SEON

seon.io

GUIDE

Your Guide to Effective Sanctions Screening

Contents

Your Guide to Effective Sanctions Screening

The sanctions screening process is a requirement for financial bodies and other regulated industries, and will be part of a greater KYC program. Implementation of a strong sanctions screening protocol is a commitment from that entity to do their due diligence when it comes to preventing money laundering, terrorism, and other financial crimes.

Depending on applicable national jurisdictions, there are hundreds of different sanctions lists maintained by various governing bodies that must be observed. Failure to do so in an effective way can result in punishments that vary in severity – but all of which represent a huge risk for the success of ongoing business operations.

Many governing bodies are aware of the challenges that developing an airtight Financial Crime Compliance (FCC) program entails, citing both the ever-expanding sanctions lists themselves, as well as the financial mechanisms in place to hide ultimate beneficial ownership. However, with the right resources, this is a challenge that all businesses can be adequately prepared for. Here's how.

Why Is Sanctions Screening Important?

For businesses in regulated verticals like money services and real estate, the importance of an effective sanctions screening process is twofold: being part of the effort against terrorism and international money laundering, and minimizing risk from noncompliance punishments.

In the case of the former, the benefits of not being a part of criminal or terrorist money laundering should be self-evident. The potential for reputational damage is extremely severe if, for example, a legacy bank was publicized as being instrumental in processing funds that end up in the hands of the Russian war effort.

In terms of direct impact on a company's bottom line, the risk of noncompliance punishments looms much larger. In 2022 alone, two of the major international arbiters of sanctions regulations, the Financial Conduct Authority (FCA) in the UK and the Office of Foreign Assets Control (OFAC) in the US, handed out over $266 million and

$42 million in fines respectively to offenders.
These fines, however, can be just the tip of the legal iceberg. Severe and repeat offenders who maintain business contacts with sanctioned entities risk becoming sanctioned entities themselves – the worst-case scenario for any business.

The importance of a strong FCC or Sanctions Compliance Program (SCP) is thus directly tied to the importance of business operations. Developing a business model that does not incorporate such a program – with capabilities commensurate to the mandated requirements – may result in either crippling fines or, potentially, the ceasing of all business operations.

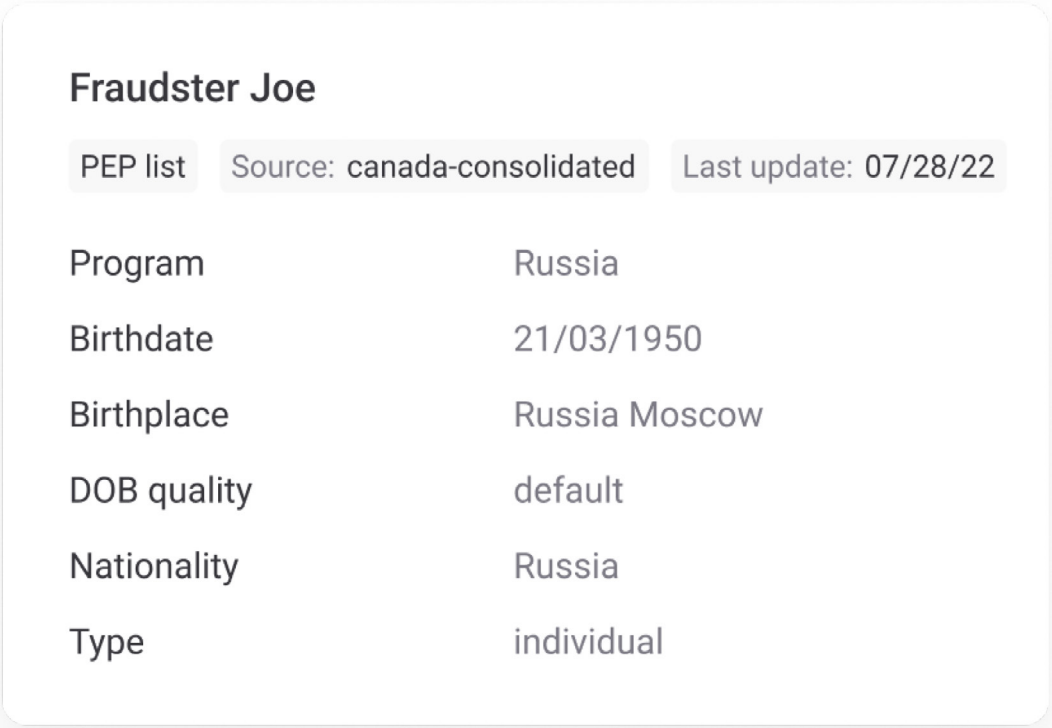
What Is the Sanctions Screening Process?

