AML Watcher

WHITEPAPER

WHY THIRD-PARTY DUE DILIGENCE IS CRUCIAL FOR SANCTIONS COMPLIANCE?

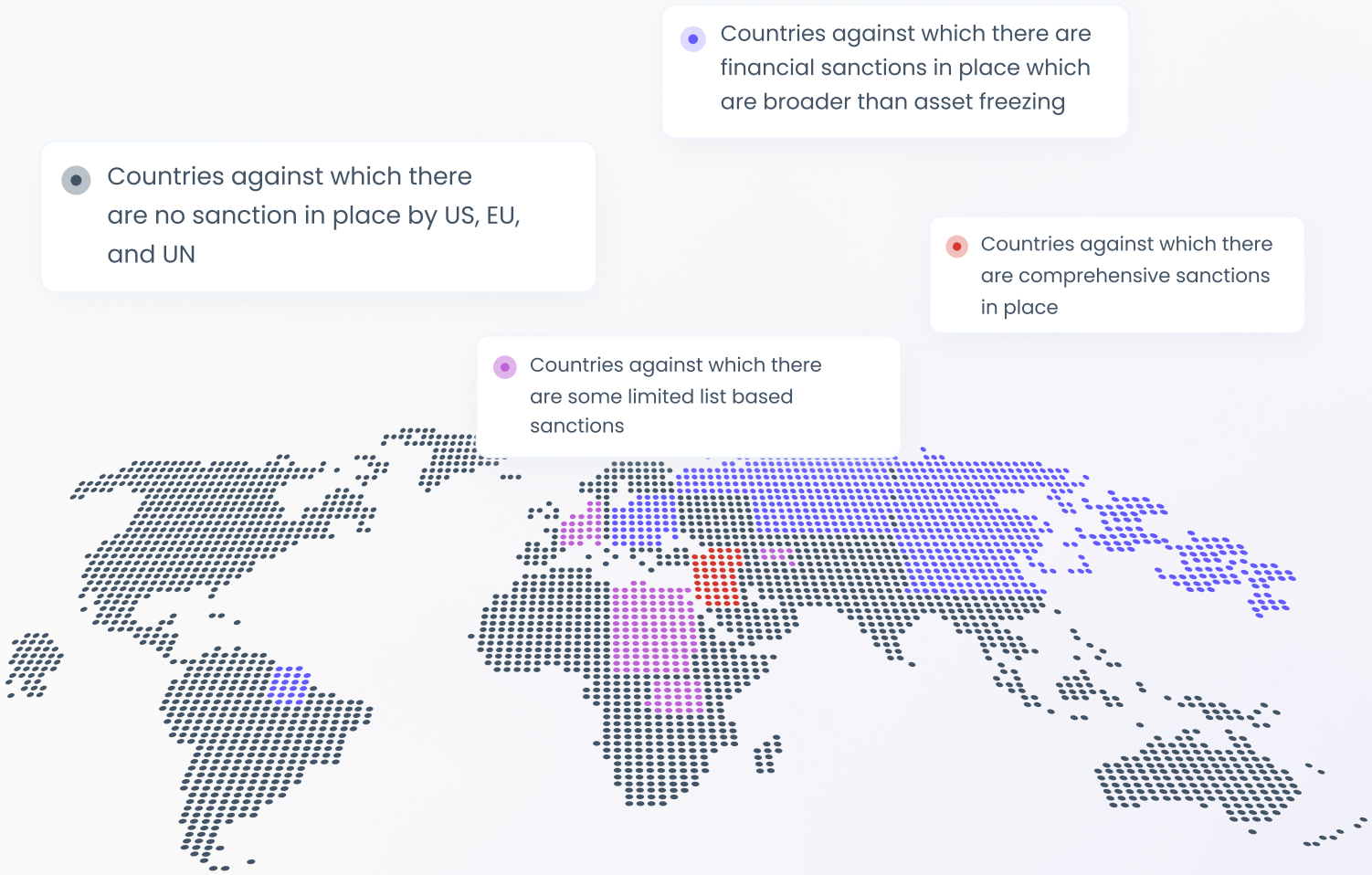
AML Watcher

Table of Content

Introduction

Recently, CNBC reported that The Netherlands is expanding its export restrictions on "advanced" semiconductor manufacturing equipment, following U.S. pressure to prevent the transfer of high-tech machines to China. The move aims to ensure that China does not gain access to advanced chip technology with potential military and AI applications, aligning with U.S. concerns about national and international security. In other words, amidst the shifting geopolitical landscape, sanctions have become an important tool making sanctions screening a critical compliance requirement for businesses.

