



WHITE PAPER: SANCTIONS SCREENING

How to reduce false positives in client and transaction screening

BY

Luca Primerano
Chief Strategy Officer, Napier

Nick Portalski
Chief Product Officer, Napier

ABSTRACT

The process of screening customers, vendors and transaction data against politically exposed persons and sanctioned entities is a critical regulatory requirement.

Financial institutions and corporations face increased scrutiny to ensure adequate due diligence is conducted on customers and vendors. Failure to comply has resulted in fines that have been averaging \$20.4m in the US over the last few years.

Some of the key challenges relating to compliance and screening processes include the significant amount of manual work caused by legacy systems that are not always able to screen efficiently.

In this white paper we explain the most common challenges and pitfalls of screening processes, and discuss how the application of the latest technologies, including artificial intelligence and big data, increases process efficiency and effectiveness.

Contents

Managing sanctions risk.....	5
Current challenges in sanctions risk management.....	14
How to approach sanctions screening.....	25
Introducing Napier.....	30
Introducing Napier's AI Advisor.....	33
About Napier.....	35

KEY CONCEPTS DISCUSSED

False positives in sanctions screening

False positives are alerts raised by the screening system, that after a significant amount of time and money spent investigating them, prove to be innocent. These alerts could be for customers, suppliers, employees or transactions.

As well as being costly to process, false positives in sanctions screening are an obstacle for compliance departments because they divert analysts' focus and time away from investigating higher risk cases.

False negatives in sanctions screening

These are customers, suppliers, employees and transactions that should be flagged as alerts by the screening system but remain undetected. This is often due to an inadequate system and the sophisticated skillset of those playing the system deliberately to remain under the radar.

Managing sanctions risk

Sanctions are economic and/or political measures that aim to influence the behaviour of a regime, group or individual. They are created by international, regional and state bodies and can change regularly.

From travel bans and asset freezes, to import/export restrictions, sanctions help protect national security, financial and national services, as well as a country's economy.

Sanctions are typically against particular foreign countries and regimes, terrorists, international narcotics traffickers and those engaged in activities relating to the proliferation of weapons of mass destruction, as well as other threats.¹ They prohibit transactions and, in some cases, any financial services, with a person or organisation (known as the target).²

1 U.S. Department of the Treasury. 2021. Office of Foreign Assets Control - Sanctions Programs and Information. <https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information>

2 Financial Conduct Authority. 2018. Financial Sanctions. <https://www.fca.org.uk/firms/financial-crime/financial-sanctions>

Principles of sanctions screening

The basic principle of sanctions screening itself is fairly simple: compare all data relating to the customer, supplier, employee or transaction with the data contained in external sanctions lists, such as those from the Office of Foreign Assets Control (OFAC), The United Nations, or the Office of Financial Sanctions Implementation (OFSI).

To mitigate risk, sanctions screening should be conducted not only at the beginning of a new relationship with a party, but on a daily basis and when dealing with transactions that include an external party (for example, transaction screening).

Organisations screen against a variety of lists. Some are lists of Politically Exposed People, others are 'risk lists' or 'watchlists' that contain people or entities that may be of interest to an organisation for various reasons, such as disqualified directors or people found guilty of a crime. For the purposes of this document, 'sanctions lists' is used as a term for all list types.

Chinese sanctions

Q1 2021 saw a coordinated effort by the European Union, UK, US and Canada to impose sanctions, including travel bans and asset freezes, on officials in China over human rights abuses against Uyghur Muslims.³ China immediately responded by imposing its own sanctions. In May 2021 the European parliament voted overwhelmingly to "freeze" any consideration of a massive investment deal with China, following the tit-for-tat sanctions.⁴ Most recently, China has moved forward with a law aimed at countering sanctions imposed by foreign governments.⁵

3 BBC News. March 2021. Uighurs: Western countries sanction China over rights abuses. <https://www.bbc.co.uk/news/world-europe-56487162>

4 The Guardian. May 2021. EU Parliament 'freezes' China trade deal over sanctions. <https://www.theguardian.com/world/2021/may/20/eu-parliament-freezes-china-trade-deal-over-sanctions>

5 Bloomberg. June 2021. China moves forward with law aimed at countering US sanctions. <https://www.bloomberg.com/news/articles/2021-06-08/china-moves-forward-with-law-aimed-at-counter-u-s-sanctions>

Figure 1 below outlines the basic screening process.

Every step within this process raises challenges and risks, which need managing and mitigating with meticulous sanctions, risk governance and due diligence.

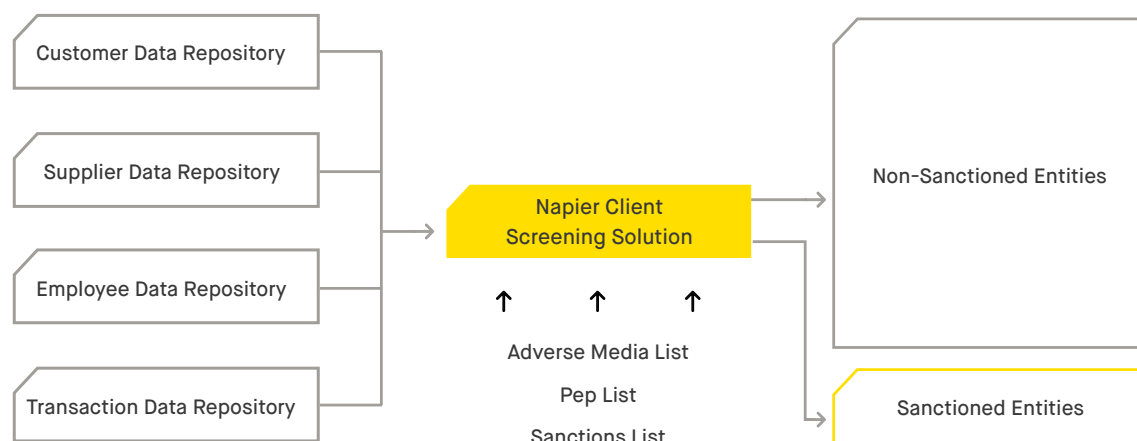


Figure 1: The basic sanctions screening process

“To mitigate risk, sanctions screening should be conducted not only at the beginning of a new relationship but on a daily basis.”