The sanctions screening process will generally be part of a risk-based due diligence and financial compliance program. Though there are small differences in sanctions regulations from country to country, they tend to align to better facilitate the international business machine.

In general, an effective sanctions screening process will include:

- the confirmation of customer identity at onboarding, likely established over the course of KYC requirements
- the cross-checking of that confirmed identity against all relevant lists, including
    - sanctions
    - politically exposed persons
    - adverse media coverage
    - crime lists
    - watchlists
    - other jurisdiction-specific lists
- the manual double-checking of any confirmed “hits” on relevant lists, to avoid false positives owing to name similarities
- the suspension of all transactions for confirmed sanctions list matches, and the reporting of the match to the internal designated compliance officer

- the labeling of high-risk customers per the results of those cross-checks, and the continuous monitoring of those high-risk individuals
- monitoring customers at the transactional level to ensure that sanctioned entities are not being included in the process
- a comprehensive internal auditing process that generates verifiable documentation of all the protocols put in place, and how they were executed



In this screenshot, an example of the results of SEON's AML lookups can be seen, with an test profile being scrutinized. Note that it shows the lists that register "hits", and includes the option to toggle continuous monitoring.

Troubleshooting the Process

There are some notable pitfalls that occur within this process, which any strong compliance program should address. Employees monitoring for sanctions screening compliance should be aware of:

- their applicable jurisdictions and the specificities of local mandates
- complexities arising from different international languages, writing systems,

and naming conventions

- the necessity of good data labeling and hygiene to accurately cross-reference lists
- the tendency for entities on sanctions lists to complicate, obfuscate, layer, and otherwise make their business ownerships difficult to ascertain
- the nature of sanctions lists to always be adding names that companies need to screen for
- the possibility of retroactive enforcement of sanctions mandates, wherein a customer or transaction that was previously considered safe is now sanctioned, leaving the company that handled the transaction liable
- the concepts of OFAC's 50 percent rule to determine ultimate beneficial ownership
- the possibility that an entity may be "sanctioned by association"

Governing bodies that require businesses to adhere to these points are, broadly speaking, aware of the difficulty in covering all these bases.

Determining, for example, all the entities that are "sanctioned by association" may include sanctioning any number of unnamed entities that appear in a video uploaded by a terrorist organization.

Pursuing that confirmation is both a requirement and often a practical impossibility. In this sense, maintaining a detailed audit trail that shows a satisfactory amount of research was completed is often as much as possible, and should serve as a protection against the most stringent punishments.

What Is Sanctions Screening in AML?

In anti-money laundering practices, sanctions screening consists of cross-checking valid customer onboarding data against numerous sanctions lists and other watchlists. The collection of personal data that is cross-referenced with the sanctions lists is part of meeting KYC requirements..

The majority of these companies will be in the financial sector, monitoring account opening and transactional behavior for signs of suspicious activity.

New sectors are being folded into this group all the time, as regulators identify more

verticals that sanctioned entities are leaning on to launder illicit funds. These include high-end real estate, art dealerships, investment companies, cryptocurrency operators, and building societies.

PEP Screening

Based on individual companies' respective risk appetites, lists of politically exposed persons should factor into a strong sanctions screening process. Keep in mind that, due to their proximity to the name on the PEP list, the relatives and close associates (RCAs) of the name on the list are also subject to the same requirements.