Sanctions screening serves as a pivotal control mechanism within Financial Institutions (FIs) to both detect and mitigate the multifaceted risks associated with international sanctions. It is a linchpin of an effective Financial Crime Compliance (FCC) program, offering a strategic vantage point for the identification of sanctioned entities, individuals, and potential illicit activities that FIs may unwittingly encounter.



According to the Wolfsberg Group Report

"Sanctions screening is a control used in the detection, prevention and disruption of financial crime and, in particular, sanctions risk. It is the comparison of one string of text against another to detect similarities which would suggest a possible match. It compares data sourced from an FI's operations, such as customer and transactional records, against lists of names and other indicators of sanctioned parties or locations".

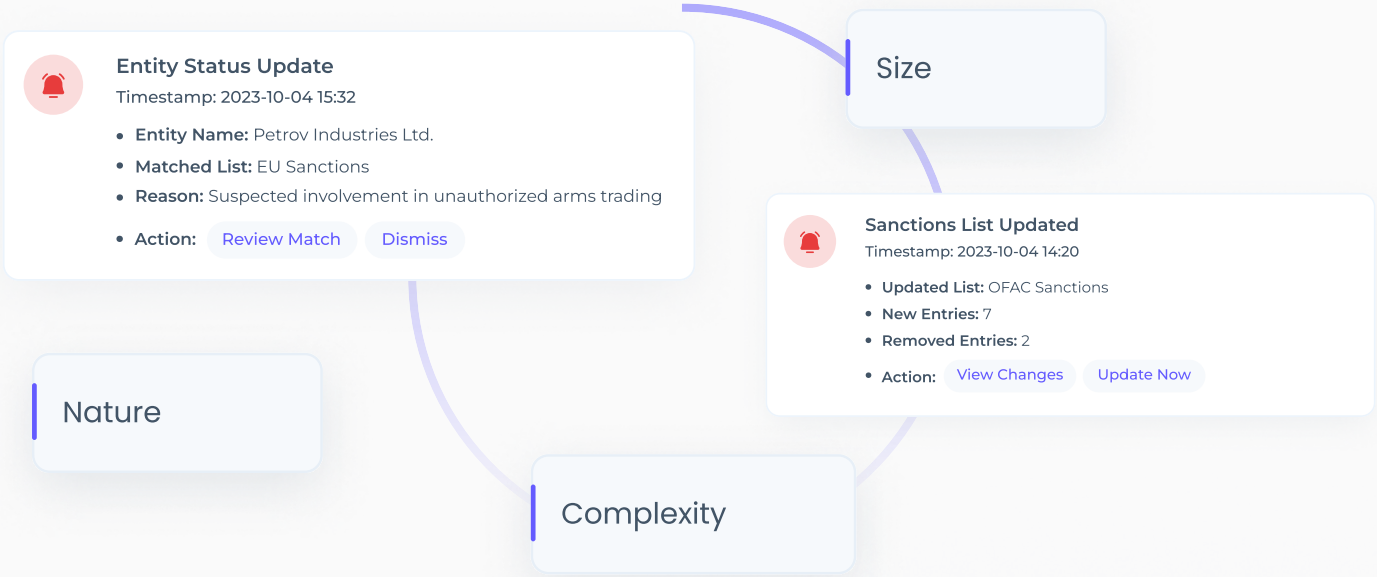
Most FIs deploy 2 screening controls:

- Transaction screening
- Customer screening.

Transaction screening is implemented to detect transactions associated with particular individuals or entities. This process aids in scrutinizing financial activities for any potential links to specific individuals or entities of interest. It plays a crucial role in enhancing the overall scrutiny and vigilance within transaction monitoring. Customer or name screening, as part of its function, is strategically crafted to identify and isolate these individuals or entities at various stages, starting from the onboarding process and extending throughout the entirety of the customer relationship lifecycle. This meticulous approach ensures a continuous and comprehensive monitoring system that remains integral to the overall risk management framework.

These screening mechanisms when combined, establish a comprehensive framework for the identification of sanctions targets. Acknowledging the inherent limitations in managing these controls is crucial, prompting the need for their seamless integration into a broader FCC program. This integration is imperative for strengthening the overall effectiveness of risk management efforts in alignment with FATF guidelines, ensuring a more resilient and adaptive approach to combating financial crime threats. The recognition of these limitations underscores the continuous evaluation and refinement required to uphold the integrity and efficacy of the sanctions identification process within the evolving landscape of financial regulations.

