The Comprehensive Guide to Sanctions Screening

Take Control of your Sanctions Process
# Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What are sanctions and sanctions screening?</td>
<td>3</td>
</tr>
<tr>
<td>Navigating Sanction Demands</td>
<td>3</td>
</tr>
<tr>
<td><strong>The Sanctioning Bodies</strong></td>
<td>4</td>
</tr>
<tr>
<td>United States (OFAC)</td>
<td>4</td>
</tr>
<tr>
<td>United Nations</td>
<td>5</td>
</tr>
<tr>
<td>The European Union</td>
<td>6</td>
</tr>
<tr>
<td>United Kingdom (OFSI)</td>
<td>7</td>
</tr>
<tr>
<td>What are PEPs and RCAs and why do they matter?</td>
<td>9</td>
</tr>
<tr>
<td>Understanding the Role of RCAs</td>
<td>10</td>
</tr>
<tr>
<td><strong>What does sanctions screening mean in practice?</strong></td>
<td>11</td>
</tr>
<tr>
<td>When should sanctions screening take place?</td>
<td>11</td>
</tr>
<tr>
<td>What happens when sanctions screening fails?</td>
<td>12</td>
</tr>
<tr>
<td>Common Problems when doing Sanctions Screening</td>
<td>13</td>
</tr>
<tr>
<td>Which companies need to screen for sanctions?</td>
<td>13</td>
</tr>
<tr>
<td>What to Look for in a Sanctions Screening Tool</td>
<td>14</td>
</tr>
<tr>
<td>The Political Landscape for Sanctions Screening</td>
<td>14</td>
</tr>
</tbody>
</table>
Sanctions are a political instrument deployed by states or political institutions to compel other nations to change their behavior. While sport and cultural bans create a diplomatic “feel-bad factor” they do not otherwise disrupt the functioning of the targeted regime – this is the purpose of economic sanctions.

The effectiveness and even the morality of economic sanctions is a matter of some disagreement but that is beside the point for the financial and other institutions that are mandated by law to enforce them. Failing to do so can have serious consequences: HSBC was fined $1.3bn by US regulators for conducting transactions on behalf of customers in Cuba, Iran, Libya, Sudan and Myanmar. More recently Standard Chartered was fined $25m by UK authorities for providing loans to a Turkish bank owned by Sberbank, an entity subject to sanctions in the wake of the Russian occupation of Crimea.

The Sberbank infraction illustrates the challenges of sanctions screening, because institutions or individuals attempting to evade sanctions will exploit the complexity and interconnectedness of the global financial system to do so.

This is not the only difficulty. Sanctions are issued by different states and bodies, and in most cases do not prohibit all economic engagement with a nation state. It is not illegal to trade with Russia, but certain activities – and individuals – are banned. The granularity of sanctions makes compliance much more difficult.

Navigating Sanction Demands

The purpose of this guide is to make it easier for banks and other institutions to navigate the challenges of sanctions screening. We propose to do this by describing the sanctions landscape: the sanctioning bodies, the nature and extent of sanctions, how sanctions monitoring needs to extend beyond the individuals explicitly sanctioned, and which businesses must screen for sanctions.

What are sanctions and sanctions screening?

The Comprehensive Guide to Sanctions Screening
The Sanctioning Bodies

United States (OFAC)

The Office of Foreign Assets Control (OFAC) is the dominant sanctioning body for two reasons: the power of the US dollar and the political cohesion of the United States.

Virtually all dollar transactions clear through the United States, drawing the trade into OFAC’s punitive orbit. In 2021, the US reached a $1,016,000 settlement with an Indonesian paper products manufacturer that had been paid in dollars for the export of cigarette paper to North Korea because the wire transfers for the shipments had been cleared in the US. In its Enforcement Release, the US Treasury Department comments drily: “This case further highlights the risks to non-U.S. persons who involve the U.S. financial system in commercial activity with an OFAC-sanctioned country, region, or person.”

Using currency exchange (FX) businesses to “sidestep” the dollar does not work. The Union de Banques Arabes et Françaises tried this trick by processing transactions for sanctioned Syrian financial institutions.
on its own books, and then settling its currency accounts through US-cleared FX transactions with third party banks. The Union de Banques Arabes et Françaises agreed to settle the apparent violations for $8,572,500.

