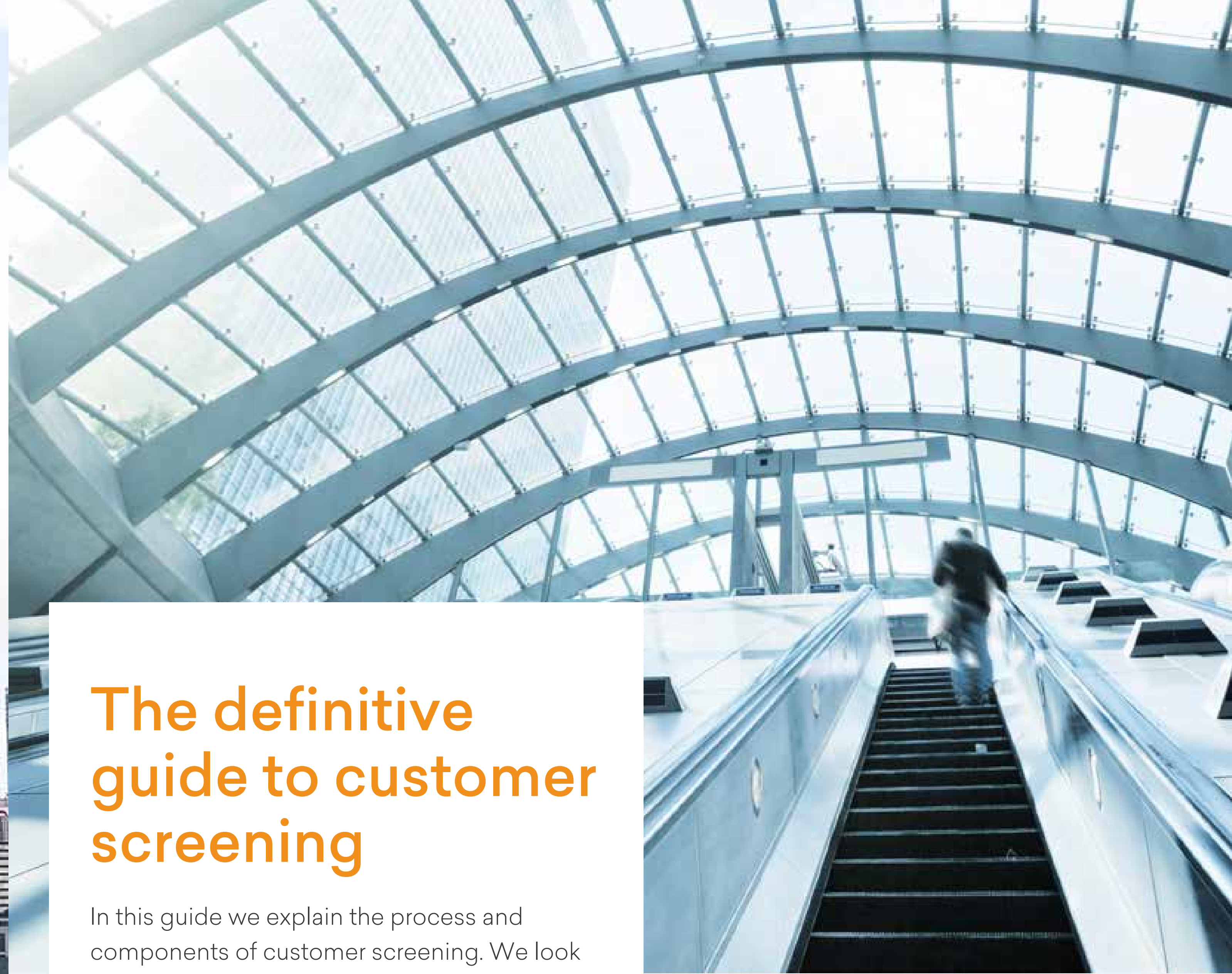
RiskScreen

powered by DOW JONES

The Definitive Guide to Customer Screening

Contents



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 to be aware of.

