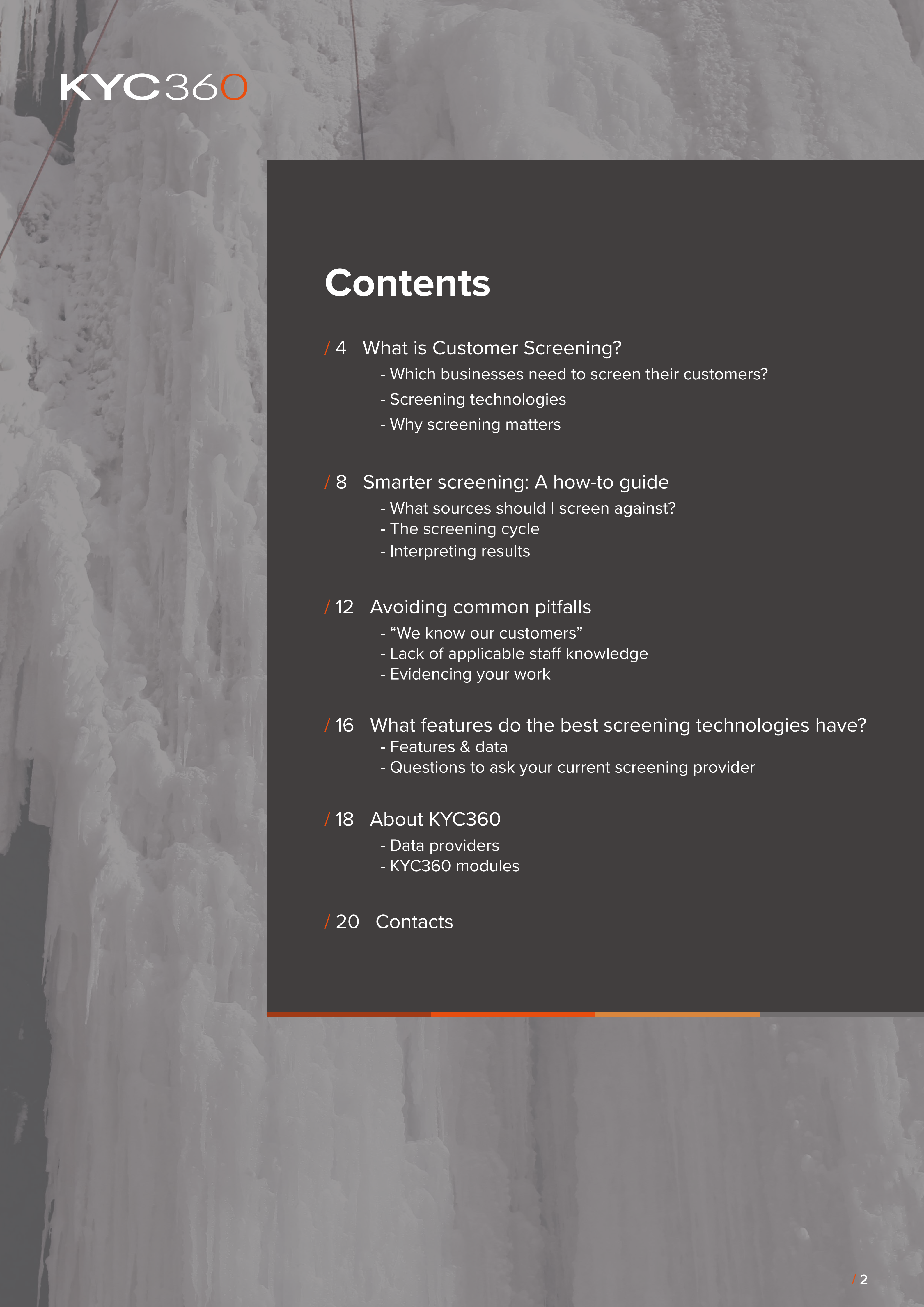
KYC360

The Definitive Guide to Customer Screening

powered by

DOW JONES | LSEG RISK INTELLIGENCE | LexisNexis®

Comply and Outperform with KYC360



Contents

KYC360

The Definitive Guide to Customer Screening

In this guide we explain the process and components of customer screening. We look at what screening involves, the technologies used to do it, and which common screening pitfalls you should be aware of.

KYC360 is an award-winning AML compliance platform, which enables hundreds of businesses, regulators and law enforcement agencies around the world to onboard, screen and manage the risk of their customers and stakeholders throughout their life cycle.

The KYC360 team also runs the world's leading AML knowledge portal, KYC360, visited daily by thousands of AML professionals; and KYC360's founder, Stephen Platt, is widely regarded as one of the world's leading experts in financial crime prevention.

What is Customer Screening?

Screening is the process of dynamically comparing the data you hold on customers, prospective customers, suppliers and counterparties against third-party data for risk management purposes.

Data you might want to screen against includes:

- **Structured data,** including sanctions, PEP (politically exposed person) and watch lists.
- **Unstructured data,** in the form of adverse media.

Why screen?

The principal objectives of screening are to manage the risk of doing business with 'bad actors' (such as sanctioned or wanted persons) and to identify customers or prospective customers who pose an elevated risk of criminality (such as PEPs) so that appropriate action can be taken to manage risk through, for example the application of enhanced due diligence (EDD).

The over-arching aim is to manage your organisation's exposure to money laundering, terrorist financing or any other form of predicate criminality such as bribery and corruption, or tax crimes. In recent years, there's been an increasing focus on the benefits of reputational risk management through adverse media screening which compares customers against less formal data sources for early indications of potential risk. These indicators might include information about an individual prior to the commencement of a criminal process, or to them becoming subject to sanctions.

Which businesses need to screen their customers?

The types of business that are legally required to screen their customers varies between jurisdictions. In nearly all countries there is an 'AML regulated sector' and businesses that fall within its ambit are required to screen as part of their Know Your Customer (KYC) obligations.

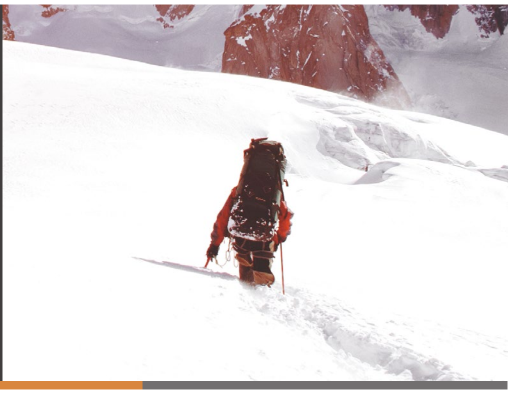
The types of business commonly included in the regulated sector include:

- Banks and credit institutions
- Investment businesses
- Money services businesses
- Company & trust administration businesses
- Law firms
- Insurance providers
- Accountancy practices
- Real estate agents
- Dealers in high value goods
- Gaming businesses

If you are unsure whether your business is regulated for AML purposes your industry body or trade association will be able to clarify the rules that apply to you.

Screening is also widely employed by businesses that fall outside the AML regulated sector to help protect against the risk of reputational damage that might arise from doing business with certain customers or becoming inadvertently involved with some form of predicate criminality. Bribery and corruption, for example, is particularly acute in the natural resources, armaments and pharma industries.