The ultimate penalty of flouting OFAC sanctions and not settling is loss of access to the US dollar – and no financial institution can afford to risk that.

In May 2022, the former CEO of Twitter and digital currency evangelist Jack Dorsey tweeted: “When did the dollar lose global reserve currency status?” Answer: it never did – nor are there any real threats to dollar hegemony. The euro project is riven with political division, and China – America’s main economic rival – protects the yuan behind a Great Wall of state protection and regulation.

OFAC sanctions reach far and wide. Rogue nations such as North Korea and Iran are locked out of the global financial system because of US sanctions; other targeted states include Venezuela, Cuba, Syria, and of course Russia.

The US sanctions regime against Russia is detailed and extensive. The first presidential order, Blocking Property of Certain Persons Contributing to the Situation in Ukraine, was signed in the aftermath of the annexation of Crimea in 2014. A raft of subsequent Ukraine-related sanctions was extended in February 2022 by the creation of “a new national emergency” to push back against the threats posed by specified harmful foreign activities of the Russian Federation, including its efforts to undermine the conduct of free and fair democratic elections and democratic institutions in the United States.

These are Washington’s geopolitical concerns and anxieties, yet they impose a burden of compliance on financial institutions the world over. But the United States is not the only nation concerned with sanctioning entities.

**United Nations**

The United Nations Security Council has the legitimacy under international law to station peacekeeping forces in zones of conflict but it also imposes economic sanctions that, in the words of its charter, “focus on supporting political settlement of conflicts, nuclear non-proliferation, and counter-terrorism”.

Its room for maneuver is limited because nations with a permanent seat on the Security Council have the power of veto. In February 2022, days after its tanks had rolled into Ukraine, Russia vetoed a UN resolution condemning its invasion – with China abstaining. This meant the legal grounds for imposing UN sanctions were never there.

The Security Council is currently imposing and monitoring 14 sanction regimes. Of these, the most extensive is directed against the activities of ISIL.
and Al Qaida. Other trade embargoes, travel restrictions and economic sanctions target entities and individuals in South Sudan, Libya, the Central African Republic and others. The Security Council has sanctions in place against North Korea but these are much more limited in scope than OFAC sanctions.

UN sanctions are binding on member states, but it can only exert diplomatic pressure to secure enforcement. However, other intergovernmental bodies are less hampered in implementing sanctions regimes.

**The European Union**

Almost half of European Union sanctions are enactments of Security Council resolutions, and for 10 sanction regimes, Brussels imposes additional restrictions – for instance, against Iran, North Korea, ISIL, and Al-Qaida. The EU imposes 25 autonomous regimes of “restrictive
Enforcement is the Achilles heel of EU sanctions policy because there is no coherent structure to do that; it falls on individual member states to identify breaches and impose penalties.

While most member states categorize sanctions violation as a crime, in Estonia and Slovakia they are considered an administrative offence. Fourteen states provide for the possibility of sanctions violations being categorized either as criminal or administrative offences, depending on their gravity.

Financial penalties vary wildly; in Austria, the maximum fine for individuals is €1.8m but in Belgium it is €25,000. The EU suffers from a lack of regulatory harmonization in this respect that makes it difficult for businesses to fully understand the level of risk they may be exposed to.

There are other cracks. The agreement to expel Russia from the SWIFT system of international settlements was not made in Brussels, but the exclusion of the banks that handle Russia’s energy exports – Gazprombank and Sberbank, the country’s largest lender – reflected EU political realities and divisions.

The EU is moving swiftly to impose uniformity in the way its sanctions are upheld. The Commission is proposing to make violations of its sanction regimes a crime across all member states. It is also drafting a directive on asset recovery and confiscation.

The invasion of Ukraine in February 2022 marks a turning point in European geopolitics, and this is reflected in the determination with which Brussels is strengthening its policy of restrictive measures. There is pressure on banks to step up their transaction monitoring to screen for sanctions breaches, as the list of blocked entities and activities grows. In July, the EU announced its seventh package of sanctions against Russia – and there will be more to follow.