RiskScreen is a next generation AML solution delivered by KYC Global Technologies, one of the world's leading RegTech business focused on eliminating financial crime through smart technology.

RiskScreen is used by over 500 organisations globally for customer screening at onboarding, periodic review and overnight batch screening

As part of its commitment to financial crime prevention, KYC Global Technologies powers KYC360 - the world's leading AML knowledge portal.

What is customer screening?

Screening is the process of dynamically comparing the data you hold on customers, prospective customers, suppliers and counter parties against the data that is held within external data sources including sanctions lists, watch lists, PEP lists and adverse media, for risk management purposes.

Why screen?

The principle 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. 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, terrorist financing or tax crimes.

Customer screening is mandated by the anti-money laundering (‘AML’) laws of most countries and extends to all businesses operating within AML regulated sectors including banking, finance, law, accountancy, trust and corporate service providers, real estate agents, dealers in high value goods, insurance, lending and gaming.

Which businesses need to screen their customers?

The types of business that are legally required to screen their customers vary 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 Client (‘KYC’) obligations. The types of business commonly included in the regulated sector include:

- banks and credit institutions
- investment businesses
- money services businesses
- company and trust administration businesses
- lawyers
- accountants
- 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 of doing business with certain customers or to manage the risk of different forms of predicate criminality including bribery and corruption, an issue which is particularly acute in the natural resource, armaments and pharma industries.

Screening technologies

Every screening solution is comprised of two components;

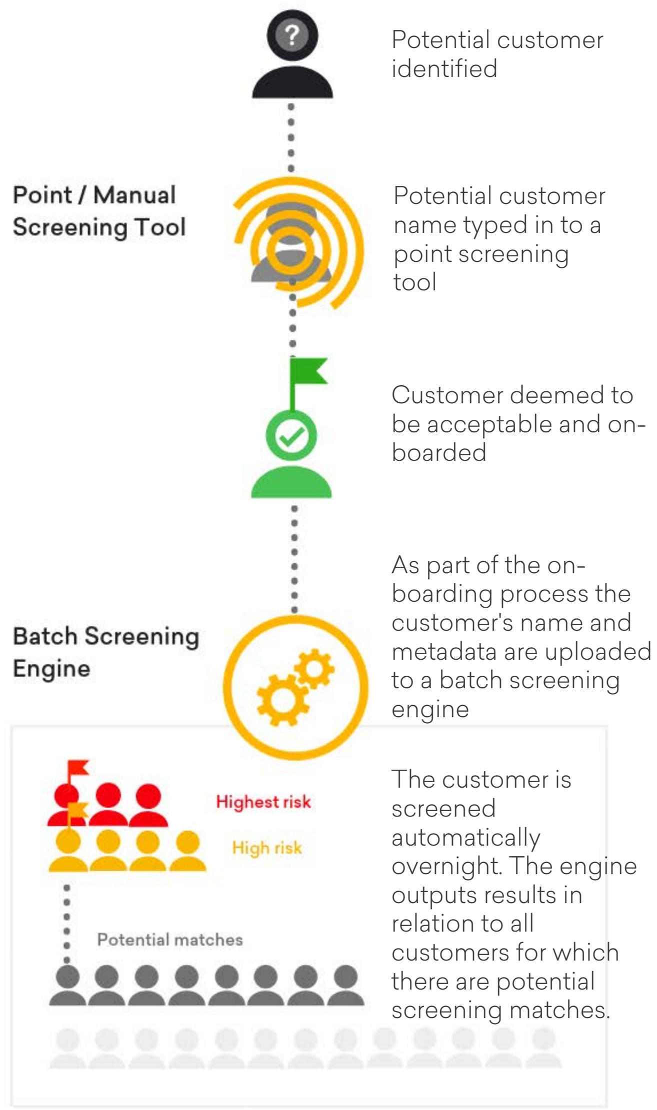
- A **screening engine** - the technology that runs the data analysis and produces the results
- The **external data** against which user customer data is compared

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 two types of screening tool:

- **Point/Manual Screening Tool** – This form of screening tool requires users to manually input the name of the customer they wish to screen. The tool then outputs the result 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

The challenge for businesses wishing to optimise their compliance performance is 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.