The FI must evaluate its exposure to sanctions risks & tailor the screening initiative according to these factors



Case Study:

Sanctions Regime in Australia

United Nations Security Council (UNSC) Sanctions:

As a member of the United Nations, Australia is obliged to enforce United Nations Security Council sanctions, often termed multilateral sanctions.
Implementation of these sanctions is facilitated through regulations governed by the Charter of the United Nations Act 1945 (Cth) (COTUNA), aligning Australia's legal framework with international obligations.

Australian Autonomous Sanctions:

Autonomous sanctions are imposed in alignment with Australia's foreign policy objectives, serving as a key tool for promoting national interests and global stability.
Implementation is carried out through the Autonomous Sanctions Regulations 2011 under the Autonomous Sanctions Act 2011 (Cth), ensuring a legal framework that facilitates the effective enforcement of Australia's autonomous sanctions measures.

RELEVANCE TO THE AUSTRALIAN BANKING INDUSTRY

Sanctions Measures

- Targeted financial sanctions, encompassing asset freezes on designated persons and entities.
- Restrictions on trade in goods and services, including 'arms or related materiel.
- Restrictions on engaging in specific commercial activities.

Applicability of Australian Sanctions Laws:

The laws apply to all activities within Australia and those undertaken by Australian citizens and registered bodies corporate abroad.
Guidelines developed for Australian Banking Association (ABA) members encompass all activities, promoting strict compliance.

CONSEQUENCES OF NON-COMPLIANCE

For Individuals and Bodies Corporate

- No requirement to prove intent, knowledge, recklessness, or negligence for guilt.
- Sanctions offenses are deemed strict liability offenses for corporate bodies.

"Compliance is viewed as an essential aspect of corporate and social responsibility, aligning with UN efforts for international peace, security, and Australian Government foreign policy"

Third-Party Due Diligence

Definition and Importance

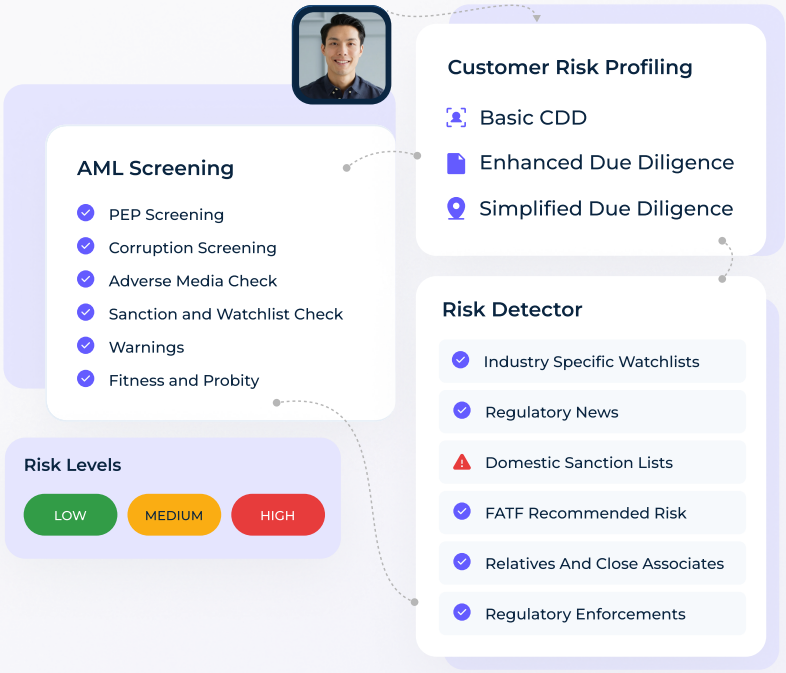
Third-party due diligence is a critical process that involves investigating and understanding one's business partners. It entails making suitable inquiries to verify the honesty and integrity of existing or prospective third parties. The fundamental objective of effective third-party due diligence is to instill confidence that agents, resellers, suppliers, and other entities engage in legitimate business transactions devoid of corruption. The goal is to confidently explain this conviction and persuade stakeholders of its validity.

Supporting Measures for Effective Implementation

For a robust third-party due diligence process, organizations should implement key supporting measures at an operational level. This includes active commitment from the top leadership, tailored training for employees and, where applicable, third parties, ongoing monitoring of the due diligence process, and the establishment of secure channels for questions and reporting of concerns. Disciplinary sanctions for non-compliance should also be clearly communicated, emphasizing the seriousness of adhering to due diligence protocols.