KYC360



Screening technologies

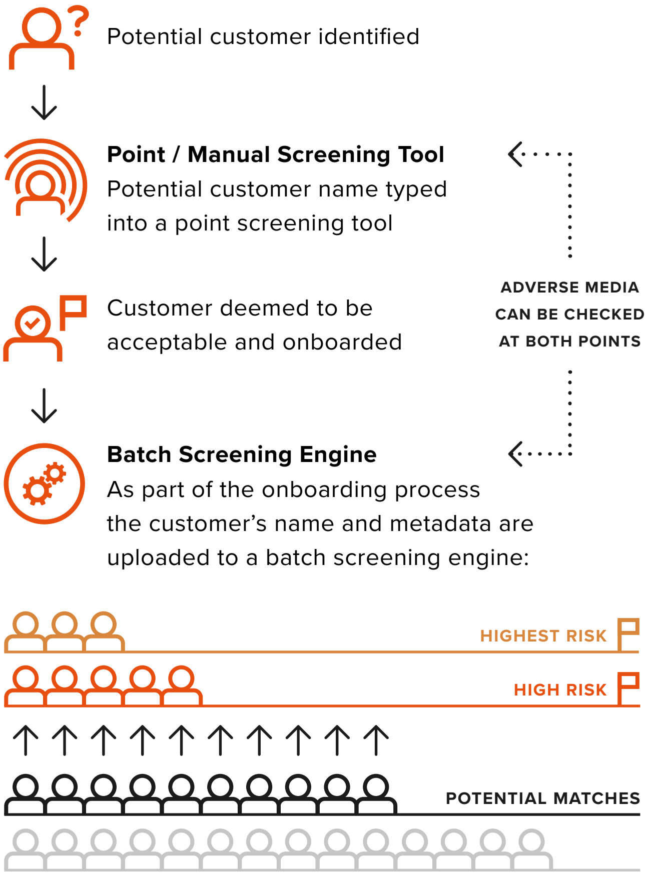
Every screening solution is comprised of two components:

- / A screening engine - the technology that runs the data analysis and produces the results
- / The external data against which user customer data is compared

The data is the fuel that drives the engine, and a screening engine is only as good as the fuel that's put into it. There are three types of screening tool:

- / **Point/Manual screening** – this form of screening tool requires users to manually input the name of the customer they wish to screen. The tool then outputs the results on a customer by customer basis
- / **Batch screening** - a screening engine to which customer names are uploaded and screened automatically with whatever regularity the business determines (normally overnight). The engine outputs results in relation to all customers for which there are potential screening matches
- / **Adverse media screening** - screening against adverse media sources can be done either as a one-off action or as part of a batch process. It takes into account a much broader set of source data, helps to provide early warning of issues that may arise - or warning of issues that don't fall within the scope of traditional screening categories - but carries with it the risk of high numbers of false positives if not done correctly.

The challenge for businesses wishing to optimise their compliance performance is to firstly identify what kind of screening they're required to undertake, either by the regulatory environment or investor expectations. Then they need to identify the best screening engine technology combined with the best quality data so that they benefit from the most accurate results whilst reducing the number of false positives.



Potential customer identified

↓

Point / Manual Screening Tool
Potential customer name typed into a point screening tool

↓

Customer deemed to be acceptable and onboarded

↓

Batch Screening Engine
As part of the onboarding process the customer's name and metadata are uploaded to a batch screening engine:

ADVERSE MEDIA CAN BE CHECKED AT BOTH POINTS

The customer is screened automatically overnight. The engine outputs results in relation to all customers for which there are potential screening matches.

What are false positives?

False positives are potential screening matches that transpire not to relate to your customers. Many screening engines require businesses to screen all customers irrespective of their risk profile in a uniform way. This often results in a very large number of false positives. Working through potential matches to identify which are true and which are false absorbs a huge amount of compliance resource and increases the risk of human error.

KYC360

Input Data Quality Assessment

At KYC360 we know that screening results are directly impacted by the quality of input data. If you put rubbish in you are more likely to get rubbish out. The better quality the data that is input into a screening engine the fewer false positives and the more true matches will result allowing you to focus on the signal of risk without the distraction of noise.

Most screening providers rely just on algorithms to compensate for poor data quality but at KYC360 we also help you to identify and correct defects in your input data through a self service data quality assessment tool that comes as part of our Batch screening module.

KYC360 is the only screening provider in the world to offer this functionality as a core component of its screening solution because we recognise that there cannot be effective screening without stringent quality control of input data.

The input data quality assessment function will check and provide you with a report on any data quality issues giving you the chance to take remedial steps and optimise your screening results.

KYC360 is the only screening provider in the world to offer this functionality as a core component of its screening solution

Why screening matters

Breaching sanctions— by doing business with a sanctioned individual or entity—is a criminal offence in almost all jurisdictions.

Increasingly harsh penalties are being applied by regulators and prosecutors to businesses that fail to screen customers adequately or fail to risk rate them appropriately. Regulators don't even need to demonstrate that an organisation has been exposed to criminality through their customer's activities – it is enough simply to show that its AML controls were inadequate.

Breaching sanctions by doing business with sanctioned individuals or entities is a criminal offence. In the UK for example prison terms of up to 7 years can be imposed in addition to unlimited fines for organisations that have failed to take precautions to prevent sanctions breaches.

In 2014 the New York Department of Financial Services fined Standard Chartered Bank $300m only two years after a penalty for the same amount was imposed for the bank's role in facilitating breaches of US sanctions against Iran. The second fine was imposed because of the bank's failure to detect a large number of potentially high-risk transactions for further review even though no actual criminality was identified. This was a salutary lesson for the entire financial services industry and emphasised the criticality of effective customer screening.

Failing to screen customers leaves your business open to a host of consequences, from fines and reputational damage to the criminal prosecution of staff and directors.

Financial crimes are not victimless

From violent drug traffickers, to fraudsters targeting vulnerable people in online scams, the ability to move illicit money without getting caught is central to a vast range of criminal activity. If your business enables it, you are facilitating the movement of money which may ultimately result in great human suffering (this conclusion was at the heart of a $1.9bn fine imposed on HSBC bank in 2012 by the US for laundering money belonging to Mexican drug cartels).

Breaching financial sanctions can also have a profound impact on international politics. As the UN recently reported, North Korea is able to fund its nuclear programme by means of a sophisticated network of shell companies and money laundering techniques, through which North Korean businesses were able to continue trading with the rest of the world.

Adverse media screening can provide early warning of these risks and also indicates a host of other risks posed by suppliers or customers to the reputation or good standing of your business. In an age where the social consciousness of consumers has become increasingly important, this has assumed a new significance.

Screening is not a panacea. But it is a critical first step in ensuring that your business doesn't become a conduit for criminal money. Failing to screen leaves your business open to a host of consequences, from fines and reputational damage to the criminal prosecution of staff and directors.

/ What sources should I screen against?

As a minimum you should screen against sanctions lists, PEP lists, and government watch/black lists.

/ Sanctions

Individual countries and multinational bodies (e.g. the EU and the UN) impose sanctions measures to pressure other countries or organisations to change their behaviour. Sanctions can apply to individuals, specific businesses or whole nations. Breaching a sanctions measure, or assisting another party to do so, is nearly always a criminal offence. Businesses must scan customers against sanctions lists issued by all the jurisdictions in which they are operating or to which they have operational links, in addition to lists issued by multinational bodies.