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.

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 consequenc-es, 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 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.

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

Smarter screening: A How-to Guide

What sources should I screen against?

As a minimum you should screen against Sanctions lists, PEP lists, and government Watch/Black lists.

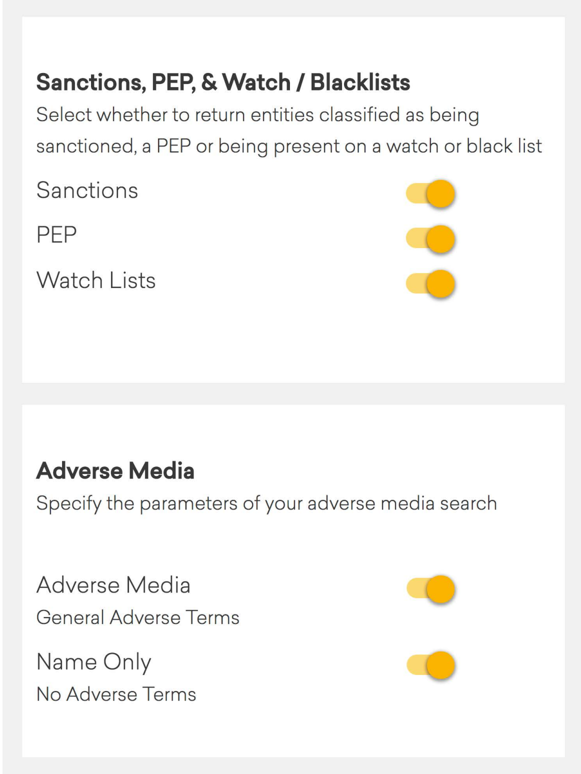
Politically Exposed Persons

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.

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.