Since the United Kingdom left the EU, an autonomous sanctions policy is now in force under the Sanctions and Anti-Money Laundering Act 2018 (SAMLA).

SAMLA transposes the policy objectives of the pre-Brexit EU sanctions regime into English law but interpretive differences between the two regimes are emerging, as well as differences in the lists of individuals, groups and entities that are subject to asset freezes.

Perhaps the most significant divergence so far is the abolition of the “necessity” test under EU law enabling the UK to impose sanctions where there are “reasonable grounds to suspect” that a person has been involved in a specified activity. This...
means that there is now a lower threshold for adopting sanctions than under EU law.

For financial and other institutions tasked with sanctions screening, Brexit meant they had to parse and consult another list of sanctioned entities and individuals — adding yet more strands to the compliance workflow.

OFAC, European Union, and UK sanctioned individuals and entities overlap of course, but they never mirror each other and this is where the challenge lies.

The UK body responsible for the enforcement of SAMLA sanctions is the Office of Financial Sanctions Implementation (OFSI) which, similar to the OFAC model, resides under the Treasury. Its Consolidated List of Financial Sanctions Targets in the UK names thousands of entities and individuals. For Afghanistan, there are five entities and 135 individuals. The list for Russia is much longer with 158 entities and 1,331 individuals.

The level of detail is staggering: name (in Cyrillic and Latin script for Russian individuals), address, date of birth, nationality, passport number (if available), telephone number (if available), (political) position, and a brief outline of the reasons for the sanction. For one individual, Oleksandr Yanukovych, the list gives 80 alternative names/spellings. Why is Yanukovych a blocked entity? It is worth quoting the Consolidated List:

“Oleksandr Yanukovych is the beneficiary owner of companies which conduct business in the separatist regions of the Donbas... He also met and negotiated business with a separatist group in the Donbas on at least one occasion.”

Source: UK Government

This single entry, out of thousands on the list, shows the importance of the UK and other sanction regimes being upheld — and also the level of control and granularity that is necessary to achieve that.

Another element of granular information that is vital to have insights into is whether the individual is a Politically Exposed Person (PEPs) or Relatives and Close Associates (RCAs). Having knowledge of these individuals is essential to any sanctions screening program as their positions of power have the potential for them to be more closely connected to money laundering than ordinary people.
Many of the individuals subject to OFAC, European Union and UK sanctions are men and women in prominent positions, such as heads of state, ministers, or members of parliament. The intergovernmental watchdog that combats money laundering and terrorist finance, the Financial Action Task Force (FATF), identifies Politically Exposed Persons (PEPs) as a discrete risk category, and defines them as follow in its guidance:

PEPs are exposed to risk, and this makes them “risky”, but this should not automatically shut them out of the global financial system, as FATF points out these are preventative measures only. They shouldn’t stigmatize PEPs as being involved in criminal activity automatically and PEPs should not be excluded from a business relationship solely due to that designation. Excluding PEPs based on their position is considered to be contrary to the letter and spirit of FATF Recommendation 12 according to its interpretive note.

As part of their risk-based approach, financial and other institutions have to “score” PEPs, usually according to three categories of risk. They are:

**High Risk PEPs**

Could include heads of state and government, active members of the government and top-ranking officials of political parties, as well as heads of the military, judiciary, law enforcement and the board of central banks.

**Medium Risk PEPs**

Could include regional government officials, ambassadors, senior officials of the military, judiciary, law enforcement and other state agencies, as well as high-ranking members of prominent religious groups.

**Low Risk PEPs**

Could include mayors and members of county, city and district assemblies.
These risk bands do not reflect the likelihood of a PEP laundering money or evading sanctions, but his or her access to levers of power and influence that would make it easier to do so.

