alessa

How to Test your Sanctions and Watch List Screening Software

Is Your Screening Software Working at Its Best?

As part of an effective Financial Crime Compliance (FCC) program, banks and other financial institutions (FIs) need to have a sanctions and watch list screening solution in place to assist with the identification of sanctioned individuals and organizations (entities).

For those FIs that have had a screening program in place for many years or for those looking to implement a new one, it is important to test its effectiveness during the initial implementation, as well as, periodically.

What does testing a sanctions and watch list screening solution entail? Well that depends on your solution but aspects that should be audited include ensuring the right people have access to the sanctions or watch list data, examining data flows for when new sanctions of third-party data files are made available, how the system filters and matches names and how potential name matches are handled, investigated and tracked.

In this article, we review key areas that compliance teams should consider auditing to ensure that their sanctions and watch list programs are effective.

Equip People with Tools They Need

A total audit cycle needs to start with the people you have on your front lines. You need to ask yourself if you have the right people and if they have the tools they need to do the job. There are a number of questions you need to answer when looking at your compliance staff:

- Are your people properly trained?
- Do they have access to all of the necessary regulatory documents, corporate standards, as well as, your FI's risk policies?
- Can they get access to those documents very quickly?
- Do you have processes in place for training and how does that training process work?
- Is that training process always used?
- Do you have analysts and frontline compliance personnel who are properly trained to both do their work on a day-to-day basis, but also understand the work ongoing?

Remember a "must-read" document in a repository somewhere where your personnel cannot get access to it, is not going to be effective. Instead, analysts and anyone else that is involved with AML and know your customer (KYC), are regularly trained and have access to all of the reference documents they need.

Are You Using the Right Risk Reference Data

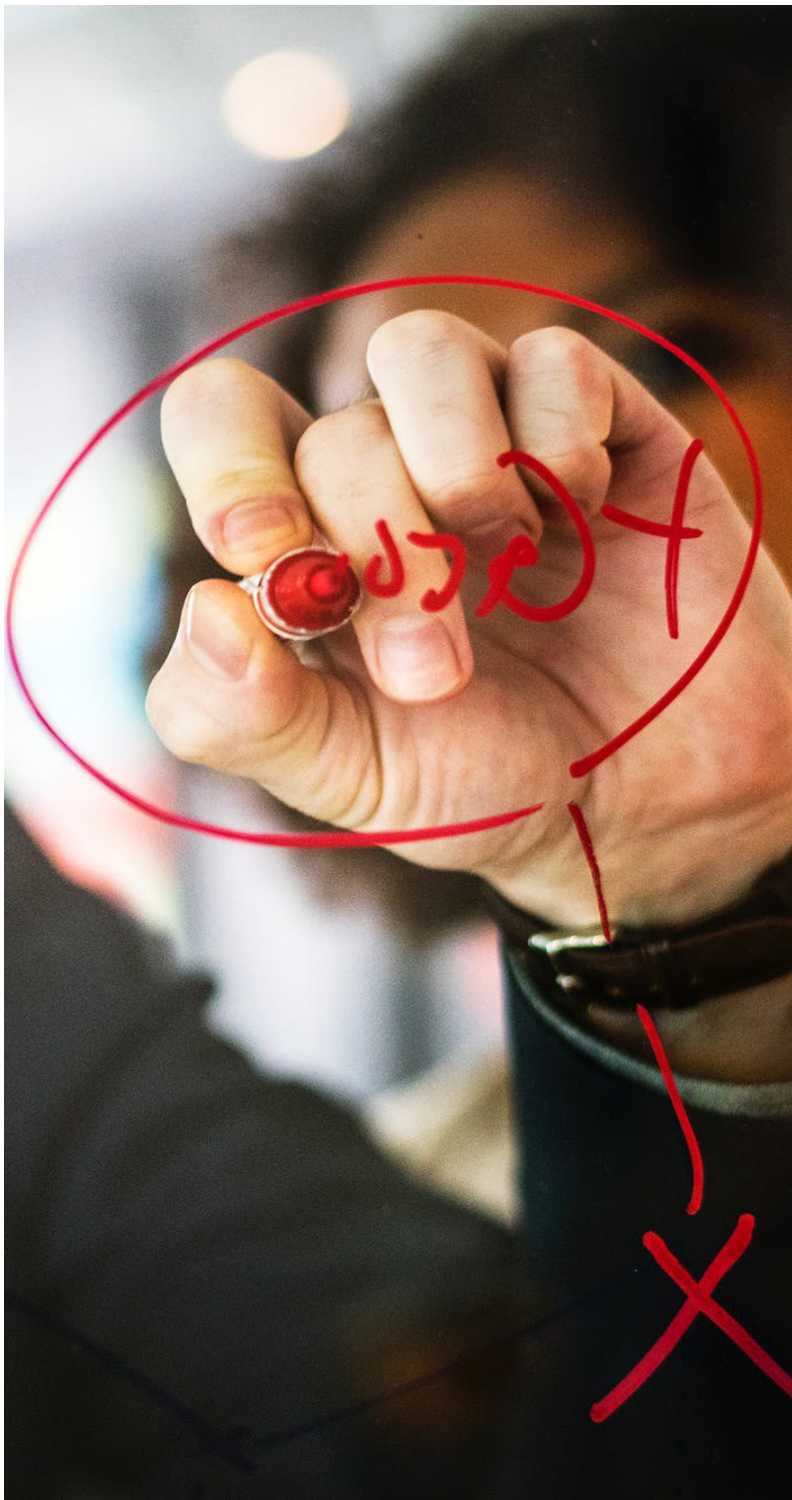
Risk reference data is a critical part of your screening system. Often, risk reference data could be data that you get directly from regulators, law enforcement and/or from one or multiple external vendors. These vendors provide different levels of quality and different levels of guarantees. Your reference data could also be information from within you own sources.