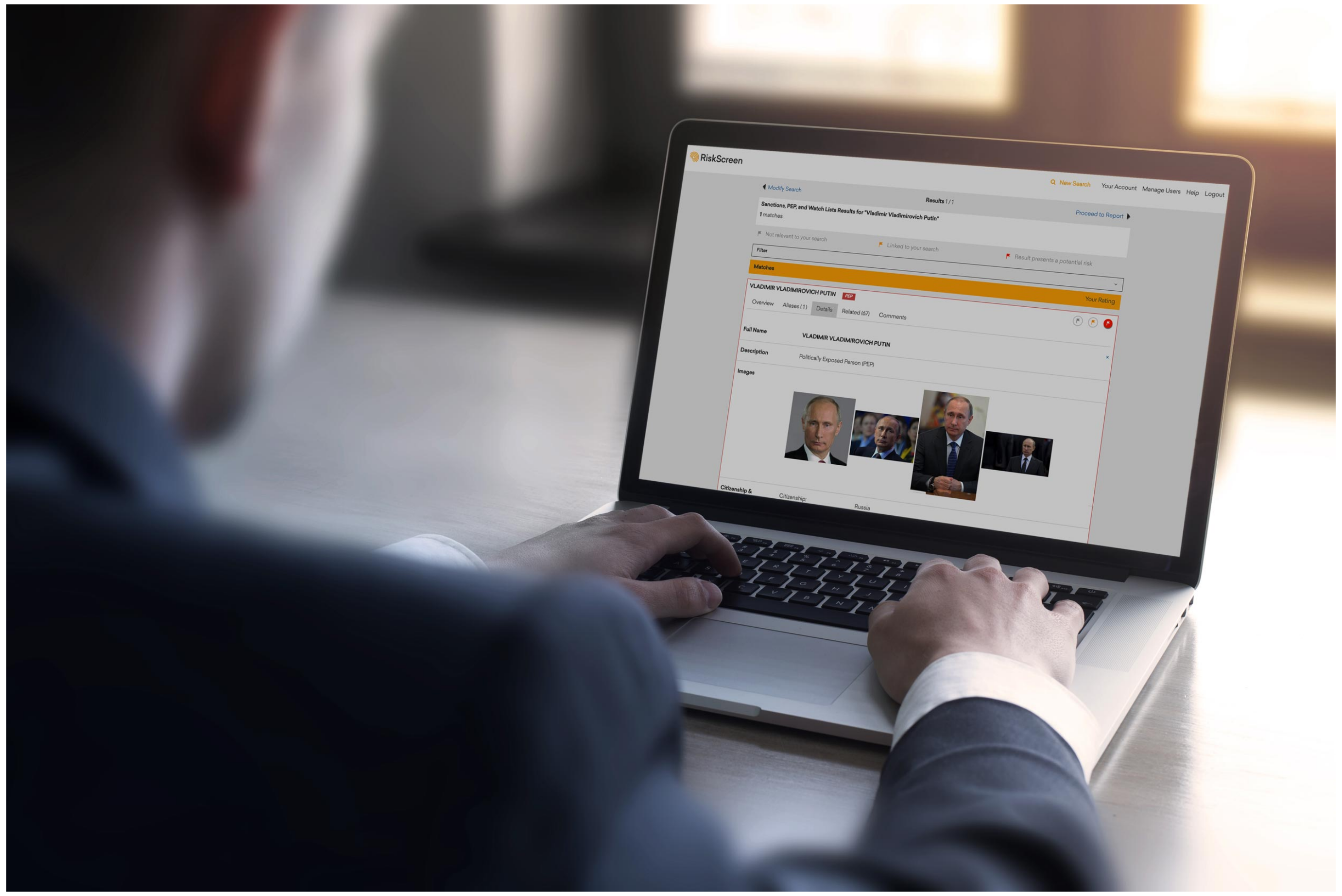
Many organisations make the mistake of only screening against a narrow list of sanctions regimes. It makes sense to screen against all publicly available sanctions regimes if you want to understand the full extent of your sanctions risk exposure.

Watch lists

Watch lists or black lists are official lists of individuals and legal persons 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. RiskScreen tracks over 4,000 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 traditional news media and publically available information more broadly. 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 inclusion on a watch list. 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.



The screening cycle

When should you screen?

The answer to this question depends upon how robust you want your compliance program to be. There are generally two approaches:

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

The second approach is much more robust because it leaves less to chance recognising that events impacting customer risk can occur very rapidly. The earlier a business is 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 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 and 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.