In the wake of the 9/11 attacks, the US has developed economic sanctions into a sophisticated tool for conducting what some commentators have described as ‘financial warfare’ against actors that threaten the country’s interests. Leveraging the status of the US dollar as the world’s de facto reserve currency, the US Treasury aggressively pursues organisations that, knowingly or not, help individuals and nations get round US sanctions.

In 2014, French bank BNP Paribas agreed to pay a record fine of nearly $9 billion for breaching US sanctions against Iran, Cuba and Sudan. As such, any businesses which make use of the US dollar, even if they have no other connection to the US, would be well advised to comply with US sanctions measures.

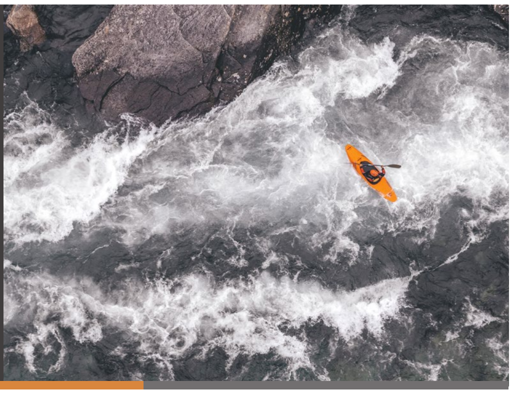
Although the outline sanctions regimes are published by some of those states that employ them, it’s still important to use a high quality data provider, because in many instances a sanctions regime will identify only an individual and not all of the entities connected to that individual - all of which will nonetheless fall within the ambit of the sanctions measure. That’s where a high quality data provider such as Dow Jones or Refinitiv World-Check will assist in identifying these linkages for you.

/ Politically exposed persons

Politically Exposed Persons (PEPs) are individuals who hold or have held a significant public function. This function might give them influence over, for example, the spending of taxpayer money or the allocation of contracts by state owned enterprises. As such, they are regarded by the Financial Action Task Force as a category of individuals which is more susceptible than most to engaging in bribery and corruption, and money laundering activity.

Screening providers maintain databases of millions of global PEPs, and Relatives and Close Associates (RCAs). Nearly all jurisdictions require their regulated sectors to establish if applicants for business are PEPs and to profile and treat them as high risk.

What is Customer Screening?



/ Watch lists

Watch lists or black lists are official lists of individuals and companies which may pose a greater financial crime risk owing to their past behaviour. They may include lists of wanted criminals or suspects, lists of persons disqualified from holding directorships or holding executive positions in the finance industry or lists of persons convicted of particular crimes. Watch lists don’t capture every criminal offence and are not a comprehensive source for criminal records.

KYC360’s data sources track over 4,500 global watch lists maintained by bodies ranging from Interpol to national financial regulators and prosecutors.

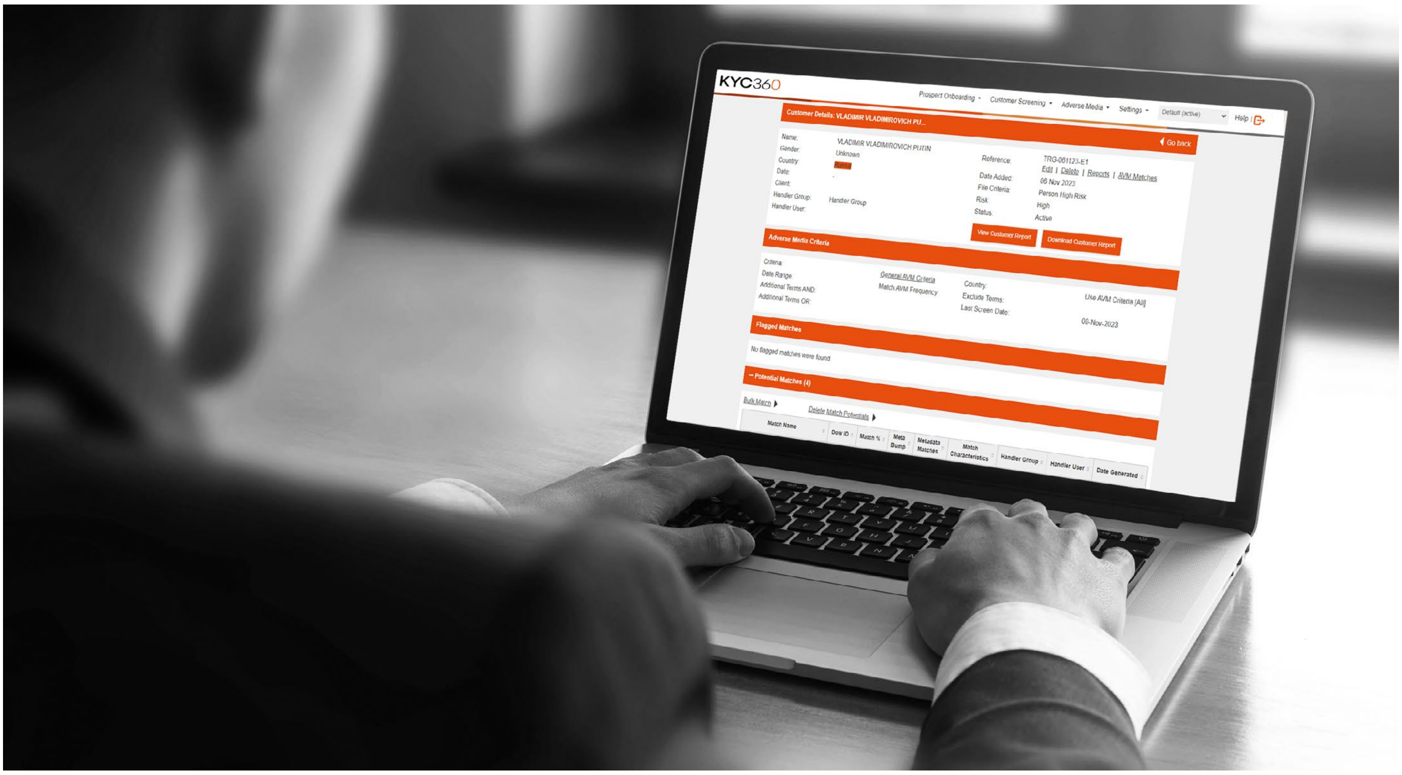
/ Adverse media

Screening an individual for adverse media coverage involves looking for any negative mentions of them in news media and wider open source information.

Adverse media screening could reveal that, for example, a potential customer was convicted of a criminal offence but not one deemed sufficiently relevant to financial crime to merit their inclusion on a watch list. Or you might find that an individual is in the process of being tried for an offence which would be relevant to financial crime - just that proceedings have not yet concluded.

In some jurisdictions, adverse media screening is reserved for enhanced due diligence checks – but it is good practice to carry out basic adverse media screening for all customers, particularly as it can reveal information not included on official sanctions, PEP and watch lists.

In recent times, regulators’ expectations have increased and many financial services businesses are now seeking to carry out continuous adverse monitoring, at least in relation to their higher risk customers.



What is Customer Screening?

/ When should you screen?