Understanding the Role of RCAs

It does not end there. Relatives and Close Associates (RCAs) of PEPs are also deemed a risk and must therefore also be screened and regularly monitored. The FATF guidance casts its net wide and RCAs include family members, such as:

- Parents and children of PEPs
- Spouse or partner
- Siblings
- Aunts, uncles, and cousins
- Indirect family members, such as in-laws;
- An individual who has a close business relationship or shares in the ownership of legal entities with a PEP
- An individual who is the owner of a legal entity which is known to have been set up for the de facto benefit of a PEP

Screening for PEPs is complex because the FATF’s definition of “a prominent public function” is very broad and the cast list is clearly enormous. Financial institutions have to rely on commercial databases for their PEP screening but when such lists are incomplete, any resulting breach is the responsibility of the monitoring entity.

The UK’s Financial Conduct Authority (FCA) requires firms to use information that is “reasonably available” to them, and this includes commercial databases of PEPs, family members, and known close associates.

“You do not have to actively investigate whether beneficial owners of a client are PEPs. However, if you know that a beneficial owner is a PEP, you should consider what extra measures, if any, you need to take when dealing with that client.”

Source: The Law Society

The Comprehensive Guide to Sanctions Screening
What does sanctions screening mean in practice?

Data entry dominates huge swathes of compliance and that remains true when it comes to sanctions screening. Manual data entry into internal forms to check names one-by-one against sanctions lists or batch screening by uploading a CSV file to check names in bulk is still a common form of sanctions screening.

It’s compliance via spreadsheet which relies on humans making zero errors and being able to focus on data-heavy work for hours at a time. This is simply not possible for most compliance officers and it’s an ineffective way to conduct sanctions screening.

Transactional, customer, business partner, and payments data is cross-referenced against sanctions lists to uncover any potential breaches. Again, without using a dedicated sanctions screening tool that automates this process it requires human-led data entry. Automation is far more accurate and results in higher levels of efficiency and speed. Using cutting-edge sanctions screening software, it is possible to screen data in real-time every time a payment is made or to screen in batches on a scheduled basis.

When should sanctions screening take place?

There are two vital moments when sanctions screening needs to take place, one is during customer onboarding where their details are
checked to make sure that they’re not a sanctioned entity. That’s an easy yes/no decision. The other is more complex, sanctions screening when conducting transaction monitoring to ensure that your business is not facilitating the movement of money to sanctioned entities.

It’s also known as transaction screening. This is a vital and necessary process to detect bad actors in the financial system, especially if they’re attempting to exploit your business to move illicit funds.

Sanctions screening in this way should not exist as a standalone process but needs to be combined with a thorough AML policy and a strong risk-based approach to compliance. Compliance officers should remain aware that it is not possible to screen for every sanctions risk due to the number of variables.

There is far more at play than name-matching when conducting sanctions screening, it involves compiling data from multiple technology systems and sanctions lists, which are often siloed and can have compatibility issues. That data should then be used for comparison using matching algorithms and risk-based alerts, this is especially the case when multiple jurisdictions are at play as there are multiple regulatory regimes that need to be accounted for.

False positives are a major challenge when dealing with sanctions screening. There are multiple ways to reduce these issues, using ‘good guys’ lists to manage false alerts that are identified, but that takes significant time to build and a strong understanding of your sanctions data. Automating your sanctions screening process is a more powerful and immediate way to achieve this.

What is often thought of as a simple name-matching process can be a complex set of processes in which data is transferred from several, often disparate, technology systems and sanctions lists for comparison, using matching algorithms and risk-based alert creation rules intended to ensure compliance with multiple regulatory regimes.

**What happens when sanctions screening fails?**

Failing to conduct sanctions screening can result in fatal
consequences for a business. One bank was forced to suffer a bank run after failing to properly conduct sanctions screening and OFAC withdrew the dollar from it.

But while this is a concerning fate, it is not a common one. It’s far more likely that a business will be fined and suffer significant damage to its reputation. In 2021, the Union de Banques Arabes et Françaises failed to comply with the US sanctions program in regards to Syria and was fined $8.5m as a result. This was part of a systematic series of fines for failures to comply across multiple banks, businesses, and individuals by OFAC which resulted in over $20m paid out in fines.

Under screening sees the opposite occur, where false negative rates hit unreasonable levels. Businesses that have implemented poor sanctions screening can see this occur. It often means that the business is at risk of facilitating criminal activity due to having no real controls in place or rules so narrow that they could not possibly pick up any sanctioned activity.