One of the things that's key for you to know is what guarantees do you have on the data and is the data meeting your compliance needs? Many FIs will buy external data and just trust that it works but it may or not be the right data for them.

For example, if you are at a small bank in Canada's Yukon, your risk profile is going to be very different than if you are a tier-one financial institution on Wall Street. Therefore, the sanctions lists that you have to comply with may be different as well.

You will likely have to comply with global sanctions and will also want to screen for politically exposed persons (PEPs). However, there may also be other data files that are applicable to the jurisdictions where you operate in and will satisfy your risk tolerance.

For the most part, it is always better to comply with more than less but you will have to evaluate cost of subscribing to data files against the time spent by personnel in investigating potential matches (especially when relying on unreliable internet searches or using poor quality data).



Is Your Reference Data Reaching Compliance?

In addition to which data files should be used, how the reference data flows into the organization, to the various lines of business and into your compliance applications is an important consideration.

When auditing your data flow, understand how your organization or your data vendor deal with additions, deletions and updates to sanction records.

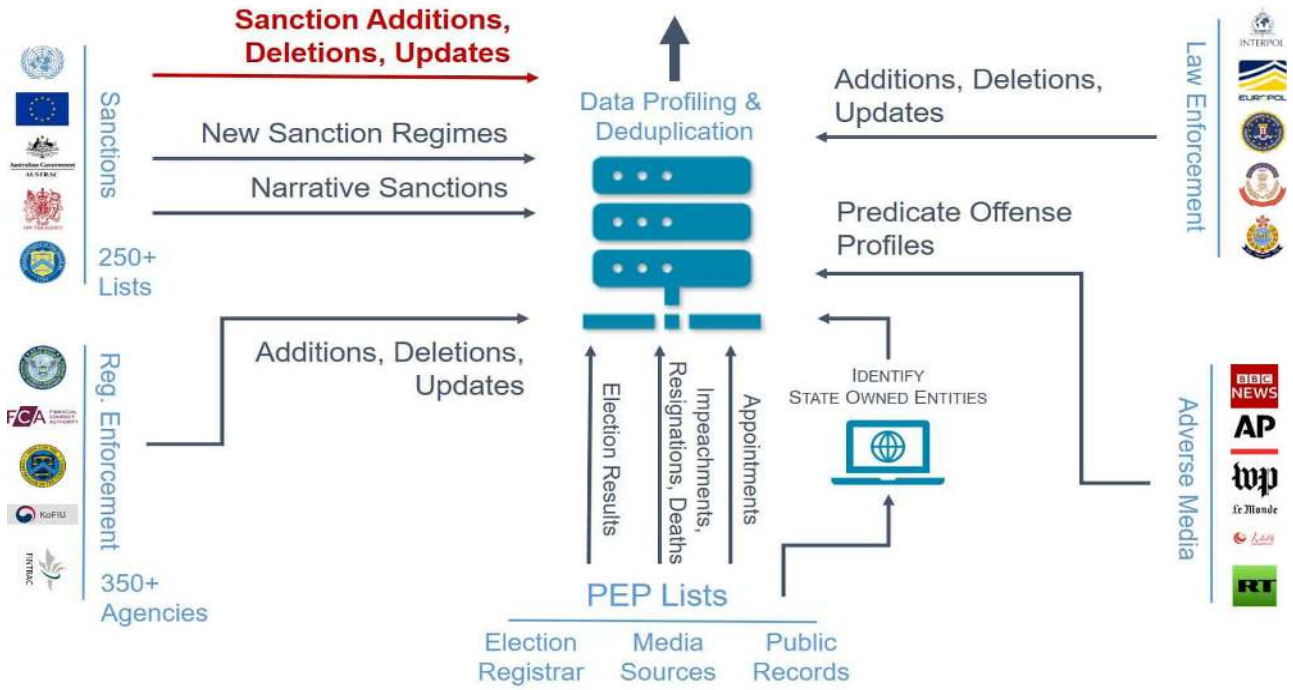
For example, when OFAC, EU, AUSTRAC or FINTRAC comes out with a new sanctions policy or a new sanction list, how are you identifying those updates?