Sanctions risk governance

Robust sanctions risk governance must be an integral part of every organisation's screening process. This includes:

1 Definition of business risk appetite

For example, is the business happy to work with individuals in a potentially sanctioned country? What flags does the business want to monitor to ensure sanctions risk is minimised for the organisation? What matching terms is the business comfortable using? See pages 15 -16 for more information on matching terms.

2 Definition of sanctions risk management policies


Sanctions risk management policies should ensure adequate risk management. For example:

a. Definition of risk tier per country

This is based on how risky it is to do business with that country, or based on other factors, such as political unrest.

b. Definition of the type of lists to be checked

There are thousands of lists available to help organisations perform effective risk management and regulatory compliance. These may be international sanctions lists (such as OFACs) or watchlists such as lists of politically exposed individuals and their relatives, the FBI's Most Wanted or HMRC's Disqualified Directors. Used effectively and appropriately these allow organisations to ensure appropriate controls are in place. For example,



a medical company may screen business counterparties to ensure they are not involved in inappropriate dealing of medical equipment.

Different lists will be used by different parts of the business as appropriate to the risk appetite defined.

c. Definition of the types of controls to be used in sanctions screening:

- i. Will each customer, vendor and employee be checked against all sanctions lists available, or only subsets based on customer specificities, for example?
- ii. Will manual reviews be used to address hits that are similar matches to individuals (for example, to account for spelling mistakes)?
- iii. Will companies that have been checked in another geographical location be included?

3 Definition of sanctions risk management responsibilities

Define the internal department that will be responsible for sanctions risk management and the operating model (such as roles and responsibilities in the team, procedures required to perform screening processes, escalation processes, operational controls, etc).



Sanctions risk due diligence

While there are globally defined standards for performing sanctions screening and due diligence, every company implements different variations according to their business strategy and risk appetite.

Sanctions risk management must be case specific with a structured approach. What's more, due diligence is a continuing obligation demanding a robust, methodological approach to ensure compliance, even when regulations or individuals change.⁶

In the UK, the view of the Office of Financial Sanctions Implementation (OFSI) is that: *"Financial sanctions are generally widely publicised and that businesses, particularly those operating internationally, will have reasonable cause to suspect that sanctions might be relevant to them. Therefore, they won't be able to avoid liability simply by failing to consider their sanctions risks."*⁷

OFSI expects all businesses who engage in activities where financial sanctions apply to stay up to date with the sanctions regimes in force, and to not only consider the likely sanctions exposure risk, but to take appropriate steps to mitigate those risks.

To add to the complexity, in any single scenario there may be several layers of sanctions. This is because sanctions may be created by multiple bodies, including those from the UN, EU, UK, US, Canada and Australia.

6 Norton Rose Fulbright. 2015. Sanctions FAQs. <https://www.nortonrosefulbright.com/en-gb/knowledge/publications/9106cdb9/sanctions-faqs>

7 Gov.uk. 2018. Reporting information to OFSI – what to do. <https://www.gov.uk/guidance/suspected-breach-of-financial-Sanctions-what-to-do>

The cost of sanctions breaches

While specific compliance requirements vary depending on where you are in the world, compliance is mandatory for all affected individuals and legal entities. Breaches are a criminal offence and can lead to fines and even imprisonment.

In the UK, the OFSI's latest guidance, Monetary Penalties for Breaches of Financial Sanctions is considered to be a significant change; it signals the regulator's strengthening determination to use its full powers to ensure compliance.⁸

Breaches of financial sanctions can lead to the following penalties (UK):⁹

Deferred Prosecution Agreements (DPAs)

Court-approved agreements between an organisation and a prosecutor who is considering prosecuting the organisation for an offence.

Serious Crime Prevention Orders (SCPOs)

Imposed by a court on the civil standard of proof. Designed to prevent an individual or organisation from further engaging in serious crime.

Custodial sentences

Offences relating to UK financial sanctions carry a maximum of seven years' imprisonment on indictment (applying to all of the UK) and, on summary conviction, a maximum of six months' imprisonment in England and Wales, 12 months in Scotland and six months in Northern Ireland.

⁸ Pinsent Masons. 2021. OFSI to get tougher on non-compliance with UK Sanctions. <https://www.pinsentmasons.com/out-law/news/ofsi-tougher-non-compliance-uk-Sanctions>

⁹ Office of Financial Sanctions Implementation. 2020. UK Financial Sanctions: General Guidance (December 2020). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/961516/General_Guidance_-_UK_Financial_Sanctions.pdf

Monetary penalties

Under the powers in the Policing and Crime Act 2017, the value of a monetary penalty may range from up to £1 million, to the greater of £1 million or 50% of the estimated value of the funds or resources. The final penalty depends on breach or failure. In the US, sanctions violation can lead to civil and criminal penalties that exceed several million dollars.

Overleaf is a graph (Figure 2) which looks at the OFAC fines in the US between 2009 and 2020.

