

The Convergence of Sanctions & AML/CFT Regimes

The Convergence of Sanctions & AML/CFT Regimes

Sanctions and anti-money laundering/countering the financing of terrorism (AML/CFT) regimes, once seen as separate, have been converging. Before, these disciplines involved different data, processes, cultures, and personnel. Now, they are part of an interconnected financial integrity risk management and compliance ecosystem.

- Sanctions regimes, which have traditionally been defined by absolutes such as published lists to be screened, frozen assets, trade restrictions, and strict liability for those who do not comply, are now designed differently, moving into the realm of anti-money laundering and risk management.
- The AML system, which was born from law enforcement, based on principles of transparency, accountability, and traceability, now encompasses national and financial security issues.

This has real world consequences for sanctions compliance and financial crime risk management professionals. Financial institutions that understand this new landscape will be better situated to manage their real and regulatory risks. Senior U.S. Treasury official, Elizabeth Rosenberg, [discussed](#) this convergence and its implications during an AML conference in late 2023.

“The two areas of highest priority for my office—sanctions to advance the foreign policy goals of the U.S., and the strengthening of the U.S.’s own AML/CFT regime—are deeply linked ...

... the continued siloing of AML/CFT and sanctions departments at some financial institutions can lead to financial institutions unwittingly, or inadvertently, processing payments involving designated entities.”



Elizabeth Rosenberg,
U.S. Treasury Assistant Secretary for
Terrorist Financing and Financial Crimes

European and American academics have recently written about these new dynamics and designed specialized programs on financial integrity covering both AML/CFT and targeted sanctions.

“With sanctions becoming an increasingly important tool in ostracizing autocratic regimes from western markets, the need for effective enforcement of AML policies is increasing. The global AML regime will be the backbone in detecting evasion of sanctions.”

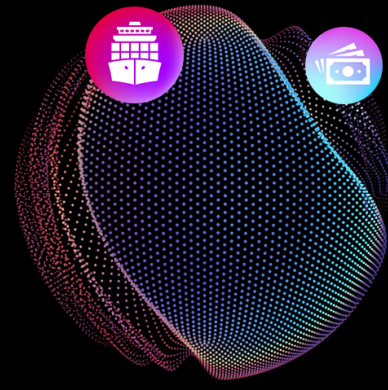
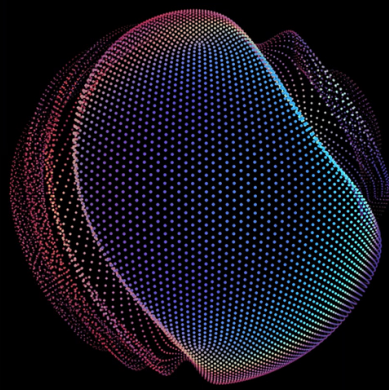


**Giancarlo Spagnolo and Theo Nyrreröd,
Stockholm School of Economics Policy Brief**

“To be truly effective, professionals must be knowledgeable about the law and policy of each of these measures (AML, CFT, and sanctions). [Our] program is carefully designed to accomplish exactly that goal.”



**Arizona State University,
Thunderbird School of Global Management,
Master of Leadership and Management with a
Specialization in Financial Integrity (MLM-FI)**



The convergence of sanctions and AML/CFT has been in motion for more than a decade but the international response to Russia’s invasion of Ukraine has significantly accelerated this development. This came into stark view when Treasury’s lead AML/CFT agency—the Financial Crimes Enforcement Network (FinCEN)—issued an alert requesting increased vigilance for potential Russian sanctions evasion attempts, and when the U.S. Treasury’s lead sanctions agency—the Office of Foreign Assets Control (OFAC)—published an advisory stressing to financial institutions the importance of implementing customer due diligence (CDD) procedures and other AML controls to mitigate risks associated with Russia sanctions.