Once you identify the updates, how are you incorporating that data? You should not rely on "hope for the best" or that your data vendor includes this data.

It is critical that every compliance department, especially the compliance head, knows how regulatory intelligence updates are incorporated into their compliance system.

Once you know how sanctions updates are identified, look at the process and the time it takes for you or your data vendor to get that data and into a structured format that can be used by your compliance application and team.

Most data vendors are going to have a guarantee time for how quickly it gets those sanction updates, but they will also have an average. You will want to know and document the worst and normal case scenario for sanction updates.



Map out how risk reference data, including additions and deletions, is flowing into your organization

Don't Forget about Narrative Sanctions

You also need to understand how your data vendor pulls in narrative sanctions (or implicit sanctions). Narrative sanctions are those sanctions where the administering body does not only list specific individuals or entities, but lists of criteria that are required for inclusion.

These non-listed entities are a challenge for financial institutions, as there is no finite sanction list to follow yet still they must ensure that they do not transact with them.

For example, in the case of Russian sectoral sanctions, a number of businesses are listed but the subsidiaries of those businesses are sanctioned as well. There could be thousands of subsidiaries that need to be identified and you need to make sure that your data vendor or your database administrator, is pulling sanctions data from source and you get access to these narrative sanctions.

Not only do you have to ensure that you get the data, you also have to ensure that you are receiving data from the right sources. This may include organizations like FinCEN, FCA, FINTRAC and any other financial intelligence units (FIUs) that regulates your operations.

Finally, you want to understand how additions, deletions, updates and new regulations are managed within your data, document the process and ensure that it complies with your risk-based approach.

Using Law Enforcement and Adverse Media Data

You want to ensure that you are screening records for relevant risk against lists from local, national and international law enforcement agencies, like Interpol, Europol and the FBI, for FATF predicate offences. These may include some or all of the list below, depending on the country's domestic laws:

- participation in an organized criminal group and racketeering;
- terrorism, including terrorist financing;
- trafficking in human beings and migrant smuggling;
- sexual exploitation, including sexual exploitation of children;
- illicit trafficking in narcotic drugs and psychotropic substances;
- illicit arms trafficking;
- illicit trafficking in stolen and other goods;
- corruption and bribery;
- fraud;
- counterfeiting currency;
- counterfeiting and piracy of products;
- environmental crime;
- murder, grievous bodily injury;
- kidnapping, illegal restraint and hostage-taking;
- robbery or theft;
- smuggling; (including in relation to customs and excise duties and taxes);
- tax crimes (related to direct taxes and indirect taxes);
- extortion;
- forgery;
- piracy; and
- insider trading and market manipulation.

Adverse media or negative news is unfavorable information found across a wide variety of news sources, blogs, social media feeds and more. Like law enforcement data, you are looking for involvement in FATF predicate offences.

When reviewing the role of adverse media in your screening or enhanced due diligence program, you want to see how structured and unstructured data is handled.

Adverse media can be a huge mountain of data. In addition, you want to look at how you deal with adverse media both from a structured and unstructured way.

When it comes to structured adverse media, do you have a data vendor that can structure adverse media profiles for you? For unstructured adverse media, where are you getting those profiles and how are you able to be as efficient as possible with screening adverse media?

What you want to avoid doing is relying on internet/ Google searches as a way to check for adverse media. More automated ways can target specific sources, filter the data intelligently, make the process more efficient and reduce the risk of missing an individual that warrants further consideration.

Managing PEPs and State Owned Entities

For PEP data, some institutions will get this from the actual sources. Other ones will get this from risk reference data.

With PEP data, watch for election results, impeachments, resignations and deaths. Sometimes people prematurely leave office or appointments may be assigned for non-democratic countries. You want to make sure these are covered, not just the election cycles.

You also need a process for identifying state owned entities. Whether that is from a data source or looking up ownership records, you need to make sure that you are identifying state owned entities and any entity that owns at least 25% (or any state ownership, depending on the jurisdiction). You also have to have a policy around state owned entities.