**Which companies need to screen for sanctions?**

The FATF list of financial institutions covers retail banks, mortgage providers, pensions funds, payment and clearance services, FX, asset management, insurance companies, wire transfer services, and others. But of course, there are other types of businesses and professions that are open to abuse from money launderers and sanction evaders. These “designated non-financial business and professions” are:

- Casinos (including online casinos)
- Real-estate agents

**Common Problems when doing Sanctions Screening**

The most common issue that businesses face when carrying out the sanctions screening part of their AML compliance program is false positives. This is a direct result of over screening, which can easily occur when implementing overly broad rules for sanctions screening and failing to have an appropriate risk-based approach in place.
• Dealers in precious metals and stones
• Lawyers, notaries, other independent legal professionals and accountants
• Trust and company service providers that act as nominee shareholder, provide registered account and/or business addresses, act as company director or secretary, or act as a formation agent of legal persons.

In the same way as financial institutions, DNFBPs must raise the alarm if they suspect a client of illegal activity.

What to Look for in a Sanctions Screening Tool

There are three key elements that should be considered with any sanctions screening solution.

1. Easily Arranged Alerts handling

Equipping your compliance teams with risk prioritization for alerts means that they can handle the highest risk factors first. By organizing and assigning alerts according to risk your compliance team is able to tackle the biggest threats to your business before moving onto smaller issues.

2. Rich Client Profiles

Information used to be everything, but to be effective your compliance team needs to have effective information management. By integrating client information with transaction data your compliance officers will no longer waste time and make unforced errors by cross-referencing data incorrectly. The relevant information will be on-screen when examining transactions.

3. Smooth Case Management Workflows

Assessments are the backbone of compliance activity. Making it possible for your compliance team to search, sort, and filter cases makes this simpler at every stage. Alerts can be assigned to specific analysts depending on their expertise and streamline the compliance workflow instead of creating administrative backlogs by requiring multiple team input when unnecessary.

The Political Landscape for Sanctions Screening

The Russian aggression in Ukraine has highlighted the urgency of sanctions as an instrument of foreign policy, and this is most keenly felt in Europe where inconsistencies in sanctions enforcement may be giving targeted
individuals and entities a way out. This is changing – and changing fast.

Financial institutions and DNFBPs are tasked with making sanctions stick, and will be fined – increasingly severely, we suspect – for failing to do so. It has long been impractical if not impossible to screen for sanctions manually by inputting a name into an online search tool for instance. “One-off” sweeps of customer databases are more effective, but only for as long as the OFAC, UN, European Union, and UK sanction regimes remain unchanged – which, in the present situation, is clearly untenable.

Best practice for identifying financial irregularities is the deployment of advanced transition monitoring technology. Such TM platforms can be extended to automate the regular screening of customer and stakeholder databases for blocked entities individuals.

Transaction monitoring can also be paired with sanction screening to monitor for illegal activity on behalf of a prohibited entity or individual. This is called “transaction screening”.

Prohibited entities and individuals exploit the complexity of the sanctions landscape and the interconnectedness of the global financial system to avoid detection, and the disruption of their activities. To thwart their efforts, financial institutions and DNFBPs need to deploy technology and automation to cut through this complexity and make sanctions an effective weapon against war and injustice.

Compliance has never mattered more.
About Fenergo

Fenergo is the leading provider of digital solutions for client lifecycle management (CLM) and digital transformation for financial institutions. Its software digitally transforms and streamlines end-to-end CLM processes - from regulatory onboarding, data integration, client and counterparty data management, client lifecycle reviews and remediation, all the way to client offboarding. Fenergo is recognized for its in-depth financial services and regulatory expertise and out-of-the-box rules engine which ensures financial institutions are future-proofed against evolving Know Your Customer (KYC), Anti-Money-Laundering (AML), Environmental, Social and Governance (ESG), tax and OTC derivatives-based regulations across 120 jurisdictions. Headquartered in Dublin, Ireland, Fenergo has offices in North America, the UK, Poland, Spain, South Africa, Asia Pacific, and the UAE.