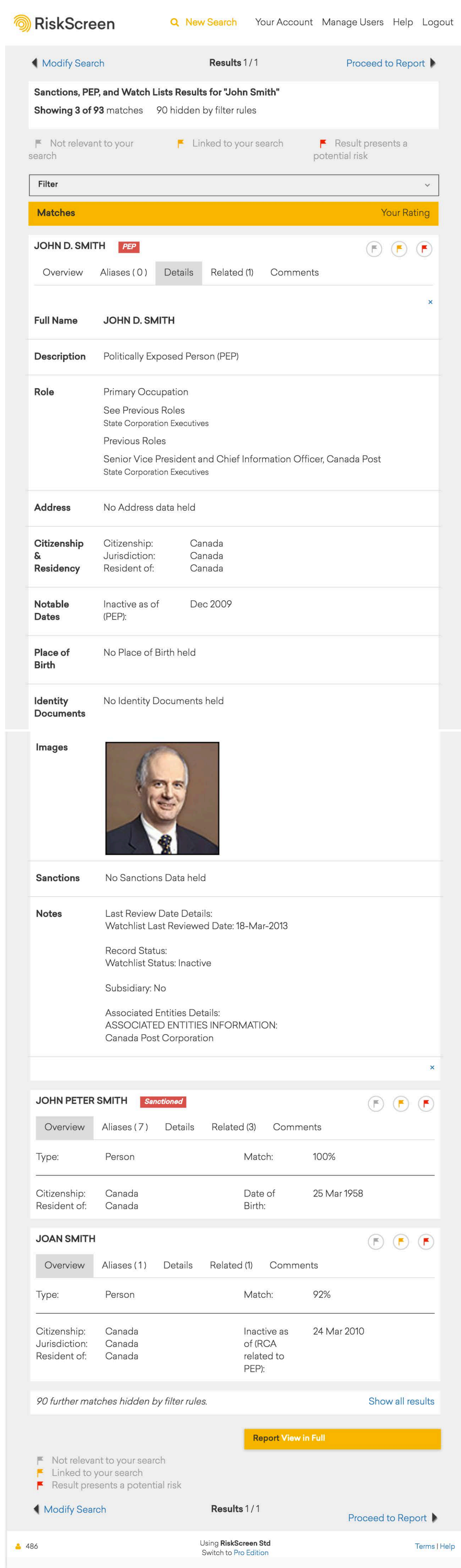
The form your EDD takes should depend on the nature and severity of the risk. It can vary from an adverse media check, to investigating corporate structures linked to an individual, to verifying income sources.

EDD should leave you confident that any risk has been mitigated and is unlikely to be realised.

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 on-boarding 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.



Interpreting results

1. Confirm that the results do indeed relate to your customer. For an exact name match, 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. PEPs, sanctions and watch lists are drawn from databases compiled by qualified authorities about individuals 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 an OpenCorporates search, 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.

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!

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.

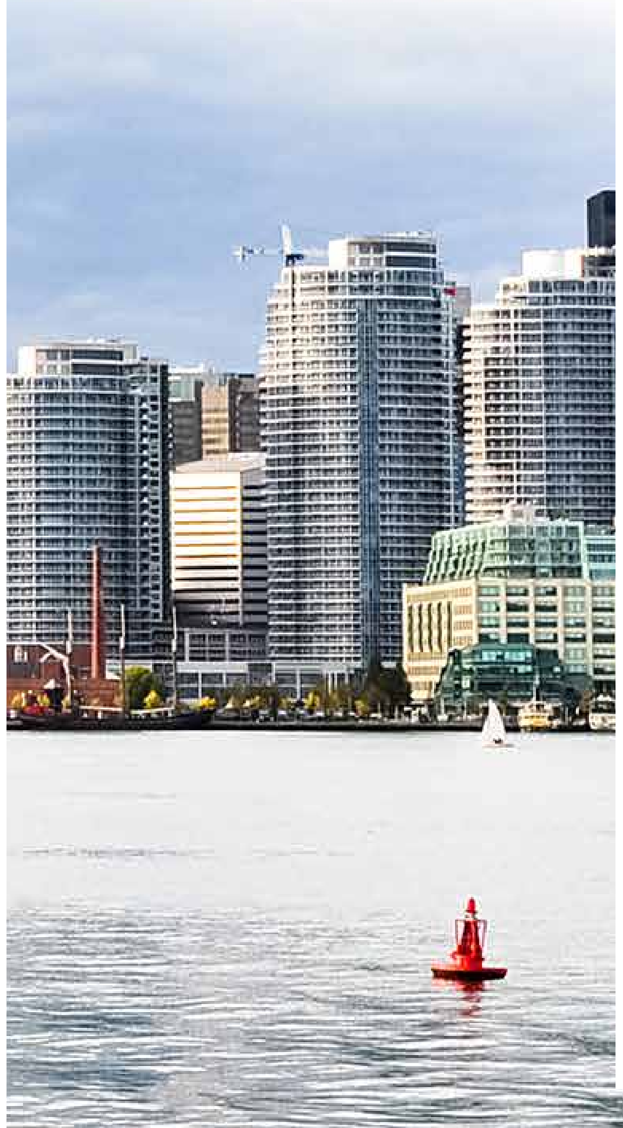
Developing staff understanding of the money laundering risks faced by your business is not expensive. Along with initial screening and risk-based transaction and profile monitoring, it should be a core element of your financial crime prevention strategy. Effective KYC requires much more than verifying 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.