At a higher level, you need to have policies in place for identifying and documenting ultimate beneficial ownership (UBO) information. There are now requirements put forth by FinCEN and by EU's AMLD5.

Making PEP, adverse media, state owned entities and UBO data available for your compliance team can be an overwhelming and complicated exercise. This is where data providers can be very helpful but you have to look at the quality of the data.

For example, someone may say they have PEP data but how deep does the data go? You want to ask detailed questions about the geographic reach, does the data go beyond world leaders, how many PEPs of each type to they have, and so on. Compare list features from providers so you can make the best choice for your organization.

Client, Transaction Data Flow and Remediating Hits

Client Data: Aside from reference data flow, you also want to look at client data flow. Starting with lines of business data, one of the first things organizations should be doing is client data de-duplication.

For many institutions, client teams have different reference databases for each line of business. Often those are in different formats and different structures. That means in some cases you are screening dozens of records separately.

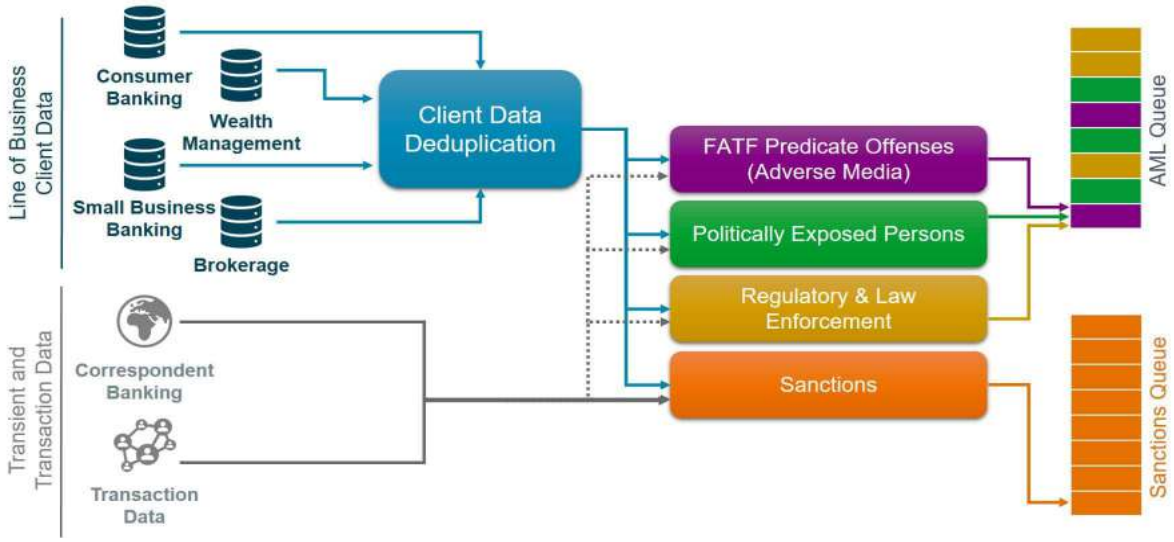
By combining the data of individual clients into one, you can ensure that you are not screening the same individual multiple times because they have different accounts in different parts of the business. You also get a holistic view of an entity's products, activities, behaviors, patterns and their associated risk.

You need ensue that you are screening your clients against the different categories of risk based on lines of business (products and services) and geographies.

When screening based on line of business, you want to make sure that you are screening them in the most risk averse way based on all of the products that they have selected. You want to screen them against sanctions, enforcement, PEPs and adverse media data.

By geography, you may select sanctions lists and adverse media. You may decide to opt out of adverse media screening based on the overall risk profile, which may depend on the value of the transaction or business and the geography.

The above criteria mean you may not need to screen your local small-value consumer banking individuals the same way as your wealth management, brokerage or foreign accounts.



Combine and deduplicate client data from different lines of business and correctly prioritize screening hits

Transaction Data: In addition to client data, you also have your transient and transactional data, which includes correspondent banking and transactional data.

These are cases where you are not engaging in regular ongoing relationships with an individual or an entity. Instead, you are dealing with immediate transactional relationships. Your screening requirements are very different in these cases.

When it comes to transactional data the most important thing is time. You want to make sure that you have mitigated your risks but you also want to make sure that you have done your screening in an efficient manner.

When it comes to transient and transactional data, it is largely an institution screening for sanctions. However, you may want to consider screening transactional data against a larger set of lists as well. This is driven by the risk profile of the transaction and would include considerations like the value of the transaction and associated jurisdictions.

Remediating Screening "Hits": It is critical that your screening "hits" are divided into separate queues – one for sanctions and one for everything else.

Some institutions that will triage screening hits in more queues, but what is critical is to have sanctions hits pushed to the top of that queue.