“ This alert provides select red flags to assist in identifying potential sanctions evasion activity and reminds FIs of their BSA reporting obligations, including with respect to convertible virtual currency ... It is critical that all FIs identify and quickly report suspicious activity associated with potential sanctions evasion, and conduct appropriate risk-based CDD or, where required, EDD ... FinCEN also strongly encourages all FIs to make full use of their ability to share information consistent with [section] 314(b) of the USA PATRIOT Act, and consider how the use of innovative tools and solutions may assist in identifying hidden Russian and Belarusian assets. ”



FinCEN Alert on March 7, 2022: FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts

“ Financial institutions must implement baseline customer due diligence (CDD) procedures and other anti-money laundering controls to mitigate sanctions risk, including to identify and minimize their exposure to activity involving Russia’s military-industrial base and those that support it. Best practices for a risk-based sanctions compliance program include incorporating information and typologies from relevant FinCEN and OFAC alerts and advisories into automated and manual AML controls. ”



OFAC Sanctions Advisory: Guidance for Foreign Financial Institutions on OFAC Sanctions Authorities Targeting Support to Russia’s Military-Industrial Base, December 22, 2023





The convergence of sanctions and AML regimes has been multifaceted and can be broken down into four main areas: targeting of common conduct, reliance on common preconditions, evolution of common compliance program pillars, and emergence of common red flags.

Common Targets

AML Predicate Offenses & Sanctions Programs Convergence

Sanctions and AML/CFT measures both serve as tools to combat illicit conduct. As sanctions programs and AML/CFT regimes have expanded significantly in recent years, there has been increasing overlap in the specific conduct targeted by both. Threats to national and collective security targeted by sanctions regimes have converged, in many ways, with serious organized crime targeted by AML regimes.

The chart on the next page describes six criminal activities considered money laundering predicate crimes targeted by AML regimes that are also types of conduct targeted by sanctions regimes. Moreover, sanctions evasion may be a predicate offense for money laundering as it involves either a specified unlawful activity in some jurisdictions or may involve criminal activity that is a predicate offense to money laundering.

AML Predicate Offenses	 UN Sanctions	 U.S. Sanctions	 EU Sanctions	 UK Sanctions
Terrorism	✓	✓	✓	✓
WMD Proliferation	✓	✓	✓	✓
Corruption		✓	✓	✓
Human Rights Violations	✓	✓	✓	✓
Organized Crime	✓	✓	✓	✓
Narcotics Trafficking		✓	✓	✓

Note: EU and UK narcotics trafficking sanctions are specific to Syria. In early 2025 the UK announced the intent to establish organized crime sanctions associated with human smuggling. The EU Commission proposed a draft law in mid-2023 to empower the EU to impose corruption-related sanctions.

Common Preconditions

Financial Transparency

For sanctions programs and AML/CFT measures to be effective, they rely on certain common preconditions, most notably financial transparency which is achieved through implementation of AML/CFT preventive measures, and information sharing and cooperation within and across institutions, economies, public and private sectors, and across jurisdictional borders.

Protecting the international financial system from criminal abuse by identifying and closing systemic vulnerabilities through heightened transparency measures has long been an overarching objective of the AML/CFT regime. At the same time, effective implementation of sanctions policy also requires a transparent and accountable international financial system to enable the identification of sanctioned activities and interests of sanctioned individuals and entities. Achieving such financial transparency and accountability requires effective jurisdictional and institutional implementation of preventive measures—backed by sound supervision and enforcement—as called for by AML/CFT regimes.

The AML/CFT preventive measures most applicable to transparency are customer and beneficial ownership identification and verification, company formation disclosure requirements, the Travel Rule requiring certain information to be included with cross-border transactions, and record-keeping requirements. Under global standards, these measures apply not just to financial institutions but also to so called “designated non-financial businesses and professions” (DNFBPs), including trust and company service providers, lawyers and accountants, dealers in precious metals and stones, real estate agents, and casinos.

Information Sharing & Cooperation

Information sharing and other forms of cooperation are critical factors for effective and impactful outcomes in implementing sanctions and combating financial crimes.