The answer to this question depends upon how robust you want your compliance program to be. Historically there were two approaches:

1. Manual screening at onboarding and periodically thereafter for example at annual review
2. Manual screening at onboarding and periodic review AND automatic overnight batch screening of all customers

Some organisations are now choosing to augment overnight batch screening with automatic adverse media screening of some or all of their customers.

The more rigorous the approach, the less is left to chance. Events impacting customer risk can occur very rapidly, so the sooner businesses can be alerted to a change in the risks presented by a customer the better.

The danger with not overnight batch screening customers is that a business is oblivious to a customer's inclusion on a sanctions, PEP or watch list or some adverse media until the next time they conduct a manual screen - perhaps several months or years later.

In those circumstances it can be very difficult for a business to demonstrate that it had undertaken sufficient KYC on the customer. In the worst cases it can lead to allegations that the business facilitated criminality through inadequate customer risk management processes.

/ When to conduct enhanced due diligence

Enhanced due diligence (EDD) means investigating a customer more thoroughly than you would in regular screening. In most jurisdictions, in the course of regular screening, you will be required to conduct EDD when you have identified that you're dealing with a high risk customer.

The form your EDD takes should depend on the nature and severity of the risk. It can vary from an adverse media check, to investigating corporate structures linked to an individual, to verifying income sources.

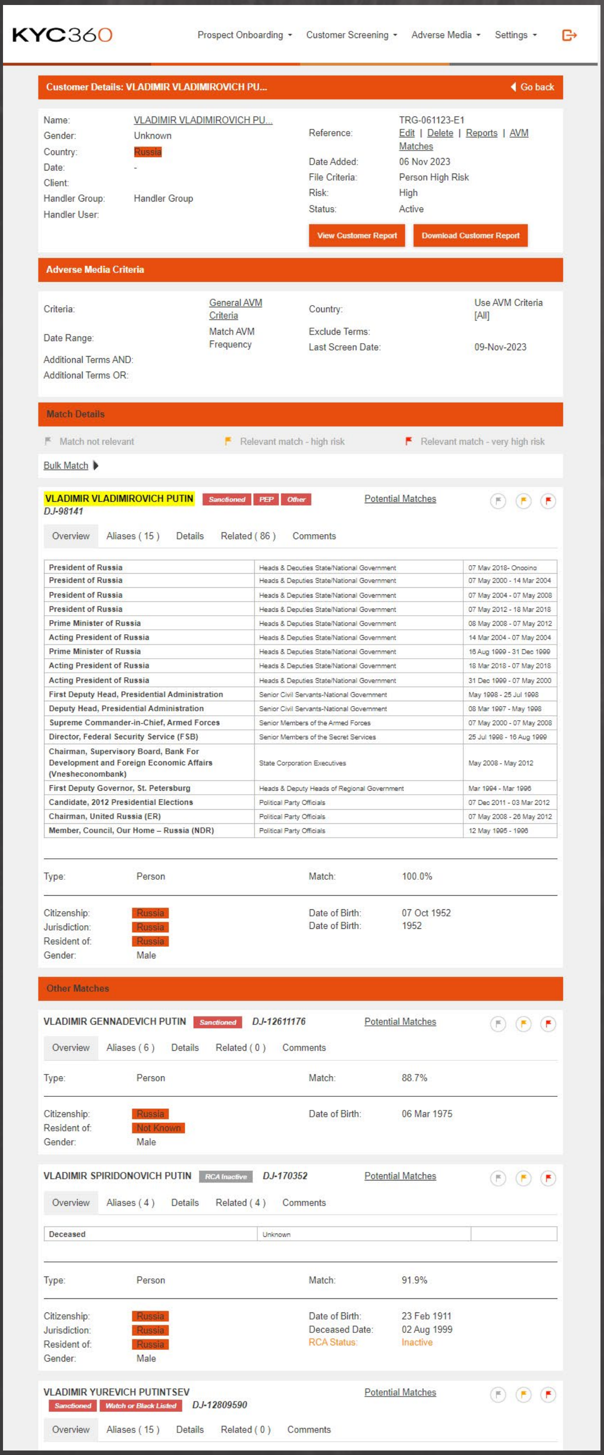
EDD should leave you confident that any risk has been mitigated and is unlikely to affect your business. Red flags that might lead you to carry out EDD include:

- A customer is a PEP or is on a watch list (PEP status alone isn't sufficient to reject a customer: the majority of PEPs are not engaged in corrupt activities, though they should be treated as high risk)
- A customer has adverse media associated with them relating either to financial crime risk or to reputational risk for your business
- A customer told you something during onboarding which causes you concern, such as an unusual proposed activity profile, or that they have family links to risky jurisdictions

Always document both the EDD you carry out and the rationale behind any resulting actions.

KYC360

What is Customer Screening?



Customer Details: VLADIMIR VLADIMIROVICH PU...

Name:	VLADIMIR VLADIMIROVICH PU...	Reference:	TRG-061123-E1 Edit | Delete | Reports | AVM Matches
Gender:	Unknown	Date Added:	06 Nov 2023
Country:	Russia	File Criteria:	Person High Risk
Date:	-	Risk:	High
Client:		Status:	Active
Handler Group:	Handler Group		
Handler User:			

Adverse Media Criteria

Criteria:	General AVM Criteria	Country:	Use AVM Criteria [All]
Date Range:	Match AVM Frequency	Exclude Terms:	
		Last Screen Date:	09-Nov-2023
Additional Terms AND:			
Additional Terms OR:			

Match Details

Match not relevant — Relevant match - high risk — Relevant match - very high risk

VLADIMIR VLADIMIROVICH PUTIN Sanctioned PEP Other
DJ-98141

President of Russia	Heads & Deputies State/National Government	07 May 2018- Ongoing
President of Russia	Heads & Deputies State/National Government	07 May 2000 - 14 Mar 2004
President of Russia	Heads & Deputies State/National Government	07 May 2004 - 07 May 2008
President of Russia	Heads & Deputies State/National Government	07 May 2012 - 18 Mar 2018
Prime Minister of Russia	Heads & Deputies State/National Government	08 May 2008 - 07 May 2012
Acting President of Russia	Heads & Deputies State/National Government	14 Mar 2004 - 07 May 2004
Prime Minister of Russia	Heads & Deputies State/National Government	16 Aug 1999 - 31 Dec 1999
Acting President of Russia	Heads & Deputies State/National Government	18 Mar 2018 - 07 May 2018
Acting President of Russia	Heads & Deputies State/National Government	31 Dec 1999 - 07 May 2000
First Deputy Head, Presidential Administration	Senior Civil Servants-National Government	May 1998 - 25 Jul 1998
Deputy Head, Presidential Administration	Senior Civil Servants-National Government	08 Mar 1997 - May 1998
Supreme Commander-in-Chief, Armed Forces	Senior Members of the Armed Forces	07 May 2000 - 07 May 2008
Director, Federal Security Service (FSB)	Senior Members of the Secret Services	25 Jul 1998 - 16 Aug 1999
Chairman, Supervisory Board, Bank For Development and Foreign Economic Affairs (Vnesheconombank)	State Corporation Executives	May 2008 - May 2012
First Deputy Governor, St. Petersburg	Heads & Deputy Heads of Regional Government	Mar 1994 - Mar 1996
Candidate, 2012 Presidential Elections	Political Party Officials	07 Dec 2011 - 03 Mar 2012
Chairman, United Russia (ER)	Political Party Officials	07 May 2008 - 26 May 2012
Member, Council, Our Home – Russia (NDR)	Political Party Officials	12 May 1995 - 1996