Some organizations have a team for dealing with sanction hits. For those who do not, deal with your sanction hits first. If there are two queues, you want to make sure sanctions goes first and everything else filters in behind those sanctions.

Using Date of Birth Configuration in Screening

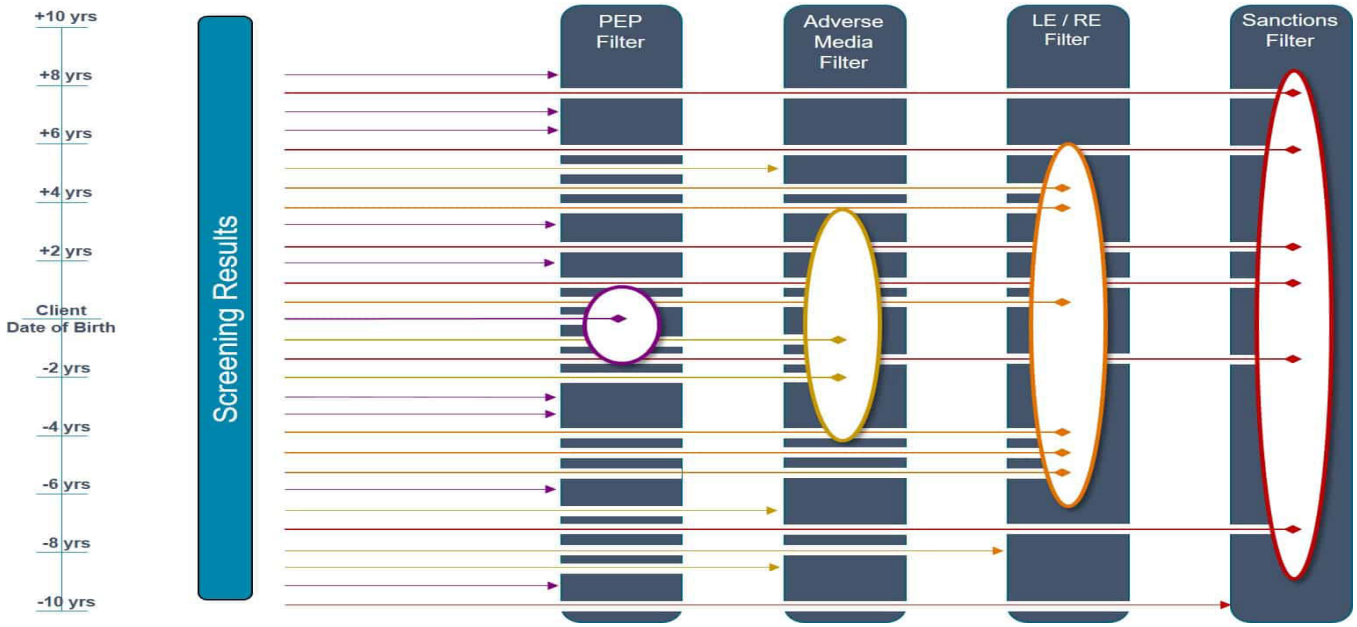
Dealing with dates of birth can be exceedingly frustrating. People have a date of birth, so why do you need to screen a large window around their date of birth? The reason is twofold. One is high risk individuals are going to do things to obscure their real date of birth. The other is that there are many jurisdictions where birth certificates do not exist.

People may not know their exact date of birth and they may not have any documentation to verify it. For some individuals, dates of birth can be guessed or interpreted based on other characteristics such as when they went to school or when they got married, this would be accurate to within a few years at best.

In the cases where an exact date of birth is not available, date of birth filters should be set to match the level of risk. For example, you can filter your screening results against a PEP filter with a configuration of plus or minus one year. This will narrow your screening hits to the most likely results and helps to balance resources spent while still allowing for a risk-based approach.

If you screen for adverse media, this can be a larger range such as plus or minus four years (depending on your risk appetite).

You will want to screen against law and regulatory enforcement data with a much wider net, say for example plus or minus five or six years.



Adjusting screening filters can reduce number of matches but risk should be considered

Finally, for sanctions screening, you want to set a very wide filter. Some institutions may decide to set the filter to 10, 15 or 20 years while others ignore date of birth for sanctions completely.

When determining your screening filters, it is always about risk versus work.

With any filter, you are introducing the risk of false negatives. It is important to understand this fact and accept it, unless you are willing to investigate every potential screening hit. You want to set your filters so you are not missing any high-risk false negatives.

You can mitigate some of the risks, depending on jurisdictions for date of birth. Some regions have reliable date of birth information so you can set a tight date range for PEPs. For high-risk jurisdictions, you will want to set a wider threshold.