Methodologies for Effective Third-Party Due Diligence

A risk-based approach is paramount when conducting third-party due diligence. The extent of scrutiny required to attain reasonable confidence in engaging a bona fide third party varies with the level of corruption risk associated with the specific context. The higher the risk, the more thorough and comprehensive the due diligence should be. Risk assessment plays a pivotal role in this process, categorizing third parties into high, medium, or low risk based on various factors such as their relationship with government entities, compensation structure, and the nature of the services they provide.



Industry Implications: Sanctions List Screening and Effective Compliance

For sanctions compliance, it is imperative for businesses to rigorously screen against global sanctions lists and watch lists, particularly in jurisdictions where they operate. Notably, transactions conducted in US dollars fall within US jurisdiction, obligating compliance with US sanctions regulations. Key sanctions lists include:

United States

The Specially Designated Nationals and Blocked Persons List (SDN) from the Office of Foreign Assets Control (OFAC) takes precedence. Additionally, businesses must heed the U.S. Department of Commerce's Bureau of Industry and Security (BIS) Entity List (EL), Denied Persons List (DPL), and Unverified List (UVL).

European Union

The Consolidated List of Sanctions, maintained by the Directorate-General for Financial Stability, Financial Services, and Capital Markets Union (DG FISMA), holds paramount importance.

United Kingdom

The Consolidated List of Financial Sanctions Targets, overseen by the Office of Financial Sanctions Implementation within HM Treasury, serves as the primary reference.

Canada

The Consolidated Canadian Autonomous Sanctions List, published by the Government of Canada, is the primary focus in this jurisdiction.

Businesses should broaden screening to include the **United Nations Security Council Consolidated List** and other relevant lists. Obtain sanctions list data from official government websites or reputable providers, and stay vigilant for updates due to frequent entity additions and removals.

Sanction Circumvention: Alternate Countries, Goods, and Other Methods

These tactics are used to circumvent sanctions, particularly by leveraging alternate countries or third-party nations and substituting sanctioned goods with acceptable alternatives.

Third-Party Trade Routes and Countries:

Sanctioned entities exploit third-party nations or less regulated countries as conduits to facilitate trade with restricted regions. By rerouting transactions through intermediaries or nations not covered by sanctions, they obfuscate the origin or destination of the goods, making detection and enforcement challenging for authorities.

For instance, the reports filed under the **Bank Secrecy Act (BSA)** by FinCen and BIS provide financial intelligence, highlighting trends like significant U.S.-origin goods sent to Russia and the involvement of intermediaries in facilitating the movement of sensitive items.

Transshipment and False Documentation

Transshipment involves rerouting goods through an intermediary nation before reaching the sanctioned destination. This strategy allows sanctioned goods to be mixed with non-sanctioned products, camouflaging the true nature of the items being transported. False documentation further aids in misrepresenting the origin, nature, or intended recipients of the goods.

For instance, in October 2022, the U.S. Department of Justice unveiled a case exposing the evasion of **sanctions by six Russian and one Spanish nationals**. Accused of operating a network of shell companies, these individuals facilitated illegal exports to Russia and violated sanctions on Venezuelan oil through transshipment points in third-party countries.

Two months later, the **DOJ revealed** another case involving five Russian nationals, including a suspected Federal Security Service officer, and two U.S. citizens. Charged with violating U.S. sanctions and export controls, this group employed a global scheme of procurement and money laundering for the Russian government. In both instances, the DOJ alleges that the defendants utilized shell companies and transshipment points in third-party countries to subvert sanctions.

1. “Financial Trend Analysis, September 2023.” FinCEN, https://www.fincen.gov/sites/default/files/shared/FTA_Russian_Export_Controls_FINAL_508.pdf. Accessed 15 December 2023.

Trade Misinvoicing and Underreporting

Entities manipulate invoice values, quantity, or descriptions to disguise sanctioned goods. This involves undervaluing or underreporting sanctioned items or falsely categorizing them as permissible goods, thus evading scrutiny during customs inspections.

For instance, in 2015, Global Financial Integrity (GFI) highlighted that trade misinvoicing led to approximately US **$800 billion** in outflows from developing countries, particularly affecting Africa. Subsequent estimations reveal that, in recent years, trade misinvoicing constitutes two-thirds of the total illicit financial flows, ranging from US$600 billion to US$900 billion, underscoring its significant role in facilitating illicit activities, including potential sanction circumvention through misinvoicing and under-reporting.