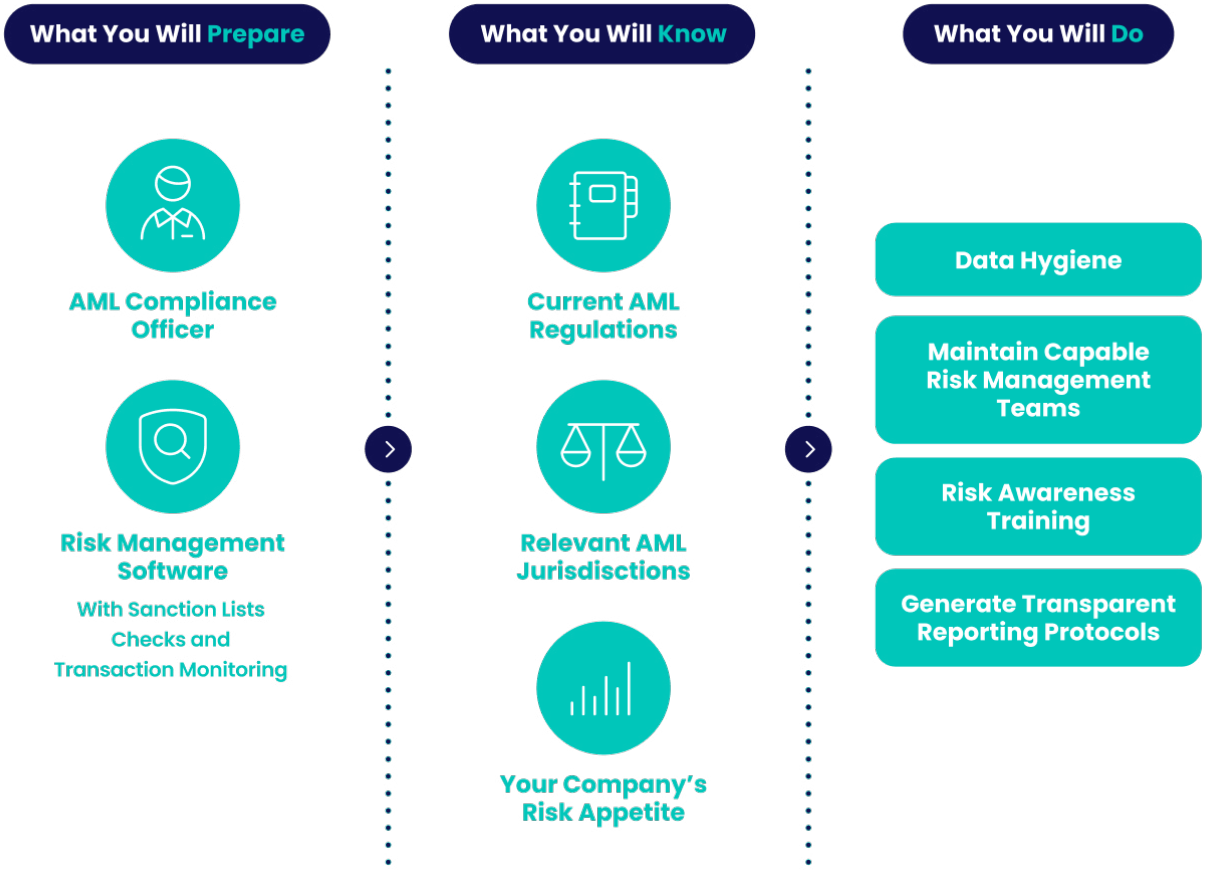
Individuals named on the PEP list are usually in a position that makes them likely to be targeted by bribes, coercion, and blackmail, and include entities like world leaders and their families, as well as people with adverse media coverage.

In many cases, businesses may want the custom of individuals on PEP lists. However, customers that constitute a high risk require more costly Enhanced Due Diligence checks, and best AML practice also suggests that they are consistently monitored, to ensure that high-risk individuals' transactions do not go from ordinary to suspicious.

How to Perform Effective Sanctions Screening

Developing and executing a sanctions screening process that minimizes risk from crime, fraud, and AML noncompliance is a multi-layered task that calls on resources from across the corporate infrastructure.

To build such a process from the ground up, there will be certain pieces to have in play, particular knowledge that should be at hand, and protocol-oriented workflows that should be adhered to.