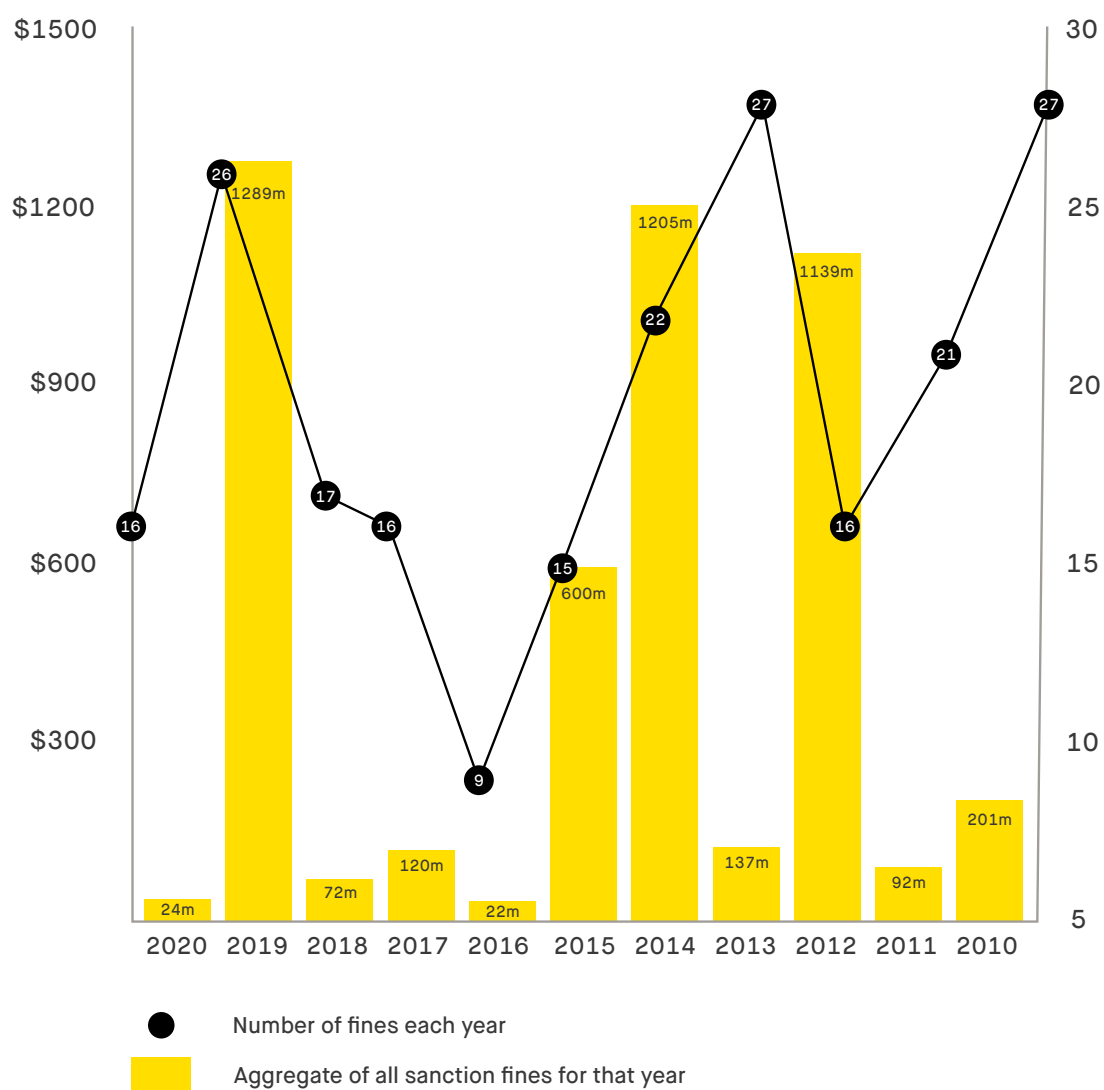


Figure 2: OFAC fines 2009-2020

The aggregate number of fines varies widely each year with no established or reliable trend. Notably, the value of the fines is also expansive, with the smallest fine being \$5,000 (2020) and the largest a staggering \$963,619,900 (2014).

<https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information/2020-enforcement-information>

Current challenges in sanctions risk management

Anti-money laundering and anti-corruption systems and controls can be integrated with sanctions compliance systems. But in order to do so, there are important differences in terms of the lists and specific prohibitions that need to be considered.¹⁰

The Financial Conduct Authority (FCA) advises that sanctions screening controls may need to be different to those for anti-money laundering purposes because sanctions compliance requires consideration of to whom payments are being made, and whether funds are from a legitimate source.¹¹

What's more, the process of screening customers, suppliers, employees and transactions against sanctions lists is fraught with challenges.

¹⁰ Office of Financial Sanctions Implementation, HM Treasury. 2020. UK financial sanctions: general guidance. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/961516/General_Guidance_-_UK_Financial_Sanctions.pdf

¹¹ Financial Conduct Authority. 2018. Financial Sanctions. <https://www.fca.org.uk/firms/financial-crime/financial-sanctions>

These challenges are driven by:

- Identity similarities
- Spelling mistakes and typos
- Data capture mistakes
- Poor data collection and organisation
- External data inconsistencies in format, datasets and geographical coverage, making direct and reliable comparisons challenging
- Poor and insufficient data
- Inadequate/legacy screening systems and technology, such as those that are slow at performing matches, inflexible and difficult to configure, which leads to manual intervention and risk of error
- Criminal efforts to purposely undermine and derail the effectiveness of the screening process, such as false identities and frequent changes of address

Despite these challenges, sanctions screening systems and controls must mitigate the risk of financial crime and meet financial sanctions obligations.

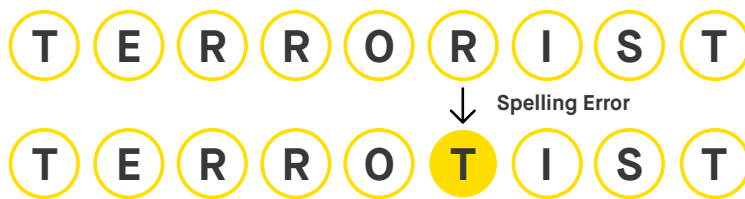
In a bid to improve the effectiveness of sanctions screening, we now look at the role of defining matching terms and the root causes of false positives.

One of the most critical points in managing sanctions risk is defining a terms matching strategy and policy that describes how the process of matching a business party against a sanctioned party should look.