Type:	Person	Match:	100.0%
Citizenship:	Russia	Date of Birth:	07 Oct 1952
Jurisdiction:	Russia	Date of Birth:	1952
Resident of:	Russia		
Gender:	Male		

Other Matches

VLADIMIR GENNADEVICH PUTIN Sanctioned DJ-12611176 Potential Matches

Overview Aliases (6) Details Related (0) Comments

Type:	Person	Match:	88.7%
Citizenship:	Russia	Date of Birth:	06 Mar 1975
Resident of:	Not Known		
Gender:	Male		

VLADIMIR SPIRIDONOVICH PUTIN RCA Inactive DJ-170352 Potential Matches

Overview Aliases (4) Details Related (4) Comments

Deceased	Unknown	

Type:	Person	Match:	91.9%
Citizenship:	Russia	Date of Birth:	23 Feb 1911
Jurisdiction:	Russia	Deceased Date:	02 Aug 1999
Resident of:	Russia	RCA Status:	Inactive
Gender:	Male		

VLADIMIR YUREVICH PUTINTSEV Potential Matches
Sanctioned Watch or Black Listed DJ-12809590

Overview Aliases (15) Details Related (0) Comments

Example screening result

/ Interpreting results

1. Confirm that the results do indeed relate to your customer. If you are unsure of the accuracy of the match, then use metadata such as passport number, date of birth, country of origin and so on.

2. If you get a name match that is close but not identical, check the metadata to ensure it isn't an alias for your customer.

3. Sanctions, PEP and watch lists are drawn from databases compiled by experienced data providers about individuals or corporates who pose some form of risk. Adverse media searches pull in material from all of the search-able web.

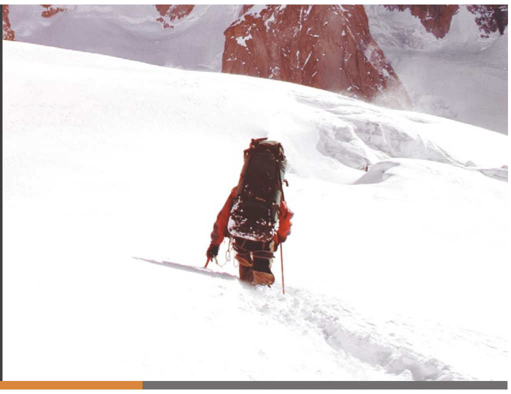
   In analysing adverse media search results it is important to consider the provenance of each result. Does it come from a well-regarded, widely-read news organisation? Or is it drawn from a smaller blog or website, the output of which may be less reliable? Unmoderated blogs or results from small, local news outlets, aren't necessarily irrelevant but you should seek to corroborate any information gleaned from them against other sources.

4. A result that says 'this person is involved in bribery' is easy to interpret. Other types of result—a complex corporate structure from a 'KYB' (Know Your Business) data provider, for example — may not be. Your staff will need a degree of understanding of money laundering 'hotspots' and methodologies in order to assess risk effectively, and should be trained accordingly.

EDD might include verifying corporate structures or verifying identity and address of individuals. Dedicated onboarding platforms exist which can carry out these activities for you, alongside screening.

KYC360

Avoiding common screening pitfalls



There are a few common pitfalls to be aware of along the way.

"We know our customers."

Businesses often develop a false sense of security about the risk profile of a particular customer or group of customers. This could be because they have met the person in question, have a longstanding professional relationship with them, or because the business and the customers are in the same jurisdiction.

This attitude of "we know our customers", especially amongst more senior staff who have an historical relationship with some individuals and personally vouch for them (think old boys' network), can lead to red flags being overlooked. In addition, the failure to recognise the risks associated with your own jurisdiction is a particularly common pitfall. Also, don't forget that customer risk can change over time. A person who has been low risk for many years may become high risk owing to a change of job, moving abroad or being elected to political office. If you don't batch screen them, you may not find out about their change in risk profile until it's too late!

/ Insufficient frequency of screening

Historically, adverse media screening has been an activity that takes place periodically, typically at onboarding and review points within a relationship. Carrying out this activity only once every two or three years risks missing important information about changes to a customer's status. Increasingly businesses are seeking to automate adverse media screening using new technology to ensure that they will always be aware of changes to a customer's status as soon as they are reported.

/ Lack of staff knowledge

Many frontline staff have a limited understanding of the ways in which their business can be abused by criminals. Staff often report that they would not feel confident analysing a customer's rationale and activity in relation to a particular product — let alone whether the rationale and activity are consistent with one another, or fit expected norms.

For example, a business loans a significant sum of money to a customer who claims to be a billionaire, to be used to purchase high value cars. The interest rate on the loan is 10%. The customer passes his screening checks, and media coverage suggests that he is indeed a billionaire as claimed. However, if the customer genuinely is a billionaire the transaction looks questionable: why borrow at 10% when you have access to cheaper capital? This is a deal which requires a closer look, and the conduct of some enhanced due diligence on the customer's source of wealth and current business activity.

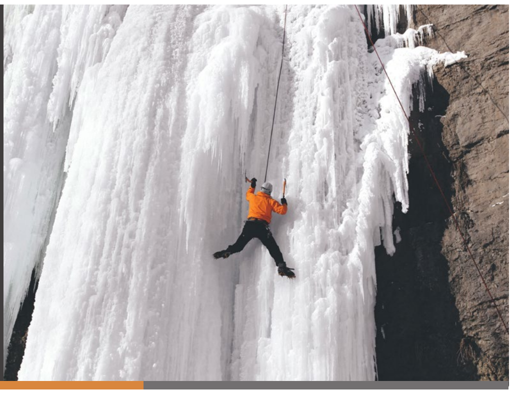
Developing staff understanding of the money laundering risks faced by your business is **not expensive.**

Along with initial screening and risk-based transaction and profile monitoring, it should be a core element of your financial crime prevention strategy. Effective KYC requires much more than verifying that customers don't have a criminal record.

It's not always possible to fully 'know' each customer, but training staff to know what the wrong sort of customers might look like will pay handsome dividends.