What You Will Bring to the Table

To design a consistent AML-compliant sanctions screening process, these are the components which must be determined to set the table:

- A designated **AML compliance officer** whose duties include maintaining this process, educating relevant staff members, as well as reportage of any incidents to higher authorities. The responsibility to ensure customers and partners are being assessed for their risk falls upwards to this person. This role is mandated by AML legislation.
- An anti-money laundering software solution – likely part of a greater platform of risk management software – that performs checks of all relevant lists, measures the risk associated with each connection, monitors transactions, and generates reports or audit trails.

What You Will Already Know

As with most of the risks associated with digitized business, knowledge and awareness are key parts of a working sanctions screening process. To implement efficiency and efficacy in that process, these things need to be known:

- Specifically **what risks fall under the organization's AML responsibility**. This includes what sanctions lists need to be checked – international businesses will certainly want to comply with US, EU, and UK requirements in addition to any local ones.
- The most **recent changes in AML regulations** should always be kept on top of. The thresholds of what is considered criminal or sanctionable change regularly, and companies must retroactively comply, per official legislation. In other words, if an entity whose transactions were previously under the sanctions radar is now sanctioned, the company that handled those transactions is now guilty of facilitating them, and is strongly encouraged to self-report this fact.
- Your company's individual **risk appetite** should be carefully defined. This will inform automated risk-screening procedures in terms of what new users and transactions are allowed to proceed, as well as how closely those touchpoints are monitored.

How You Will Proceed

With the right components and knowledge readily available, you can implement the protocols that make use of them. Workflows for every contingency associated with sanctions screening should be designed and carefully executed, and should include:

- Maintaining **data hygiene**, including a strong data-labeling process. To keep the screening process accurate, streams of information from across the organization should be centrally organized to develop data-enriched customer or partner profiles. Centralized data helps remove inconsistencies in how organizations use that data, and facilitates the most accurate risk assessment, with fewer false positives and false negatives.
- **Regular training sessions** for relevant members of staff. Even teams outside of risk management and compliance should be aware of what constitutes a potential AML or sanctions violation. Staff ought to know the current legal guidelines of what a suspicious, reportable AML transaction looks like,

including the potential for insider threat and whistleblowing procedures for reporting it.

- **Risk management teams** should be adept at using whatever risk management software is in place. Most importantly, having efficient workflows in place for conducting manual reviews of potential list "hits" is essential. Being able to interpret enriched data in user profiles is a requirement. Teams should be able to easily adjust AML transaction monitoring rules, including implementing regular or continuous monitoring where necessary.
- Transparent and **verifiable reporting protocols** should be put in place for when manual reviews return a positive match against sanctions lists. This should include a paper trail of the process, which should then be turned over to the AML compliance officer to initiate the report to relevant governing bodies.