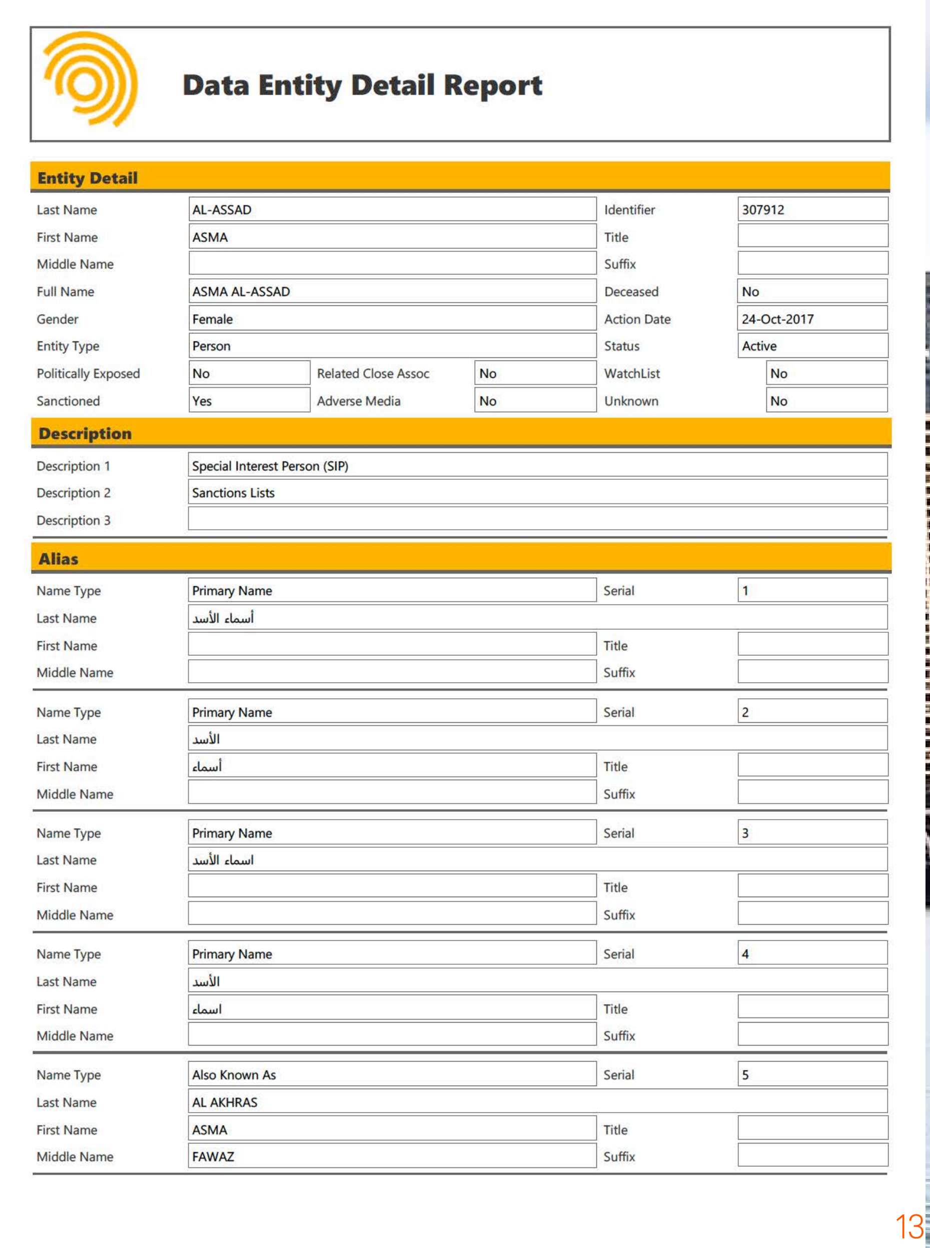
Evidencing your work

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.