Defining matching terms

Spelling errors and name variations are amongst the most common causes of false positives and false negatives. **A robust matching strategy and combination of different matching algorithms is therefore critical to minimising false positives and false negatives.** Matching terms are important for taking into account simple spelling errors and word variations, so that potential targets are not automatically counted or discounted.

The example below looks at word similarity and helps explain some of the key challenges:

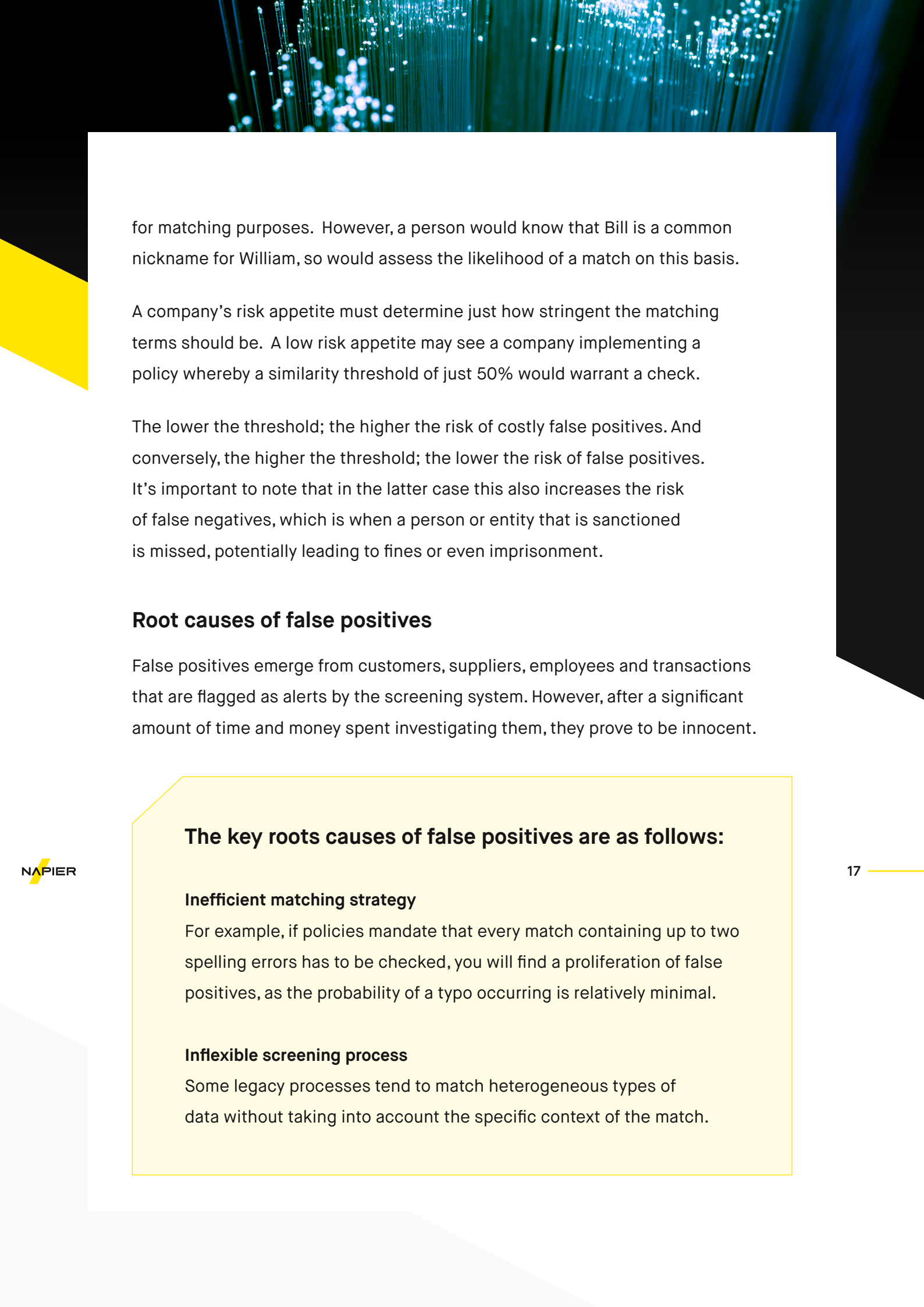


In this nine character word, eight characters are the same: they are 89% similar. If, during the screening process, the similarity threshold is set to 89%, then in the instances of nine character words, only those with one incorrect character would generate a red flag. However, should a higher threshold of 90% be set, the single spelling mistake and possible match would not be recognised, and so generate a possible false negative.

Another example that highlights the complexity of establishing matching algorithms is the task of matching shorter words, such as John versus Jon. These words are only 75% similar,¹² yet they should be regarded as a match due to the phonetic similarity of the words, and the fact that Jon is often spelled as John. Bill and William are only 43% similar,¹³ which is well below most thresholds

¹² Based on the Levenshtein distance

¹³ Based on the Levenshtein distance



for matching purposes. However, a person would know that Bill is a common nickname for William, so would assess the likelihood of a match on this basis.

A company's risk appetite must determine just how stringent the matching terms should be. A low risk appetite may see a company implementing a policy whereby a similarity threshold of just 50% would warrant a check.

The lower the threshold; the higher the risk of costly false positives. And conversely, the higher the threshold; the lower the risk of false positives. It's important to note that in the latter case this also increases the risk of false negatives, which is when a person or entity that is sanctioned is missed, potentially leading to fines or even imprisonment.

Root causes of false positives

False positives emerge from customers, suppliers, employees and transactions that are flagged as alerts by the screening system. However, after a significant amount of time and money spent investigating them, they prove to be innocent.