KYC360

Avoiding common screening pitfalls



/ Evidencing your work

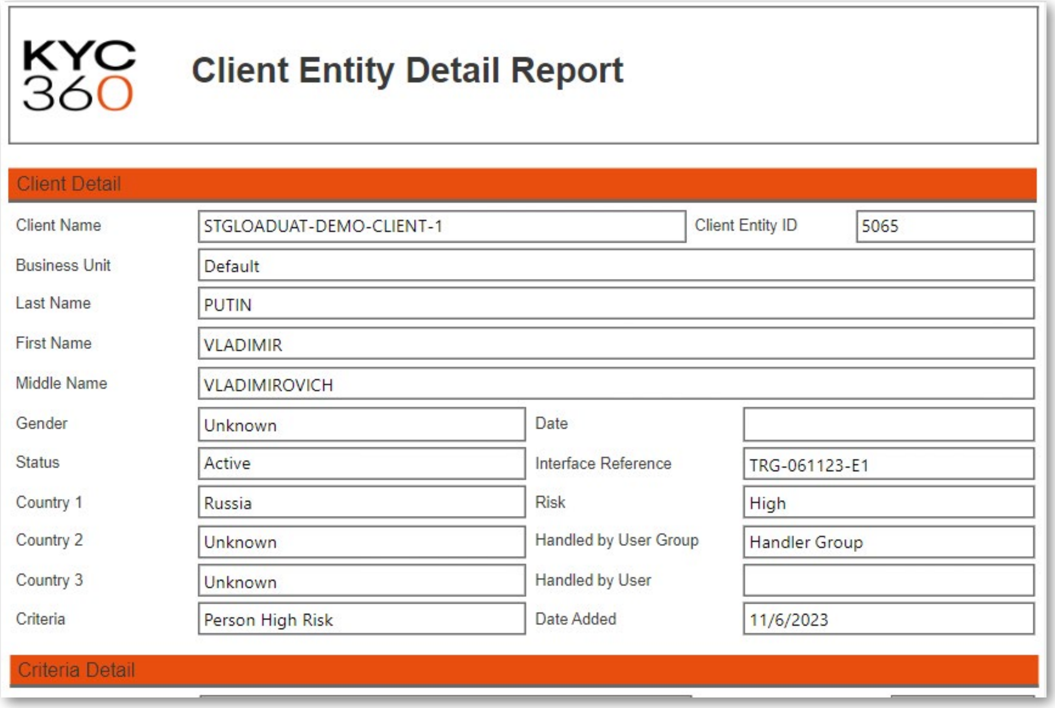
Under almost all regulatory regimes, businesses are obliged to keep good records of compliance- related work.

Document not only any screening you carry out but also any decisions you took on the basis of it (e.g. “we collected the following results and discounted them for this reason…”; “we made the following assessment of this adverse media report …”). Include minutes from relevant meetings.

Printed, filed reports are hard to search and tend to go missing; we recommend storing everything in a document management system, or at least on an appropriate shared server.

Modern batch screening technology should create a complete evidence trail automatically, showing all actions taken by your staff including adverse media searches carried out, so that the data is stored securely in one place, can easily be retrieved, and can also be analysed for management information purposes.

When assessing a batch screening tool, it is important to consider the audit trail which the solution provides. Whilst all solutions will record the results of screening, not all will capture users’ actions, reasons for taking a particular course, commentary, or supervisor comments which could be critical to evidencing the decisions that your business took in the context of future regulatory enquiries.



KYC 360

Client Entity Detail Report

Client Detail

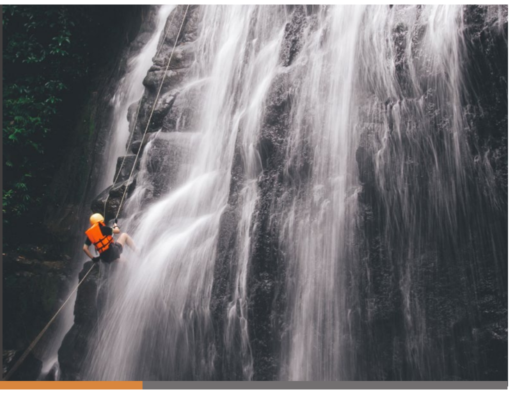
Client Name	STGLOADUAT-DEMO-CLIENT-1	Client Entity ID	5065
Business Unit	Default		
Last Name	PUTIN		
First Name	VLADIMIR		
Middle Name	VLADIMIROVICH		
Gender	Unknown	Date	
Status	Active	Interface Reference	TRG-061123-E1
Country 1	Russia	Risk	High
Country 2	Unknown	Handled by User Group	Handler Group
Country 3	Unknown	Handled by User	
Criteria	Person High Risk	Date Added	11/6/2023

Criteria Detail

Example detail report

KYC360

How KYC360 helps automate the screening process



To screen at scale successfully, you must not only have the best possible data at your fingertips, but you must also know exactly what to do with it. At KYC360 we've developed our screening technology to automate this for you.

Effectively reduce false positives by up to 95%.

The world's best data sources

We partner with the world's biggest data providers including Worldcheck, Lexis Nexis and Dow Jones. Our partner databases are updated daily giving you the security and peace of mind that comes from knowing that you are screening against the most extensive and accurate databases on the market.

System generated aliases for more precise results

We supplement the data from our partners with system generated aliases to augment the data and reduce the risk that incorrect inputs in first name and or middle name fields will lead to false negative results. This process protects our customers against the risk of missing relevant profiles in their search results.

Data Quality Assessment

We help you to identify and correct defects in your input data through a self service data quality assessment tool that comes as part of our Batch screening module. The function will check and provide you with a report on any data quality issues giving you the chance to take remedial steps and optimise your screening results.

Application of a risk-based approach to filtering and risk scoring

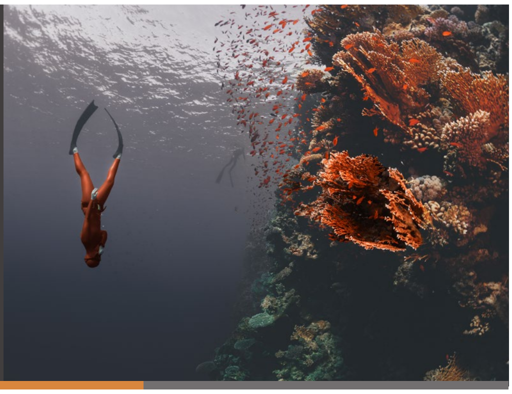
We then apply a risk-based approach to filtering and prioritisation of results. Our risk-based technology enables you to effectively reduce false positives by up to 95% while ensuring that you never miss a true match.

Configuration of risk based screening parameters

Our intuitive screening platform enables you to pre-set screening parameters based on a customer's risk scoring, enabling you to optimise your compliance operations while allowing you to evidence that you are following a risk-based approach even in the application of the technologies that form part of your three lines of defence against financial crime.