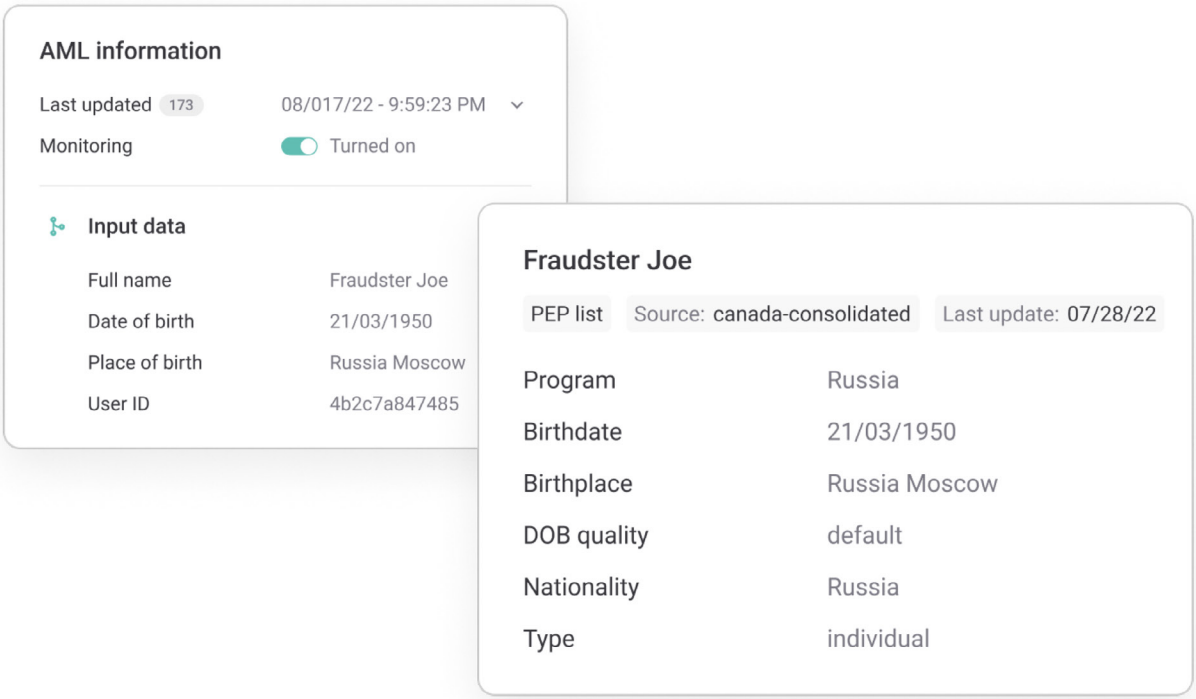
By addressing each of these points, organizations which need to be AML compliant should be able to design a procedure that minimizes noncompliance risk.

Legislators are aware that some sanctioned entities are much harder to identify than others, but having a transparent process in place similar to the above framework should be enough to verify that maximum due diligence has been carried out – a strong paper shield to wave at the possibility of fines or worse.

How SEON Facilitates the Sanctions Screening Process

The SEON software suite is a perfect tool to help compliance teams ensure their sanctions screening processes are AML compliant.

SEON addresses these needs by providing a constantly-updated portfolio of sanctions lists and other watchlists. In the process of adhering to KYC and Enhanced Due Diligence mandates, gathering customer names and addresses, SEON can automatically flag potential "hits" for manual review. SEON's low-friction data enrichment process provides a deep profile of those possible hits, to assist the reviewing team member in identifying the user as a match, or not.



In case a user is on a sanctions list, SEON can generate rich data on both their identity and their history with your organization, to assist with reporting. Moreover, the individual can be put on a blacklist, whitelist, or custom list that determines how they are able – or unable – to proceed inside the infrastructure.

At the transaction level, SEON's behavioral monitoring can be set to detect potentially risky transactional behavior based on your company's risk appetite, including the risk of incurring legal punishment. Particularly for those users determined to be high-risk, the platform enables you to perform regular, close monitoring, if you choose to continue your relationship.

Unfortunately, the nature of an optimized sanctions screening process means that no software can be deployed to automatically bring your company into AML compliance.

SEON, however, can help companies ensure their risk exposure is minimized, both in terms of avoiding fines and legal complications as well as keeping criminals and fraudsters from denting reputations and bottom lines.

FAQ

What are sanctions in AML?

Within anti-money laundering mandates, sanctions are restrictions imposed upon entities that are meant to prohibit that entity from furthering their agenda through business. These entities generally have been determined to be malicious or otherwise detrimental – for instance, members of terrorist groups and warmongers.

Who should be screened for sanctions?

For companies that fall within the AML perimeter, all new users should be screened against all relevant sanctions lists during the onboarding process. Existing users determined to be risky should also have their transactions monitored for involvement with sanctioned entities, as well as for suspicious behavior associated with corruption.

Who needs to do sanctions screening?

Depending on the jurisdiction, including any country business is being conducted, certain verticals need to do sanctions screening as part of a valid KYC process. Regulated verticals typically include financial institutions, building societies and other money services, gambling institutions, and in some cases high-end retail like art dealers and real estate services.

Sources:

https://www.fca.org.uk/news/news-stories/2022-fines

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

SEON

Easy fraud detection
for every business

Try for free

seon.io info@seon.io +44 20 3997 6090 SEON Technologies Ltd.