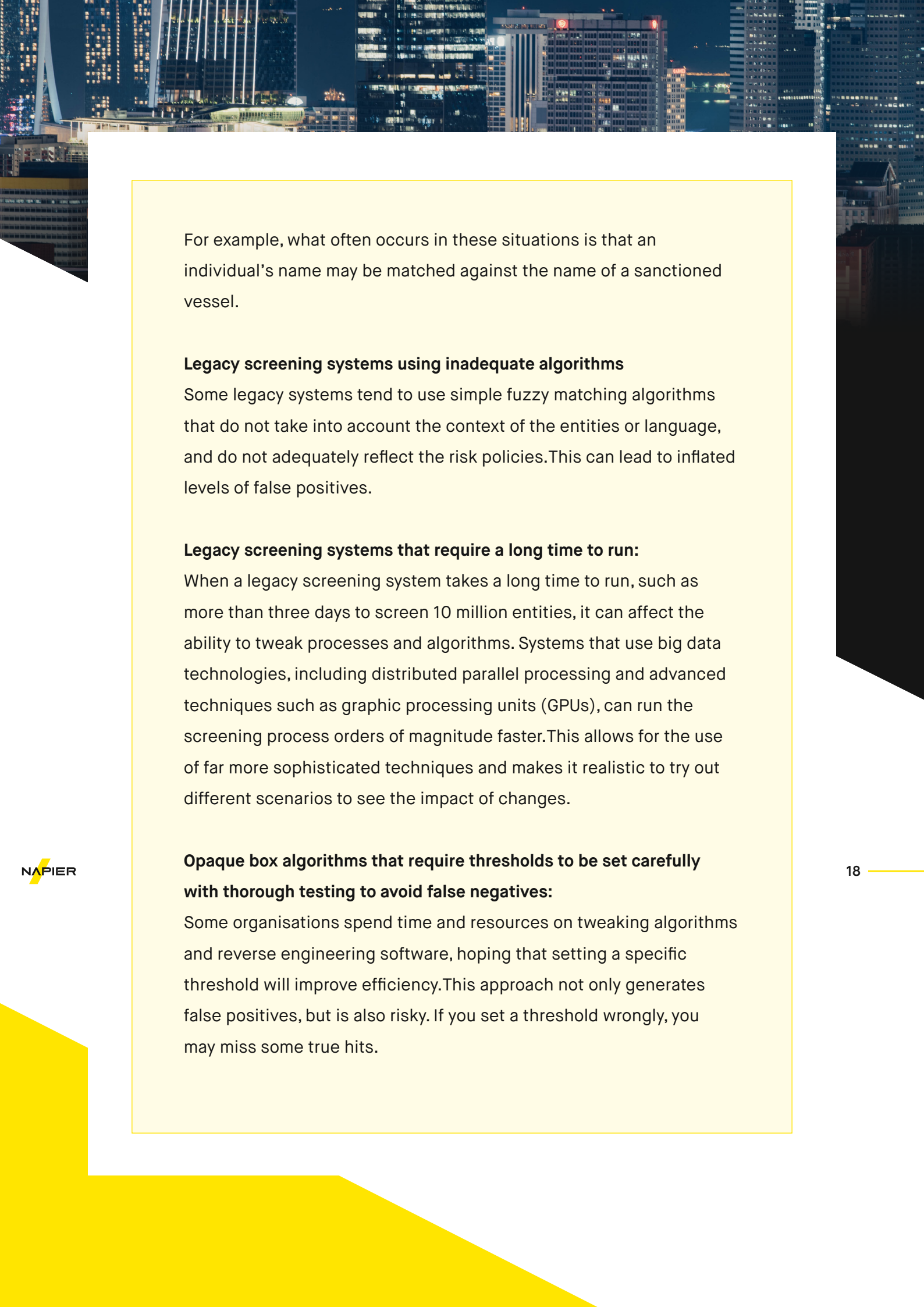
The key roots causes of false positives are as follows:

Inefficient matching strategy

For example, if policies mandate that every match containing up to two spelling errors has to be checked, you will find a proliferation of false positives, as the probability of a typo occurring is relatively minimal.

Inflexible screening process

Some legacy processes tend to match heterogeneous types of data without taking into account the specific context of the match.



For example, what often occurs in these situations is that an individual's name may be matched against the name of a sanctioned vessel.

Legacy screening systems using inadequate algorithms

Some legacy systems tend to use simple fuzzy matching algorithms that do not take into account the context of the entities or language, and do not adequately reflect the risk policies. This can lead to inflated levels of false positives.

Legacy screening systems that require a long time to run:

When a legacy screening system takes a long time to run, such as more than three days to screen 10 million entities, it can affect the ability to tweak processes and algorithms. Systems that use big data technologies, including distributed parallel processing and advanced techniques such as graphic processing units (GPUs), can run the screening process orders of magnitude faster. This allows for the use of far more sophisticated techniques and makes it realistic to try out different scenarios to see the impact of changes.

Opaque box algorithms that require thresholds to be set carefully with thorough testing to avoid false negatives:

Some organisations spend time and resources on tweaking algorithms and reverse engineering software, hoping that setting a specific threshold will improve efficiency. This approach not only generates false positives, but is also risky. If you set a threshold wrongly, you may miss some true hits.

Legacy screening solutions that lack the ability to enhance matching results by leveraging additional data:

Leveraging additional data is an important part of sanction screening. For example, you may be able to exclude entities from a list of suspects by leveraging the date of birth of an individual, their passport number or by checking the picture provided during the know your customer (KYC) process with the picture provided by screening

False positives divert analysts' focus and time away from investigating higher risk cases.



Examples of false positives

01

Matching companies that contain similar data.

For example Test123 Services Limited vs Toast12 Services Limited. The legacy system thinks the two entities are similar due to 'Services' and 'Limited' being present in both names. However, the only key term for matching is 'Test123' vs 'Toast12', which are significantly different.

02

Matching individuals without considering the order of names.

For example, matching John Richard Smith with Richard John Smith when you know with certainty that Richard and John are the middle names.

