligence to understand the nature and purpose of customer relationships to develop a customer risk profile.

### BUSINESS ISSUE

## Legacy Watchlist Screening Solutions Are Manual & Prone to False Positives





Adopting a KYC watchlist screening program also allows organizations to address similar requirements from various regulating bodies, such as the FDIC Bank Secrecy Act and Anti-Money Laundering Act and FinCEN KYC requirements, as well as reduces the risk of OFAC enforcement actions.

In reality, putting this requirement into action has FIs conducting screening of customers against a long and growing set of watchlists. Think tedious, manual review against a company's customer accounts and daily transactions. For a typical bank conducting these KYC watchlist screenings, 75%-85% of the daily alerts that they must manage and remediate are false positives.

In contrast, the ideal KYC solution will use automation to accelerate the screening process and reduce false positives.

### WATCHLIST SCREENING RECOMMENDATIONS

With expanding watchlists combined with transaction and customer growth, organizations need a KYC solution with global watchlist matching technology that scales to automatically address the search requirements and eliminates the challenges of manual reviews and false positives.<sup>1</sup>

## BUSINESS VALUE

# Increases Screening Accuracy and Efficiency to Confidently Assess Risk

When evaluating KYC solutions, look for the following watchlist screening capabilities:

- Broad integration with worldwide watchlists, including the 1,100+ sanctions and enforcement lists, 6,000 politically exposed persons (PEP) lists, and adverse media screening lists
- Advanced search capabilities that make it easy to filter search queries and drill into data sources, countries, and other criteria
- Smart matching technology with techniques such as equivalent and phonetic name matching and options for exact or fuzzy name and date of birth matches

<sup>1</sup>The Global Treasurer. False positives: a growing headache. October 2015.



## Requirement 3: Continual Watchlist Monitoring

To effectively prevent money laundering and financial crime, there are many worldwide KYC-focused regulations that require watchlist screening, and, generally, they require the process to be ongoing.

### BUSINESS ISSUE

## Maintaining an Accurate Status on Customer Risk Is Time Consuming and Ineffective

Specifically, the CDD Rule requires FIs to “conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.”

Putting this rule into practice has created challenges for organizations like FIs, and the pragmatic results of truly knowing the current risk profile of an FI's customer base have, largely, been ineffective.

Conducting annual—or even quarterly—audits on an organization's customer accounts against current watchlists is not only a laborious effort, it's immediately stale and out of date the moment the audit is done. This manual approach means businesses can only reasonably check against a portion of watchlists and involves more complexity when attempting to answer the question, “Do my customers currently present a risk?”

## CONTINUAL WATCHLIST MONITORING RECOMMENDATIONS

Instead of manual customer base audits for risk, businesses should seek a KYC solution that will continually audit the organization's customer base against the current and broad set of worldwide watchlists.

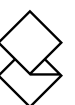
A KYC solution that proactively and consistently monitors watchlists against an organization's current accounts and customer list will provide the most accurate measure of their customers' present risk profile. This approach empowers institutions to immediately act on any new customer risks so that they can mitigate any potential financial loss or damage to the corporate brand.

Building on the watchlist screening requirements, businesses should look for the following continual watchlist monitoring capabilities when evaluating KYC solutions:

- Allows FI to import current customer accounts into a “customer monitoring list” to create a complete customer base to monitor
- Following an initial screen, adds identity to FI's “customer monitoring list” to automatically maintain a current list of customers
- Consistently query global watchlists daily, at minimum, and sends alerts to designated personnel when a customer's status changes

### BUSINESS VALUE

## Continual Watchlist Monitoring Effectively Provides a Current Assessment of Customer Risk



## Socure's Next-Generation Approach to KYC

Socure's mission is to be the single source of trusted identity for every business-to-consumer transaction, eliminating identity fraud while fueling growth. Socure's holistic solution for identity management encompasses intelligent KYC, real-time identity fraud risk scores, proactive watchlist monitoring, and analytics-based document verification that enables organizations to streamline identity management accurately and effectively.

Socure's ID+ KYC uses advanced analytics coupled with broad data sources to deliver the highest identity match accuracy with over 90% auto-approval rates, and detailed risk and reason codes for every identity element to provide businesses with actionable intelligence.

With ID+ Global Watchlist Screening, Socure enables organizations to automate the screening process by searching identities against a wide range of sanctions and enforcement lists. Applying smart matching technology, organizations will gain more accurate results that improve customer experience and eliminate the operational overhead. When combined with Socure's proactive watchlist monitoring, businesses can also continuously and accurately answer the question, "Do my customers currently present a risk?"

## Conclusion

If there's one thing organizations can count on, it's that perpetrators will continue to advance their identity fraud techniques for financial gain. To mitigate this risk, businesses who conduct digital transactions need a KYC solution that provides a strong foundation of advanced analytics to identify and thwart these attempts accurately and efficiently.

In the pursuit of the ideal KYC solution, organizations should use the three requirements outlined in this paper to vet, select, and ensure their new identity verification solution can effectively position their business for success—now, and for years to come.

## Learn More

Boost your top-line revenue growth and increase auto-acceptance rates with Socure's Intelligent KYC solution. To learn more, contact us at [salesinfo@socure.com](mailto:salesinfo@socure.com) and [schedule your demo](#) today.