Data Entity Detail Report

Entity Detail

Last Name	AL-ASSAD			Identifier	307912
First Name	ASMA			Title	
Middle Name				Suffix	
Full Name	ASMA AL-ASSAD			Deceased	No
Gender	Female			Action Date	24-Oct-2017
Entity Type	Person			Status	Active
Politically Exposed	No	Related Close Assoc	No	WatchList	No
Sanctioned	Yes	Adverse Media	No	Unknown	No

Description

Description 1	Special Interest Person (SIP)
Description 2	Sanctions Lists
Description 3	

Alias

Name Type	Primary Name	Serial	1
Last Name	أسماء الأسد		
First Name		Title	
Middle Name		Suffix	
Name Type	Primary Name	Serial	2
Last Name	الأسد		
First Name	أسماء	Title	
Middle Name		Suffix	
Name Type	Primary Name	Serial	3
Last Name	اسماء الأسد		
First Name		Title	
Middle Name		Suffix	
Name Type	Primary Name	Serial	4
Last Name	الأسد		
First Name	اسماء	Title	
Middle Name		Suffix	
Name Type	Also Known As	Serial	5
Last Name	AL AKHRAS		
First Name	ASMA	Title	
Middle Name	FAWAZ	Suffix	

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 including or excluding 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 URL's
- Mobile enabled to allow searches to be conducted by 'front line' staff whenever and wherever necessary
- 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.

Book a free demonstration of RiskScreen by visiting www.riskscreen.com

Questions to Ask Your Current Screening Provider

	Point / Manual Screening Tool	Batch Screening Tool
Q. 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 manually and overnight in a risk based fashion?
Q. 2	Is your tool mobile enabled?	Can we handle potential matches in a risk based fashion?
Q. 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?
Q. 4	Do your profiles contain URL's to on-line sources? If so how do you ensure those URLs are live to protect us against look back risk?	What percentage of names screened result in false positive matches?
Q.5	Do you maintain a record of the searches we conduct?	Does your solution have full audit capture?
Q.6	Does your tool have EDD screening functionality?	Can we run reports containing live data for MI reporting purposes?

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

RiskScreen powered by 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**

RiskScreen CORE

A highly cost effective, powerful manual screening tool designed for on-boarding and periodic review

- Search world leading Dow Jones Data and public search engines in one application
- Add additional users across multiple locations at no additional cost
- Designer led user interface
- Mobile enabled
- Full reporting functionality
- Multi language capability
- Entry level cost of only £675

RiskScreen BATCH

Next-generation batch screening technology for ongoing monitoring of customer risk profiles

- Risk based overnight screening of up to 20m customers
- Searches world leading Dow Jones data
- Reduces false positives by 90%
- Risk based match handling
- Full audit capture
- Full reporting functionality
- Ultra-secure On-site or Hosted versions
- Link to CRM through easy to install API

To learn more or to schedule a demo visit www.riskscreen.com

RiskScreen powered by DOW JONES

Contacts

To discuss the points raised in this paper in relation to your organisation, contact:

Stephen Platt

Chief Executive Officer, KYC Global Technologies

T: +44 (0) 1534 816444
E: stephenplatt@kycglobal.com

Mark Cobby

Sales Manager, KYC Global Technologies

T: +44 (0) 1534 816444

E: markcobby@kycglobal.com