03

Matching two companies that appear to be similar.

Such as matching Test Medical Equipment Facilities Limited and ABCD Medical Equipment Facilities Limited. While these two names are 88% similar and there are just four letters of difference, in reality these two companies are completely different.

As well as potentially very damaging and costly (see Figure 2, page 13), false positives in sanctions screening are an obstacle for compliance departments because they drive analysts' focus and time away from investigating higher risk cases.

Commonly used words cause false positives

Commonly used words can cause false positives without due consideration for context and relevance. Below is a summary of the most common words in 2020 company registrations. A sophisticated screening process would decrease the importance of these words when matching company names.

Rank	Word	Uses	Percent
1	UK	7140	2.5653%
2	Property	6670	2.3965%
3	Group	6164	2.2147%
4	Solutions	5764	2.0710%
5	Holdings	4821	1.7321%
6	Management	4403	1.5820%
7	Company	3875	1.3923%
8	Home	3096	1.1124%
9	Bar	2409	0.8655%
10	Design	2387	0.8576%
11	London	2382	0.8558%
12	Health	2221	0.7980%
13	Global	2049	0.7362%
14	Food	2007	0.7211%
15	Media	1769	0.6356%
16	Trade	1467	0.5271%
17	Auto	1437	0.5163%
18	Business	1327	0.4768%
19	Fit	1296	0.4656%
20	Digital	1247	0.4480%

Figure 3: Most common words in 2020 company registrations

Source: Tide. 2020. Company naming trends: what should you call your company in 2020? <https://www.tide.co/blog/tide-update/company-naming-trends/>

The problem with legacy sanctions screening systems

Legacy sanctions screening systems are outdated in terms of technology, standards and processes. For example, systems solely built on relational databases do not lend themselves well to the performance and scalability requirements that a modern screening solution requires.

Legacy systems often lack integration with modern enterprise search tools for fast random access and do not have suitable databases for storing large amounts of unstructured data.

Table 1 below compares how some of the most common sanctions screening system features vary between legacy and modern systems.

	Legacy System	Modern System
01 CONFIGURABILITY OF RULES AND SCENARIOS	Often based on a static threshold using one metric (e.g. names that are 75% similar)	Combines multiple metrics to cater for different types of matches and context
02 ABILITY TO DERIVE SCENARIOS FROM RISK POLICIES	Requires multiple manual adjustments to configuration parameters (e.g. tweaking a static threshold) in order to match the company risk policy	Policies can be defined in the system upfront and are mapped directly to the customer risk policies
03 TESTING OF SCREENING PROCESS IN SANDBOX	Non-scalable technology resulting in extremely slow test runs (e.g. screening ten million names in a test environment may take up to three days)	Ability to run multiple tests in segregated sandbox environments in hours
04 FILTERS	Ability to filter terms using manually defined whitelists	Ability to run context related analytics to dynamically weight the significance of words in matching legal entity names
05 REFERENCE DATA	Leverages limited amount of data from a single external provider (e.g. OFAC list including list of sanctioned individuals)	Uses diverse datasets from multiple providers to reduce false positives and increase accuracy (e.g. uses photo identity, address data, date of birth and links to news articles etc to verify identity)

Table 1: Legacy vs modern screening systems

The impact of legacy systems and processes

The true cost of legacy sanctions screening systems and processes is hidden in unnecessarily high levels of false positives and false negatives.

1 High levels of costly false positives

False positives are false matches, which must be dealt with by teams of analysts, performing the same checks repeatedly. The average false positives rate can reach up to 5-8% in legacy systems. This means that if one million entities are screened, 50,000 to 80,000 will need to be manually reviewed. What's more, with an average number of 5-8 hits per entity, for every one million entities there can be up to 400,000 hits to manually review.

If each false positive has to be documented with an explanation as to why it is a false positive, and that it takes between 30 seconds and one minute to review a false positive, the cost of false positives per million customers or transactions could exceed £200,000.

The true cost of legacy sanctions screening systems and processes is hidden in unnecessarily high levels of false positives and false negatives.

2 High levels of costly false negatives

False negatives can ultimately lead to sanctions violation. In the US, the average sanctions breach fine between 2018 and 2020 was \$20.4m. The enormity of this average is largely owing to substantial fines levied upon UniCredit Bank and Standard Chartered Bank in 2019.¹⁴

¹⁴ U.S. Department of the Treasury. 2021. Basic Information on OFAC and Sanctions: FAQs. <https://home.treasury.gov/policy-issues/financial-Sanctions/faqs/topic/1501>

The cost of false positives

When you have a proliferation of false positives it becomes a drain on resources, time and money.



30 SECONDS TO 1 MINUTE TO REVIEW EACH FALSE POSITIVE

5-8%

AVERAGE FALSE POSITIVE RATE FOR EVERY MILLION ENTITIES SCREENED

50K-80K

THE NUMBER OF TRANSACTIONS MANUALLY REVIEWED PER ONE MILLION ENTITIES SCREENED

**circa
200,000**

POTENTIAL COST PER MILLION CUSTOMERS/ TRANSACTIONS SCREENED BASED ON THE NUMBER OF TRANSACTIONS AND THE TIME TAKEN TO MANUALLY REVIEW EACH ONE

The cost of false negatives

Failing to report anomalies as a result of false negatives creeping into analysis reports can result in monetary penalties as evidenced by figures from OFAC and OFSI.

THE AMOUNT PAID IN A SINGLE FINE IN 2014

<https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information>

\$963,619,900

AGGREGATE NUMBER OF PENALTIES IMPOSED BY OFAC FROM 2018-2020

49

AVERAGE PENALTY IMPOSED BY OFAC FROM 2018-2020

\$20.4m

LARGEST PENALTY IMPOSED BY OFSI (2020)

<https://www.gov.uk/government/collections/enforcement-of-financial-sanctions>

£20.5m

How to approach sanctions screening

The overriding aim in sanctions screening must be to correctly identify sanctions risk within customers, suppliers, employees and transactions to minimise false positives and false negatives.