Cooperation in both areas comes in many forms and often supports multiple outcomes including AML/CFT and sanctions-related investigations, analysis, indictments, assets freezing and seizing, and civil and criminal penalties.

One suspicious activity report filed by a financial institution or DNFBP may contain important lead information for multiple domestic and foreign agencies working collaboratively to disrupt terrorist support networks, human rights abusers, or sanctions evaders facilitating the proliferation of weapons of mass destruction, to name just a few examples.

According to the Financial Action Task Force, “effectively sharing information concerning possible cases of abuse of the financial system with relevant authorities is one of the cornerstones of an effective AML/CFT system.” FATF has published several reports on this subject, including [consolidated standards](#) for information sharing which are set out in 25 of 40 of its recommendations and impact seven immediate outcomes of the FATF Methodology for assessing effectiveness; information sharing among competent [domestic authorities](#); [private sector](#) information sharing; [data protection, technology](#) and private sector information sharing; AML/CFT and [public-private sector partnership](#); and recovering international proceeds of crime through [inter-agency networks](#).

Sanctions-related interagency and international cooperation has reached a new high in response to Russia’s full-scale invasion of Ukraine, including the establishment of new task forces and coalitions. The U.S. Department of Justice established [Task Force KleptoCapture](#), staffed with prosecutors, agents, and analysts from seven agencies to enforce Russia sanctions and export controls. Multilaterally, the 27 members of the European Union, the members of the G7 (Canada, France, Germany, Italy, Japan, the UK, and the United States), and Australia established the [Price Cap Coalition](#) to place a price cap on Russia origin crude oil and petroleum products to restrict the revenue Russia receives to fund its war in Ukraine.

Common Compliance Program Pillars

The chart below demonstrates that the essential elements of a sanctions compliance program and an AML/CFT program, as articulated by global standard-setters, are largely the same. Given the significant overlap, integrating these programs can lead to a more efficient program and overall stronger risk management for institutions.

Consistent with global standards, financial institutions are required under the Bank Secrecy Act (BSA) and similar laws in non-U.S. jurisdictions, and associated AML regulations and guidance, to establish and maintain an AML/CFT compliance program that includes the pillars shown above.

Sanctions Compliance Program Pillars	AML/CFT Program Pillars
Governance and Management Commitment	Governance and Management Commitment
Risk Assessment	Risk Assessment
Customer Due Diligence / Know Your Customer	Customer Due Diligence / Know Your Customer
Internal Controls <ul style="list-style-type: none"> Aimed at identifying, assessing, and managing sanctions-related risks 	Internal Controls <ul style="list-style-type: none"> Aimed at identifying, assessing, and managing money laundering and other financial crime-related risks
Independent Testing and Auditing	Independent Testing and Auditing
Training	Training

The U.S. Treasury's Office of Foreign Assets Control (OFAC) in 2019 published [guidance](#) strongly encouraging organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States, U.S. persons, or using U.S.-origin goods or services, to employ a risk-based approach to compliance with U.S. sanctions. Although it notably stopped short of mandating a sanctions compliance program, it described in detail the pillars shown above and made clear that lack of an effective compliance program is the root cause for sanctions violations and a factor in pursuing enforcement actions.

Common Red Flags

Since Russia's invasion of Ukraine in February 2022, the U.S. Departments of the Treasury and Commerce have repeatedly highlighted how Russia seeks to evade sanctions and export controls in support of its war effort, such as using third-party intermediaries and transshipment points to circumvent restrictions. These alerts have provided examples of red flags that can signal when and how third parties and intermediaries may be engaged in efforts to evade sanctions or export controls.

Many of these red flags are the same or similar to longstanding AML-related red flags, demonstrating that AML controls and investigations can be helpful in detecting sanctions evasion and uncovering assets and transactions of designated individuals and entities.