KYC360

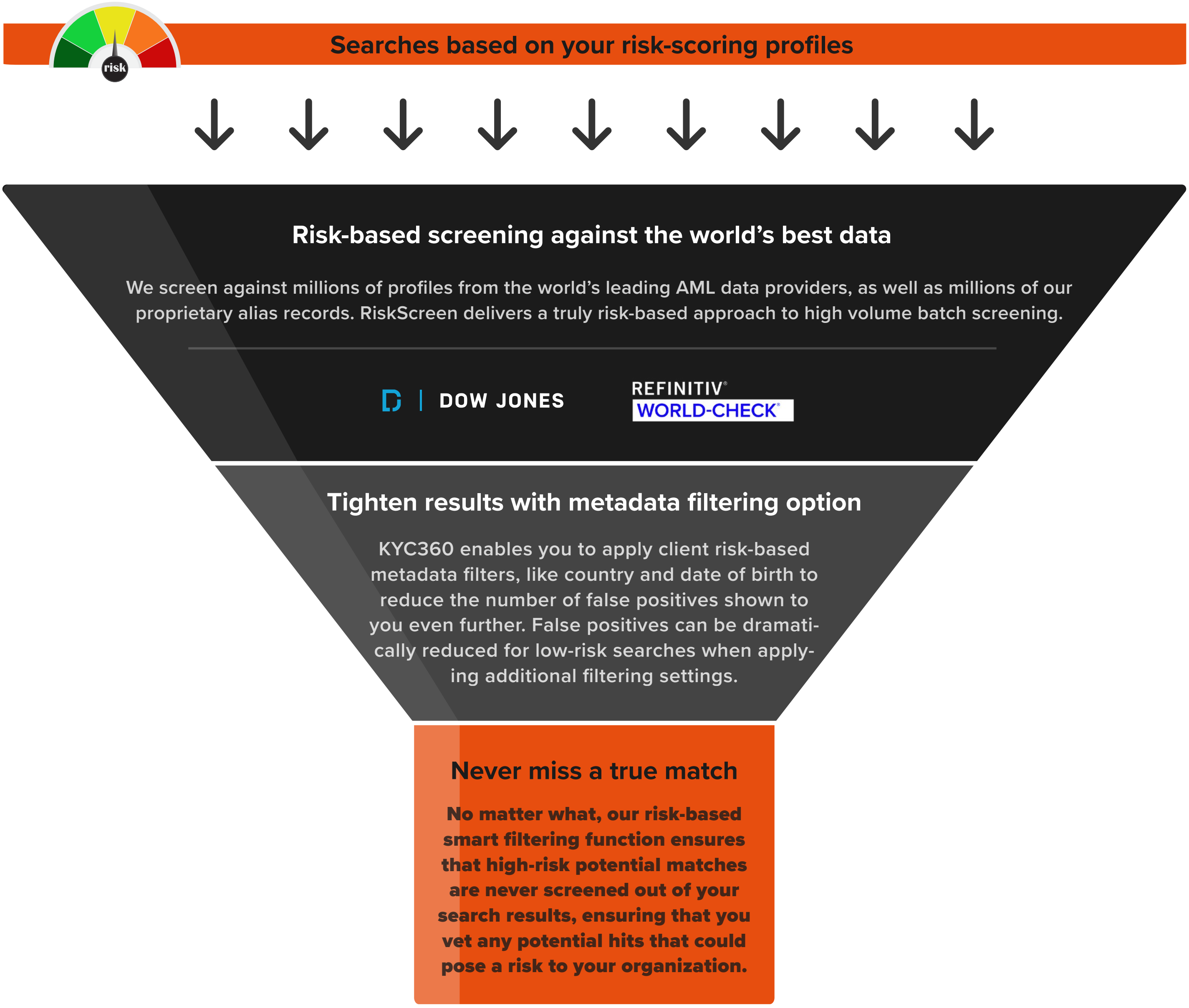
What is the 3D Risk-Based Approach?



1. Initial risk-based screening against the latest data from Refinitiv or Dow Jones. With KYC360, parameters are automatically adjusted according to a client's predetermined risk scoring, enabling you to effectively manage different risk levels.

2. The application of client risk-based metadata filtering options, including date of birth and country, to dramatically reduce false positives.

3. Our smart-filtering function automatically disapplies filter settings for any potential high-risk matches. Knowing you'll always see a potential sanctions hit enables you to tighten search and filter rules without worrying about missing important results.



Searches based on your risk-scoring profiles

Risk-based screening against the world's best data

We screen against millions of profiles from the world's leading AML data providers, as well as millions of our proprietary alias records. RiskScreen delivers a truly risk-based approach to high volume batch screening.

Tighten results with metadata filtering option

KYC360 enables you to apply client risk-based metadata filters, like country and date of birth to reduce the number of false positives shown to you even further. False positives can be dramatically reduced for low-risk searches when applying additional filtering settings.

Never miss a true match

No matter what, our risk-based smart filtering function ensures that high-risk potential matches are never screened out of your search results, ensuring that you vet any potential hits that could pose a risk to your organization.

What features do the best screening technologies have?

/ Technical features

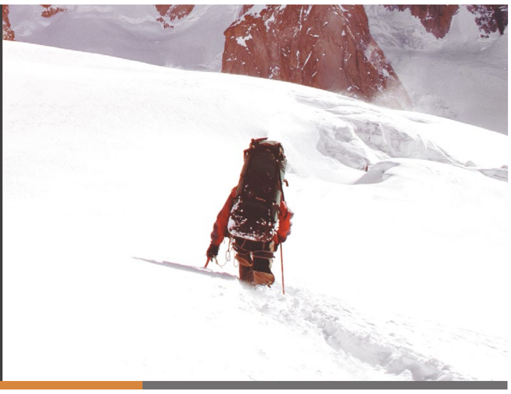
- The ability to conduct risk-based screening of customers.
- Maximum optionality on search parameters including, for example, inclusion or exclusion of social media sources.
- Full audit capture and reporting functionality.
- The ability to scrape web page content for inclusion in customer screening reports instead of subsequently relying on dead URLs.
- Automatic batch screening of unstructured adverse media sources as frequently as required.
- Multi-language enabled.

/ Data

- **Quantity of data.** It is vital that the data sources you are screening against are as extensive as possible including for example secondary sanctions ownership data.
- **Accuracy of data.** The data has to be constantly maintained and be as up to date and accurate as possible.
- **Organisation of data.** The data has to be well organised to enable the screening engine to utilise it in a consistent fashion to deliver accurate results.
- **Alias data.** Many ‘bad actors’ engage with businesses utilising aliases. The best data sets contain the most alias data.
- **Images.** The best data sets contain images to help users identify whether potential matches are true or false.
- **Languages.** The best datasets capture data across as many languages as possible.