It is worth mentioning again that with screening filters there is a chance you will miss something but you do need to take a responsible view of how to balance costs versus risk.

While ideally you would want screen every potential high-risk individual, realistically you want to ensure that your screening is targeted and that you catch the worst offenders.

Tackling the Complicated Task of Testing Name Variations

Name variations is an exceedingly complicated part of the screening process. Every organization should ensure that they spend enough time testing their system to ensure that it can handle name variations, including variations in upper and lower cases.

Variations to test for include:

- **Identical matching** is where you match the full name against all the lists. Not only are you testing the matching process, you are also testing the data flow to ensure that you get a positive match against your different sources
- **Phonetic similarities** is where you test names that sound similar, like Craig and Greg
- **Missing or additional hyphens or spaces** can occur when you are converting character sets (a non-Latin name to a Latin name). You want to make sure that you can deal with differences in punctuation, missing components or letters.
- **Missing components/letters or truncated name** can become important an important consideration with very long last names. You want to know the character limitation of the different fields that you screen against and what happens if it passes that limitation?
- **Incorrect database fields** can occur if data is entered from other systems are not divided correctly.
- **Spelling differences or similar names** is where a name can be spelled in different ways. For example, Sean versus Shaun, Shawn or Sian or Jennifer versus Jenifer, Jenniffer or Genifer. You can also have Willliam, Bill, Will or Willy.
- **Titles and Honorifics** are titles likes Reverend, Imam, Mister, Miss, Lady or Lord. If during screening some includes a title or honorific, is your system able to capture that?
- **Out of order components** is when given names are switched with surnames etc.
- **Multiple languages** – can your system handle names in their native character set like Arabic or Chinese?
- **Nicknames**, whether known or AKAs (also known as), you should test how your system these variations. You should also know how your system identifies and deals with low-quality AKAs and how does it risk rank those as results.
- **Initials** – what happens if someone enters an initial rather than the full first name?
- **Similar names** are names like Amelia, Melia and Emelia which may sound similar but are different.
- **Noise simulation** is more difficult to test but can include cases where characters are added or are switched. For example, how does your system deal with extraneous characters or when a zero is used instead of the letter O?

Accents, Transliteration and Translation: Screening names in their non-Latin native characters can be a challenge for FIs that communicate in languages that use Latin characters. However, even languages that use Latin characters, like Spanish, Portuguese, Dutch, French and German, can be challenging to test with their unique letters and accents.

As an example, you have the Hispanic name Jose, or José. Your system needs be able to deal with names with and without the accent. You also need to decide how it will handle variations like Joe, or Joseph, which can be a translation of José.

You may find variations of a name such as Johanna in German, which can become Joanna or Joanne. It is the same for thing Alessandro in Italy to Alexander, Alex, or Sasha in Russian. Understanding and having the ability to deal with these transitions becomes important.

When we talk about non-Latin conversions, it gets even more complex. Some may transliterate their names while others may translate their name.

Transliteration is the process of transferring a word from one alphabet or language into the corresponding, similar-sounding characters of another alphabet. Translation tells you the meaning of a word in another language. For example, ﷲ when transliterated is “Allah” and the translation is “The God”.

Testing Technique Used	Given Name	Surname
Identical Matching	Jeniffer Beaney	CAMACHO CAZARES
Phonetic Similarity	Jennifer Beaney	CAMACHO CASARES
Missing or Additional Spaces and Hyphens	Jeniffer Beaney	CAMACHO-CAZARES
Missing Components or Letters	Jenifer	CAMACHO CAZARES
Incorrect Database Fields	Jeniffer	Beaney CAMACHO CAZARES
Spelling Differences	Jenniffer Beany	CAMACHO CASAREZ
Titles and Honorific	Mrs.	CAMACHO CAZARES
Nicknames	Jenny	CAZARES
Out of Order Components	Jeniffer	CAZARES CAMACHO
Truncated Components	Jeniff	CAMACHO CAZARES
Initials	JR	CAMACHO CAZARES
Similar Names	Jenny B	CAMACHO CAZARES
Noise Simulation	J3niff3r 4eaney	CAMACH0 CAZARE$

Test different name variations to measure effectiveness of name matching algorithm

Some people will transliterate their name while others may translate their name, which adds complexity to the screening process. Below are some examples of names that may be transliterated or translated from Korean or Thai

The Many Names for Muhammad: The name Muhammad is one of the most common first names in the world and therefore can be one of the most misspelled when onboarding clients. There are at least 65 common variations of the word of the name Muhammad based on different jurisdictions, different standards across different countries and in different scripts.