Use of Cryptocurrencies and Digital Platforms:

The advent of cryptocurrencies and digital platforms offers new avenues for evading sanctions. Sanctioned entities utilize these technologies for financial transactions, bypassing traditional banking systems and detection mechanisms.

For instance, FinCEN issued an alert in 2022 highlighting the potential role of cryptocurrencies in evading extensive U.S. sanctions imposed on Russia and Belarus in the aftermath of the Russian invasion of Ukraine. Financial institutions, especially those involved in convertible virtual currency transactions, were urged to stay vigilant. While large-scale government-level sanctions evasion using CVC may have posed challenges, the alert emphasized the risk of sanctioned individuals, illicit actors, and networks utilizing CVC and anonymizing tools to bypass U.S. sanctions and safeguard their global assets.

Case Study:

Evasion of Russian Export Controls

In light of escalating geopolitical tensions involving the Russo-Ukraine war, many countries have implemented sanctions against Russia. For instance, the UK enforces sanctions against Russia, as mandated by the Sanctions and **Anti-Money Laundering Act 2018**, through the Russia (Sanctions) (EU Exit) Regulations 2019 and subsequent amendments. These regulations encompass a range of prohibitions and requirements aimed at discouraging destabilizing actions in Ukraine and preserving territorial integrity. Notably, sanctions cover financial, trade, defence, energy, and tourism sectors, urging compliance and vigilance to uphold these directives.

In similar vein, the United States government, through agencies such as the Financial Crimes Enforcement Network (FinCEN) and the Bureau of Industry and Security (BIS), has intensified efforts to restrict Russia's access to crucial technologies and goods through comprehensive export controls. In 2022, **FinCEN and BIS** issued a collaborative alert, shedding light on the imperative measures financial institutions must undertake to curb potential evasion of export controls imposed on Russia.

Background and Alert Context

The FinCEN and BIS joint alert was prompted by the need to address attempts to evade export controls imposed by the BIS, particularly in the wake of Russia's unprovoked aggression against Ukraine. The alert aims to fortify ongoing U.S. government endeavors to limit Russia's procurement of vital military and defense resources by illicit means.

Impact of Sanctions and Export Controls

The enforcement of extensive sanctions and export controls has considerably hampered Russia's military-industrial complex, creating significant challenges in replenishing lost equipment. This has led to an upsurge in attempts to bypass export controls, making it critical for financial institutions to remain vigilant.

The Case of Illicit Aviation Technology Export:

There was an arrest of two individuals from Kansas who were involved in a clandestine scheme to export aviation-related technology to Russia, breaching U.S. export controls. The accused owned and operated **KanRus Trading Company**, concealing the true end users and end destinations of their exports, often employing transshipment tactics to mask their activities.

New Export Control Measures and Evasion Tactics

Recent export control measures were introduced to impede Russia's access to critical components. The case study underscores the utilization of third-party intermediaries and transshipment points as a prevalent tactic to evade export controls and ensure the acquisition of restricted items.

Identifying Red Flags:

To mitigate the risk of export control evasion, financial institutions are provided with red flag indicators. These flags serve as crucial markers, aiding in the identification of suspicious transactions and prompting further due diligence.

The case study emphasizes the necessity for financial institutions to stay updated with the evolving export control landscape, adopting a proactive approach to identify and report potential evasion attempts. By leveraging the guidance provided in the joint alert, financial entities can significantly contribute to the larger effort of curbing illicit procurement activities linked to Russia's export control evasion.

Technology-Driven Sanction Screening Amid EU's Shift to Criminalize Violations

The Council and European Parliament have reached a political agreement to criminalize the violation of EU sanctions, marking a significant development under the Spanish presidency of the Council. This directive establishes criminal offenses and penalties for the following actions:

- Providing financial services or performing financial activities which are prohibited or restricted
- Trading sanctioned goods and running transactions with states or entities which are hit by EU restrictive measures
- Covering up the ownership of funds or economic resources by a person, entity or body which is sanctioned by the EU."
- Helping persons subject to EU restrictive measures to bypass a travel ban.

The law extends liability to legal persons, with potential penalties including disqualification of business activities. Member states are mandated to ensure effective, proportionate, and dissuasive criminal penalties for sanctions violations, aligning with efforts to strengthen the enforcement of EU sanctions.