This section outlines the basic principles of an effective sanctions screening process:

1. Capture data in a clear, structured way

With so much data to be processed and analysed, it's essential systems capture data in a clear, structured way. This means, for example, gathering title, first, second, and last names in different fields. Not only does this avoid any potential ambiguity, but it becomes easier to match against data in an external sanctions/data list.

With careful data capture design, the risk of a data capture error should be minimised, such as inserting a first name into a surname field.

An example of structured data from the OFSI is outlined in Table 2 overleaf.

Heading	Description
Name 6	The last name of the individual / the full name of the entity
Name 1	The first name of the individual
Name 2	The second name of the individual
Name 3	The third name of the individual
Name 4	The fourth name of the individual
Name 5	The fifth name of the individual
Title	Honorary, professional or religious title
DOB	Date of birth (in dd/mm/yyyy format)
Town of birth	Town of birth, including alternatives
Country of birth	Country of birth including alternatives
Nationality	The citizenship and/or nationality of the individual
Passport details	Passport number(s) - where issued, issued/expiry dates
NI number	National identification numbers e.g. ID card numbers, Social Security Numbers etc.
Position	Official title/position
Address 1	The first line of the address i.e. where the individual permanently or temporarily resides/ lives (legally or illegally). For entities this could include where that entity has branches.
Address 2	The second line of the address
Address 3	The third line of the address
Address 4	The fourth line of the address
Address 5	The fifth line of the address - normally the town
Address 6	The sixth line of the address - normally the town, state or region
Post/zip code	Any known postal identifying codes
Country	The country where the address is
Other Information	Supplementary data in addition to that in the above categories. This could include gender, nicknames, low quality single name aliases, UN reference number, details of family etc
Group type	Individual or entity
Alias type	Prime alias, AKA (also known as) or FKA (formerly known as)
Regime	Title of the Financial Sanctions regime under which the target is listed
Listed on	The date the target was added to the Consolidated List by the Treasury (previously the Bank of England) i.e. the publication date of the relevant notification, notice and/or news release
Last updated	The date that the identifying details of the target were last changed on the Consolidated List by the Treasury
Group ID	The unique identifying code given to all records/data permutations relating to a specific individual or entity

Table 2: OFSI consolidated list format guide¹⁵

¹⁵ OFSI. 2018. Consolidated list format guide. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/292095/fin_sanc_consolidated_list_format_guide.pdf

2. Use as much data as possible

The more relevant data you have for verification, the lower the risk of false positives and false negatives occurring.

Of course, data is not always available and the desire of criminals and terrorists to remain undetected will be high. This drives tactics like changes of name and moving from one country to another, in an attempt to remain under the radar.

3. Improve matching algorithms

You should use different matching algorithms that account for different cases. These should be weighted based on the scenario and contribute to the overarching score that determines the sanctions risk.

For example, for a company name a higher importance can often be placed on the first name in comparison to the other names, which are often more common and less relevant when it comes to matching. Consider, for example, Test123 Management Consulting Limited and Test360 Management Consulting Limited.

The ability to calculate average scoring and standard deviation is also beneficial as it may give important information on whether different approaches “agree” in considering whether an alert is a false positive or a true hit.

In order to reduce false positives and false negatives, care should be taken when combining matching algorithms and configuring them based on language, scenarios and company policies. High order correlations between scores are also problematic because they are difficult to detect without using advanced analytics.

Algorithm examples

Both of the algorithms below measure the edit distance between two sequences (words) which quantifies how different two names are.

Damerau–Levenshtein distance

Measures the minimum number of operations required to change one word into the other. Operations consist of deletions, insertions or substitutions of a single character, or transposition of two adjacent characters.

According to Frederick J. Damerau, these four operations correspond to more than 80% of all human misspellings when considering only misspellings that could be corrected with at most one edit operation.¹⁶

Jaro–Winkler distance

Measures the minimum number of single-character transpositions required to change one word into the other. By using a prefix scale it gives more favourable ratings to strings that match from the beginning for a set prefix length.¹⁷

4. Continuously improve your screening process

Reviewing the output of your screening process, including reviewing hits and false positives, may help improve the rules and scenarios that have been configured in your system, or potentially help you improve the policies you are adopting.

¹⁶ Wikipedia. 2021. Damerau-Levenshtein. https://en.wikipedia.org/wiki/Damerau-Levenshtein_distance

¹⁷ Wikipedia. 2021. Jaro-Winkler Distance. https://en.wikipedia.org/wiki/Jaro-Winkler_distance



5. Use whitelists to your advantage

The opposite of blacklists, whitelists can be used to support sanctions compliance efforts by identifying and saving repetitive matches that materialised as a false positive.

Whitelists can help reduce the occurrence and cost of false positives but can increase the risk of false negatives. In the case of a sanctions breach, it can be difficult to satisfactorily explain to regulators why further investigations weren't made. Whitelists should therefore be used with caution, and only as a means of supplementing screening processes.

6. Use alternative scoring

Using traditional distance-based scoring alone can lead to excessive levels of false positives because thresholds are set manually. Using alternative scoring in addition to distance-based scoring, however, can complement and enhance the screening process, leading to more reliable results. For example, machine learning generated classification scores can take into account different dimensions within a match, such as average length of words, average similarity score, and maximum similarity score.

Introducing Napier

Napier offers a complete and comprehensive customer, supplier, employee and transaction screening solutions that combines the latest technology to minimise the incidence of false positives in the sanctions screening process by more than 90%.

Napier's screening solutions can augment the capabilities of a legacy system by deploying its components on top of the existing system. This allows companies to significantly and cost-effectively improve the screening process in their current workflow with minimal system integration effort.

Napier implements a four-phase approach to enhance the efficiency and effectiveness of the screening process by optimising data context.