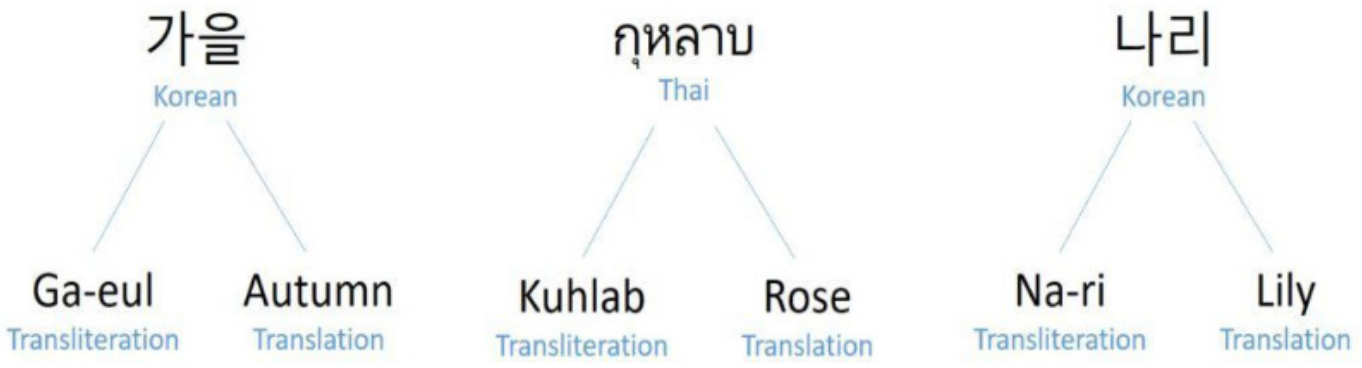
One of the big challenges is when someone comes into your institution with the name Muhammad, you need to ensure the way they spell it is the way is actually appears on file. This could be an error in data input or how the name was entered.

Where Muhammad gets even more complicated in jurisdictions that have no last names. For example, if you look at Indonesia, Somalia and Burma, those three countries in general do not have surnames. People go by only one given name.

Indonesia is one of the largest Muslim countries and Muhammad is one of the most common names, so you end up with countless people in Indonesia whose name is simply Muhammad. It becomes very difficult to name to match because you have no other information to go on other than the one name and possibly a date of birth.

But with millions named Muhammad globally, even having a date of birth can make this difficult. So you need to perform additional due diligence.

Another issue is names crossing between one ethnicity to another. Moe is a very common nickname for Muhammad. It can be a very common name for Italian Americans and it can be short for Moses.



Transliterations versus translations

Naming conventions vary by region: There are also many other complexities, such as surname conventions with marriage. In Western Europe and North America, many people are familiar with a person's surname being your father's last name. Additionally the standard was that when you get married a wife would adopt her husband's last name, but that tradition is changing.

That is not the standard in Spanish speaking Latin America; your last name is your father's first last name and then your mother's first last name. In most countries in Latin America, you do not change your name when you get married.

That changes when you are talking about Portuguese speaking countries. In Brazil, it is your mother's first last name followed by your father's first last name. Therefore, you have some complexities where if you have someone who is originally from Brazil, but now has moved to Columbia, it can pose some very interesting issues as those names may now be changed.

Other variations include:

- In Eritrea, Ethiopia and Iceland you have cases where you don't have a traditional last name but instead you last name is your father's first name
- In Arab world, names may be [first name] bin [father's name] [sometimes another descriptor like a family name or ancestral home]
- In Japan, China and Korea, the last name appears first. Although Japan is working to change that convention to western style in documents that appear with the Latin alphabet.
- In Mongolia, your father's first name appears first — before your first given name

You want to make sure that your software understands the most common variations, especially the most common in your jurisdictions. You will also need to be prepared to deal with more false positives as you move names around to deal with these global conventions.

Where Should Your Review Start?

1. Audit all of the lines of business for which you are responsible. This includes newly acquired or established lines of business. The chief compliance officer needs to ensure that with any acquisition of any bank or any growth of the business, that compliance is a core part of that discussion. This is not something where you want to just trust or make assumptions.
2. Identify reference data depth and breadth request information on global coverage. Does your data vendor provide truly global coverage? Are there holes in their coverage? Identify where those holes are and see if they align with your business. Do you need to supplement the data you have already?
3. Identify points of latency. How long does it take from when an account is created to when it is put into a database to be available to the compliance team? What can be done to reduce that amount of time?
4. Ensure that your reference includes sectoral and narrative sanctions and ask how that data is being kept up to date
5. Ask your vendor how they are dealing with Ultimate Beneficial Ownership (UBO) data and know how you are dealing with UBO as a financial institution. These are or soon to become regulations in many jurisdictions
6. Subscribe to regulatory intelligence updates, whether that is through the regulator or data vendor. Subscription services are usually not expensive and all of the regulatory agencies have email lists to make sure that you are staying up to date to changes in regulations, new sanction regimes, policy changes and enforcement actions. Review these every day and make sure that your teams know how to respond to any changes.
7. Work with your screening vendor to evaluate your current rule set. How are all of the filters (like date of birth) set? What does the matching percentage mean? What is and isn't being included? Make sure you understand all the configurations, thresholds and rules and do that on a regular basis.
8. Have a conversation with your vendor every year about what is working and what isn't working. Use metrics like your false positive rates, the efficiency rate of your analysts, how many profiles are reviewed per day, your false negatives during reviews as the basis for your conversations.
9. Test your screening software for name variations to identify matching holes and scoring parameters.