- ▶ Use of corporate vehicles (i.e. legal entities, such as shell companies, and legal arrangements) to obscure (i) ownership, (ii) source of funds, or (iii) countries involved, particularly sanctioned jurisdictions
- ▶ Use of third parties to shield the identity of sanctioned persons and/or PEPs seeking to hide the origin or ownership of funds, for example, to hide the purchase or sale of real estate
- ▶ Accounts in jurisdictions or with financial institutions that are experiencing a sudden rise in value being transferred to their respective areas or institutions, without a clear economic or business rationale
- ▶ Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration
- ▶ Company registered in jurisdiction previously associated with Russian financial flows and that has seen a notable increase in new company formations

- ▶ Transactions involving public officials and funds moving to and from countries with which the public officials do not appear to have ties
- ▶ Transactions involving public officials related to high-value assets, such as real estate or other luxury goods, that are not commensurate with the reported source of wealth for the public official or that fall outside that individual's normal pattern of activity or lifestyle
- ▶ Documents corroborating transactions involving government contracts (e.g., invoices) that include charges at substantially higher prices than market rates or that include overly simple documentation or lack traditional details (e.g., valuations for good and services)
- ▶ Jurisdictions previously associated with Russian financial flows that are identified as having a notable recent increase in new company formations
- ▶ Transactions involving entities with little or no web presence (such as a website or a domain-based email account) or the online presence suggests business activity inconsistent with the stated line of business

Sources: [Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note: Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls, March 2, 2023](#)

FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts, March 7, 2022

Case Study

Sanctions Evasion, Financing of Terrorism, Tax Evasion

In 2023, the U.S. Department of the Treasury reported on a network of 52 entities and individuals in Lebanon, the United Arab Emirates, South Africa, Angola, Cote d'Ivoire, Democratic Republic of Congo, United Kingdom, and Hong Kong that were used to assist a designated person (Nazem Said Ahmad) evade sanctions and finance Hizballah. The network facilitated the payment, shipment, and delivery of cash, precious gems, art, and luxury goods. It utilized legal and illegal arrangements to falsify certificates, to manipulate diamond prices and taxes, and to give the business the appearance of legitimacy.

The network also used aliases, front companies, and fraudulent documents to enable Ahmad to purchase or consign high-priced luxury goods and artwork from auction houses and galleries worldwide. The network undervalued invoices for imported goods and cleared bulk items through seaports, enabling the assets to be moved into Lebanon without paying the applicable taxes and duties. Many of these red flags, such as the use of aliases, front companies, and falsified documents, are indicators of multiple types of offenses.

This case study highlights a broader theme: the more permissive areas of the financial system and related ecosystems are attractive to illicit actors including money launderers, corrupt officials, sanctions evaders, and their networks. For example, the market in luxury goods such as art has several characteristics that makes it more vulnerable to misuse.

- The high value of these items relative to other goods and commodities, and often with relatively small size
- The subjective valuation and lack of stable pricing
 - Note: This makes it difficult for border authorities to identify when the value of works is mis-declared. For example, a [U.S. investigation](#) in 2007 identified that a work of art that was acquired with the proceeds of fraud had been illegally imported from the Netherlands into the United States with a declared value of \$100 when it was later appraised at \$8 million.
- The transportability of items including across international borders and difficulty in the ability of law enforcement to monitor these movements
- The accepted use of third-party intermediaries to purchase, sell, and hold artwork while clients remain anonymous

Source: [U.S. Treasury's Study of the Facilitation of Money Laundering and Terror Finance through the Trade of Works of Art, February 2022](#)

Conclusion

Ultimately, sanctions and AML/CFT regimes together define financial integrity and security.

All those concerned with advancing collective security interests through financial pressure campaigns and with protecting the financial system from use by illicit actors must understand this overlap.

Financial institutions that understand this new landscape will be better situated to manage their real and regulatory risks. And well-trained financial integrity professionals who recognize this convergence of sanctions and AML/CFT will be better positioned to advance their careers, the interests of their enterprises, and the broader financial integrity mission.



**Join Us in Protecting
the Integrity of the
Financial System**