These steps are outlined in Figure 4 below:

Napier Context Optimisation

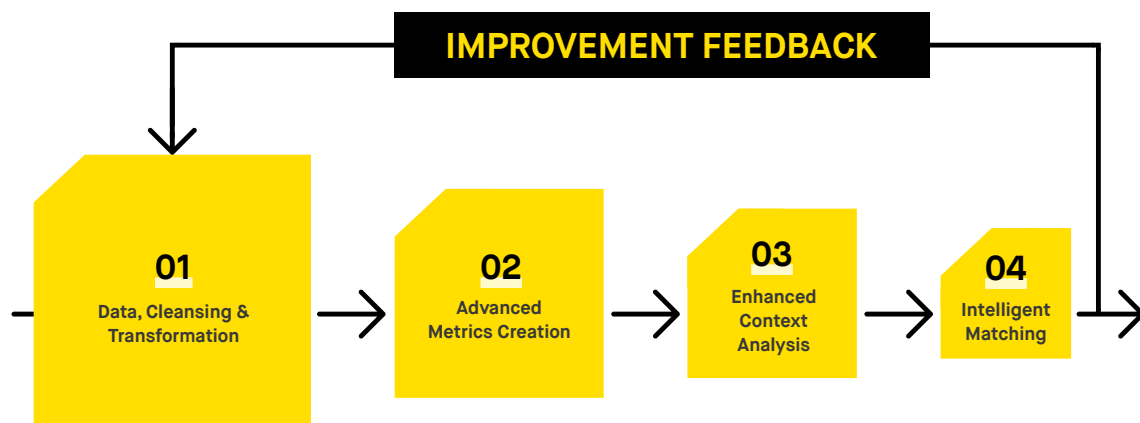


Figure 4: Napier context optimisation engine



Stage 1

Data cleansing and transformation

Data stored in original data repositories, such as transactional systems and customer record systems, are ingested and processed by the system. This can be achieved using connects for specific systems, leveraging file transfers or by using an application programming interface (API). The system can also ingest already processed alerts and potential hits, aiming at using these as inputs in its false positive reduction process.

Once the data is ingested, it is then transformed and cleansed with initial filters applied based on the input type. For example, duplicates may be removed, and data may be enriched and normalised.

Stage 2

Advanced metrics creation

Metrics are generated based on data type. For example, a set of distance metrics is generated between the client name and the client in a sanctions list. Initial thresholds are set based on current policies and risk appetite and can be configured by the client, such as acceptable spelling errors in a match. Features are then created to describe statistics of input data.

Stage 3

Enhanced context analysis

Input data is analysed in detail to weight terms based on context. For example, the engine assesses the weight of each term in a company name.

In comparing the legal entities below, although the majority of the characters and words are similar, it is clear they are two different companies:

- Legal entity 1: Fortytwo Management Services and Partners
- Legal entity 2: Paper Management Services and Partners

Therefore, the context and relevance of each term is considered when performing a match.

Stage 4

Intelligent matching

Multiple techniques including policy application, rules and disparate scores are applied to the input data, leveraging initial thresholds and labels. The most relevant matches are presented for review with a detailed explanation for the reason the system is suggesting a review.

The discounted entities are not presented to the user, however, a detailed description explaining the reason for the dismissal is provided.

The Napier screening solution provides a natural language explanation for the reasons why matches have been discounted, including a link to policies and reference data used to automate the discount decision. This can be used to help justify the decision to the regulator, improve policies, and support data sampling.

Introducing Napier's AI Advisor and additional functionality

Napier's screening solution offers the following added functionality, including smarter false positive reduction with its unique AI Advisor feature:

- **Napier's AI Advisor** is an optional feature within Napier's screening solutions that helps analysts review alerts faster, by identifying the false positives in screening. By using machine learning to analyse screening outcomes and improve match scoring, it can determine if the match should be discounted or requires further review.

AI Advisor works alongside a rules-based approach: rules determine the screening matches, and AI Advisor determines how good the match was, and if the match warrants further investigation.

It does this by scoring each match, showing the components that contributed to the score in a clear visual on the screening dashboard to help analysts make quick decisions about the quality of the match. AI Advisor also provides an explanation alongside the score to help analysts understand the key factors in its decision. This helps users understand why a match was created and what was unusual about it.

The additional insights from AI Advisor, which analyses multiple additional variables to score a match, can help reduce false positives further by up to 40%.

- **Creates additional rules** to match specific scenarios, such as matching on nicknames, name variations and the use of phonetic variances for specific languages. Importantly, a trade-off must be found between allowing for all name variations in all languages and focusing on the key ones.
- **Adds additional features** to the data to increase the likelihood of accurate matching. For example, by automatically deriving the gender of individuals from their given names using machine learning techniques. Another example is the use of machine learning to assess face similarity by comparing images gathered at onboarding with images from the sanction list provider.
- **Implements a workflow** to continuously improve the screening process, by leveraging analyst feedback in automatically classifying matches as correct or incorrect.

A background image of a London skyline at sunset, featuring prominent skyscrapers like The Shard and the Gherkin.


About Napier

Napier is a London-based specialist compliance technology company founded in 2015 with offices in North America, Singapore, Australia, Ukraine, and Malaysia.

Trusted by the world's leading financial institutions, our next generation Intelligent Compliance Platform is transforming AML & Trade Compliance.

We design and build compliance technology to help companies in any sector comply with money laundering regulations, detect suspicious transactions, screen potential customer & business partners and help analysts predict customer behaviour.

Napier uses deep industry knowledge and cutting-edge technologies such as artificial intelligence and machine learning to help businesses detect suspicious behaviours and fight financial crime.



Discover how Napier can transform your compliance processes

Learn more about how Napier can transform your screening processes at www.napier.ai where you can book a demo or contact us.

Email us

Book a demo



NAPIER.AI