Summary

Many compliance teams assume their systems are configured properly. This can be a dangerous assumption and you have to consider nothing works unless you have tested it.

It is vital to update your software when your provider adds new features or vital security patches. In the world of financial crime fighting, those changes are going to come as developers work to stay ahead of the money launderers and criminals.

Personnel, data, software reporting must all be tested and audited regularly. You should set that schedule. Most institutions do this annually, but you should set a schedule that make sense for your institution.

Reference data and client data flows must be analyzed. Look for the weak points and the delays. For example, look at batch processes that are configured to run every few days when they should be run every few hours.

Screening software should be tested. Be informed about how date of birth and other attributes affect screening, how results are represented and how global name variations are matched. What are the different issues and risks associated with each?

Benchmark everything! Benchmark false positive rates by geography and line-of-business. This will allow you to see when processes are working well and not working well. It also allows you to measure changes over time as your data and software configurations change.

AML Compliance with Alessa

Alessa provides all the anti-money laundering (AML) capabilities that banks, money services businesses (MSBs), fintechs, casinos and other regulated industries need – all within one platform. Capabilities of the product include:

Customer Due Diligence: To support KYC, CDD, and EDD processes, Alessa combines data from onboarding, transaction monitoring, and other core systems with identity verification and risk intelligence data to provide updated risk profiles and scores that are based on activities and relationships.

Sanctions Screening: Alessa screens individuals and businesses against multiple lists including PEPs, negative news, OFAC, and other sanctions lists. Screening can be done in native characters and in real time, periodically or on demand.

Transaction Monitoring: Alessa can analyze every transaction in real time and, using an extensive library of analytics and scenarios, generate alerts for suspicious activities. These are sent to the appropriate personnel via text or email for investigation and/or reporting.

Regulatory Reporting: All suspicious activity alerts include data needed for regulatory reports. Once it is determined that a Suspicious Transaction Report or a Suspicious Activity Report needs to be filed, Alessa can auto-populate (and electronically file) as many as 70% of these reports. Alessa can also automate as much as 100% of CTRs.

Risk Scoring: Alessa uses data from various sources, including sanctions lists, to provide an assessment of the risks of doing business with an individual or business. The solution also periodically reviews an organization's customer base and updates their risk level based on their activity and third-party data.

Configurable: With Alessa, organizations can select the functionality they need or the complete solution. Permission-based functionality allows different users to access only the information they need to perform their responsibilities, and data can be maintained in the cloud or on-premises, ensuring compliance with regulations.

Data Management: Alessa accesses data from any platform, including ERPs, bespoke applications, and core business systems. The data is then cleansed and aggregated to increase its accuracy, and cross-referenced to reveal big-picture insights. Better data means better insights.

Investigation Tools: Alessa offers dynamic workflows to guide processes and investigations. Enterprise search capabilities allow for easy searching of data within internal and external sources, while case management offers a collaborative approach to investigations, compliance, and decision making.

Metrics & Insights: Alessa offers configurable dashboards that track key metrics and allow compliance staff to drill down into the alerts. Advanced analytics allow for sound decision-making and actions to be taken based on comprehensive information and insights.

To learn more about how Alessa can help with your AML compliance activities, visit *alessa.caseware.com*

About CaseWare RCM

CaseWare RCM Inc. is the maker of Alessa, a financial crime detection, prevention and management solution. With deployments in more than 20 countries in banking, insurance, fintech, gaming, manufacturing, retail and more, Alessa is the only platform organizations need to identify high-risk activities and stay ahead of compliance. To learn more about how Alessa can help your organization ensure compliance, detect complex fraud schemes, and prevent waste, abuse and misuse, visit us at www.caseware.com/alessa.

150 Isabella Street, Suite 800,
Ottawa, ON K1S 1V7, Canada

1-844-265-2508

alessa@caseware.com

www.caseware.com/alessa

alessa