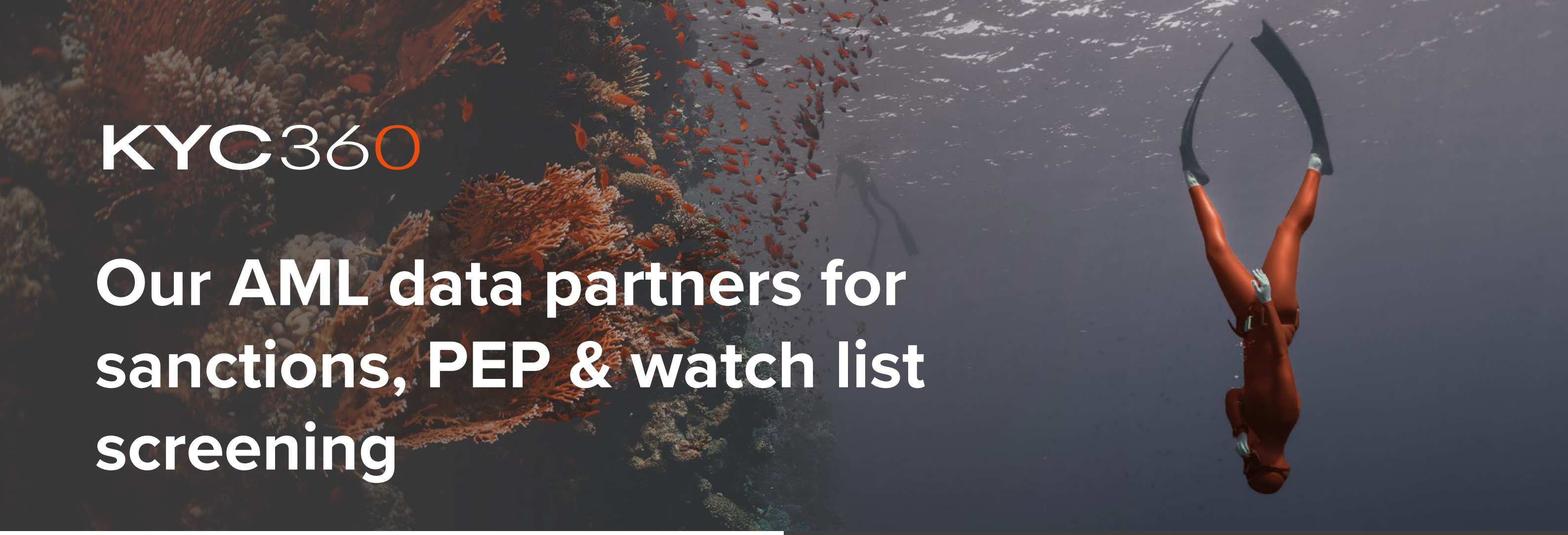
KYC360

Questions to ask your current screening provider



	/ Point / manual screening tool	/ Batch screening tool
1.	Can we add additional users of the tool at no additional cost or do we need to purchase additional licenses?	Can we screen our customers both instantly and overnight in a risk- based fashion?
2.	Can I customise the adverse media source that I am searching?	Can we handle potential matches in a risk-based fashion?
3.	Are the searches we conduct live or are we searching against a catalogue of profiles?	Can we utilise the metadata we hold on our customers as well as customer names to increase match accuracy?
4.	Do your profiles contain links to online sources? If so, how do you ensure those links remain live to protect us against the risk of losing source data?	What percentage of names screened result in false positive matches?
5.	Do you maintain a record of the searches we conduct?	Can your solution automatically search unstructured adverse media sources?
6.	Does your tool have EDD screening functionality?	Does your solution have full audit capture, and offer reporting using live data?
7.	Do you offer a full integration with Salesforce, if we use - or are considering using - it as our CRM system?	

If your current screening provider is unable to answer any of these questions in the affirmative, consider switching to KYC360 to optimise your screening practices, benefit from operational efficiencies and improve your risk governance performance.



KYC360

Our AML data partners for sanctions, PEP & watch list screening

DOW JONES

Providing truly global coverage Dow Jones data is maintained by a team spread across five dedicated research and monitoring centres providing 24 hour coverage across 68 languages. Over fifty percent of the Dow Jones research team are educated to Masters or PhD level.

One key advantage Dow Jones researchers have is the ability to leverage Factiva, Dow Jones' 40 year old archive of more than 32,000 sources in 28 languages. Hundreds of thousands of articles from these sources are added to Factiva daily.

Dow Jones Data is relied upon for AML/KYC screening purposes by the following:

- 3 of the 4 largest US banks
- 5 of the 6 largest Canadian banks
- 44 of the 45 largest Chinese banks
- 5 of the 7 largest Japanese banks
- 5 of the 6 largest Spanish banks
- 4 of the 5 largest French banks
- 4 of the 5 largest Scandinavian banks
- 7 out of the 13 Wolfsberg Group

LSEG RISK INTELLIGENCE

LSEG World-Check's world-class database of over four million records allows organisations to better have better awareness, knowledge and understanding of risk associated with their customers.

Hundreds of dedicated researchers and analysts based around the world help to maintain the World-Check database, allowing for coverage of over 700 unique sanction, regulatory and law enforcement watch lists.

World-Check's independent global media reports detail incidents relating to financial crime, fraud and corruption – information you may not find on official lists.

World-Check is established across five continents, allowing for around-the-clock monitoring of regulatory lists, major media outlets and governmental institutions.

The most stringent and well-established research methodologies are followed, ensuring validity and accuracy of all World-Check data.

KYC360's Screening Modules

/ Ad-hoc screening

The ability to quickly screen prospects or customers against datasets or adverse media sources on-line is essential. Our intuitive web-based manual screening solution 'Risk Screen' powered by KYC360 technology allows you and your employees to rapidly conduct manual screening across global sanctions, PEP and watchlist information provided by leading data provider Dow Jones as well as the whole of the world wide web from mainstream news to blog and social posts.

With no limit on the number of users you can deploy the use of RiskScreen across your organisation including front line staff and empower your first line of defence against financial crime.

- Screen individuals and companies online in real time
- Includes alias names for 'bad actors'
- Common name variants, across multiple languages
- Control risk-based search parameters
- Exclude irrelevant URLs
- Red flag results of interest
- Consolidate findings in a single report for future audit purposes
- Include your assessment of the search subject's risk level based upon search results
- Add comments
- Optional MRZ analyser allowing you to analyse and validate passport data

/ Batch screening

The KYC360 Batch screening solution is an award-winning technology that enables businesses to automatically screen customer names and meta-data on a continuous basis utilising the risk-based approach. Capable of screening anything from just a few hundred names to tens of millions of names overnight the solution can handle huge volumes at all risk levels giving businesses the assurance they need to evidence compliance with the risk-based approach irrespective of volumes.

- Virtually eliminate false positives with the world's first truly risk-based batch screening engine
- Handle tens of millions of names. Our screening solution can handle huge volumes at all risk levels
- Fully integrated with the world's best data sets from Dow Jones. World-Check and Lexis Nexis providing you with maximum optionality
- Complete workflow and audit capture – All activity at any single moment in time is captured for audit purposes
- Laser-sharp MI and reporting
- Super-flexible integrations

KYC360

KYC360's Screening Modules

/ Adverse Media Monitoring

Screening customers against adverse media sources on a continuous basis is now regarded as essential by businesses attempting to manage risk effectively. It is an important component of customer due diligence particularly for higher risk customers.
KYC360's adverse media monitoring function operates as an optional component of our Batch screening solution so that screening results are captured and handled in one place. With full open source coverage, our award winning functionality minimises false positives while maximising search accuracy.

- Store results alongside your sanctions, PEP & watch list screening records
- Subject AVM results to the same levels of audit & reporting as dataset screening
- Carry over handling of potential matches into periodic reviews
- Exclude hits which have already been viewed
- Refine search results by date and country
- Tailor searches by frequency or search terms
- Tailor searches by individual or groups of customers
- Massively reduce AVM false positive results with KYC360's award winning 3D risk based technology

/ Salesforce App

Our API technology enables full headless integration of KYC360 with your core platform. In addition to dozens of other integrations we are proud of being the first screening provider in the world to be invited to build an integration with Salesforce, the world's largest CRM provider. Our Salesforce native screening App is utilised by a large number of organisations for frictionless and automatic screening of leads and customers natively without the need for data import/export.

- Consolidate your system stack
- Save on tech licensing and support costs by eliminating your stand-alone screening solution
- Use KYC360 dashboards and workflow to allocate and handle potential screening matches
- Reduce false positives by up to 95% with KYC360's award winning 3D risk based technology
- Improve AML risk governance through full audit capture
- Comprehensive MI
- Integrated with world leading datasets

KYC360

Contact

See why hundreds of other businesses around the world trust KYC360 for their onboarding, screening and lifecycle management needs.

Get a demo today.
/ sales@kyc360.com
/ www.kyc360.com