Similarly, in the United Kingdom, a new unit, the Office of Trade Sanctions Implementation (OTSI), is set to intensify efforts against companies evading Russian sanctions, with increased powers to issue penalties and refer cases for criminal enforcement. The OTSI's focus includes investigating companies attempting to bypass sanctions through intermediary countries, aligning with the UK's commitment to staunchly implement sanctions and disrupt illicit trade. The establishment of OTSI reinforces the UK's severe sanctions package, which has already led to a significant **94% reduction** in goods imports from Russia.

1. Council and Parliament reach political agreement to criminalise violation of EU sanctions." Consilium.europa.eu, 12 December 2023, https://www.consilium.europa.eu/es/press/press-releases/2023/12/12/council-and-parliament-reach-political-agreement-to-criminalise-violation-of-eu-sanctions/. Accessed 13 December 2023.
2. "New unit to crack down on firms dodging Russian sanctions." GOV.UK, 11 December 2023, https://www.gov.uk/government/news/new-unit-to-crack-down-on-firms-dodging-russian-sanctions. Accessed 13 December 2023.

Note

OFSI, operating under HM Treasury, focuses on implementing financial sanctions to support UK foreign policy and national security. In contrast, OTSI is tasked with implementing and enforcing trade sanctions, including the authority to levy financial penalties for violations, along with an advisory role encompassing business engagement and guidance on trade sanctions.

This highlights the demand for robust tech-enabled sanction screening becomes evident. Technological solutions play a crucial role in ensuring effective enforcement, detection, and prevention of sanctions breaches, aligning with the stringent measures outlined in the newly proposed directive.

Establishing an Effective Sanctions Screening Program

Creating a robust sanctions screening program involves several pivotal steps:

1 . Risk Assessment and Obligations Determination

Start by evaluating your business's sanctions risks and obligations. Identify relevant sanctions lists for your operating jurisdictions. Seek insights from industry experts for guidance.

2 . Software Selection

Choose dependable Anti-Money Laundering (AML) sanctions screening software capable of handling your data efficiently, with scalability to meet future demands.

3 . Customization

Tailor internal controls, procedures, screening tools, and configurations to effectively identify and manage sanctions risks within your organization.

4 . Integration:

Seamlessly integrate the selected sanctions screening software into existing systems and workflows to ensure a streamlined and efficient process.

5 . Employee Training

Conduct training sessions for employees, emphasizing the use of screening software and the significance of sanctions compliance.

6 . Regular Screening:

Implement sanctions screening during onboarding and regularly screen all customers, vendors, and other entities your business interacts with.

7 . Stay Updated

Stay vigilant about sanctions list changes and promptly adjust your screening program to align with these updates.

8 . Monitoring and Evaluation

Implement monitoring and evaluation procedures to assess program effectiveness. Ensure scalability and adaptability to business and regulatory changes. Explore OFAC's Compliance Commitments Framework.

Challenges in Sanctions Screening:

Sanctions screening poses various challenges for businesses. Common issues include data quality impacting result accuracy, managing large volumes of customer data swiftly, ensuring real-time updates to sanction data, resource-intensive program establishment, and navigating diverse and ever-evolving global regulations. Addressing these challenges requires investment in advanced screening tools, high-quality data management, compliance procedures, and regular updates to sanctions lists. Businesses must also adopt efficient case management tools and escalation workflows to facilitate effective sanctions screening processes.

Impact of Non-Compliance

Financial institutions (FIs) and businesses face substantial fines for non-compliance with sanctions, as demonstrated by the surge of over 50% in global fines in 2022, totaling around $5 billion, according to Fenergo. The regulatory landscape, intensified by geopolitical events like the Russian invasion of Ukraine, demands robust compliance measures.

Case Study

Non-compliance with OFAC sanctions on Crimea has resulted in Swedbank Latvia being fined a substantial amount of **$3,430,900**. This serves as a significant financial consequence for the institution, emphasizing the critical importance of implementing effective sanctions compliance controls to avoid severe penalties and reputational damage.

What Should Be Your Plan Of Action?

Considering your next steps?

Prioritize legal compliance with our specialized suite, crafted to facilitate a clear understanding and seamless adherence to regulations. Drawing insights from 200+ sanctions rules spanning 235 countries, we aim to equip you with reliable information. Learn from past incidents for informed decision-making and effortlessly avoid potential pitfalls.

Our commitment is to simplify your compliance journey, ensuring a genuine and effective solution for navigating the complexities of regulatory obligations.

AML Watcher

Turn Insights into Strategy

Get in touch for more information:

info@amlwatcher.com

amlwatcher.com