
# The evolution of sanctions and PEPs

Sanctions have been used throughout history to bring about change. They can influence a country's or an individual's activities or policies—particularly if breaches of international law or human rights have occurred, or if a democracy is under threat. Recently, sanctions have been used to target the activities of terrorists and countries involved in nuclear proliferation. While they can take a number of forms, financial sanctions and trade-related sanctions have been the most frequently used over time.

## War or embargo: A historical view of sanctions

Embargoes date back to America's Founding Fathers when they were used as a weapon of diplomacy and first alternative to war. The lessons learned from applying economic leverage against Britain were sufficient for America to ultimately achieve independence. From 1794 to 1812, the new republic attempted to balance its belief in freedom of the seas with its use of economic measures to influence European behavior. Since the War of 1812, the U.S. Department of the Treasury (DoT) has been involved in economic sanctions against foreign states.

A significant milestone in the history of sanctions came on October 6, 1917, with the passing of the Trading with the Enemy Act. Designed to stop any American from trading with their enemies and the allies of their enemies during World War I, the Trading with the Enemy Act was patterned after the 1914 act of the same name prescribed by the U.K. Parliament. It defined "enemy" as foreigners and countries at war with the U.S. What makes the Trading with the Enemy Act so interesting is that it provides a glimpse into the future of international sanctions, the severe penalties for noncompliance and the governance over forfeiture of assets.

The authority to establish the Office of Foreign Assets Control's (OFAC) earliest predecessor, the Office of Foreign Funds Control (FFC), was derived from the Trading with the Enemy Act. Administered by the secretary of the treasury throughout World War II, the FFC's Proclaimed List of Certain Blocked Nationals, also known as the "Black List," contained individuals and firms with German, Italian and Japanese links that were blocked from doing business in America. The list was a precursor to the Specially Designated Nationals (SDN) list issued by OFAC.

OFAC was established by a Treasury Department order in 1950 following the entry of the People's Republic of China into the Korean War. All Chinese and North Korean assets subject to U.S. jurisdiction were blocked when President Harry S. Truman declared a national emergency.

Formal legal discussion of the legitimacy of sanctions did not occur until the 20th century with the formation of the League of Nations and later the U.N. Between 1960 and 1990, the majority of sanctions were imposed unilaterally—most frequently by the U.S. By the 1990s, a large fraction were imposed by intergovernmental coalitions, which typically included the countries of Western Europe and the U.S.

Today, global sanctions include those issued by the U.S., the EU and the U.N. (See Graph 1). Recent coalition negotiations with Iran led by the U.S. include the potential easing of sanctions over a period of time if Iran meets requirements in the agreement for scaling back its nuclear program. Likewise, after 50 years of Cold War, the U.S. is moving to normalize relations with Cuba.

In addition to Iran and Cuba, Russia poses some of the latest challenges for financial institutions. EU foreign ministers recently approved the decision to extend for another six months "sectoral sanctions" on Russia, which target energy, defense and financial firms. The sanctions were due to expire on July 31, 2015. The extension of sanctions will likely cause the number of Russian and Ukrainian individuals and entities added to the OFAC SDN list to grow. Since the outbreak of violence in the region, OFAC has added names and companies to the list eight times.

The events in Iran, Cuba and Russia are representative of the moving sanctions target. These changes will no doubt place a strain on existing resources. To keep up, financial institutions will require more robust AML systems to handle continuous monitoring and negative news screening, and a change in mindset to adapt to more frequent monitoring.

## Expanding regulatory compliance beyond sanctions

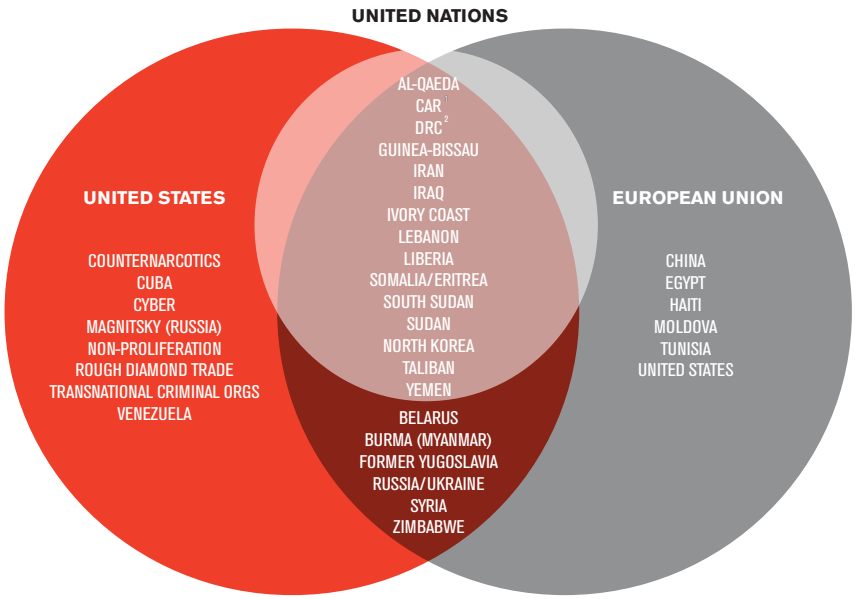
In 1970, the U.S. Congress passed the Bank Secrecy Act (BSA), also referred to as the anti-money laundering (AML) law, to safeguard the financial system from money laundering. Administered by the Financial Crime Enforcement Network (FinCEN), the BSA requires financial institutions in the U.S. to record and report cash purchases of negotiable instruments of more than $10,000 and to report suspicious activity that might indicate money laundering, tax evasion or other criminal activity.

At the G7 Summit in Paris in 1989, the Financial Action Task Force (FATF)—an intergovernmental organization—was established to study money laundering trends and develop policies to combat money laundering. FATF's 40 Recommendations set the international standard for AML measures while allowing countries to implement these principles in accordance with their constitutional frameworks.

Terrorist financing came under the spotlight for the first time in 1995 when President Clinton issued an executive order prohibiting the transfer of funds, goods and services to any individual or organization that threatened to disrupt the Middle East peace process. The Specially Designated Terrorist (SDT) label was introduced followed by the 1996 designation of Foreign Terrorist Organizations (FTO). Internationally, the FATF mandate was expanded to include terrorist financing following 9/11.

The late 1990s also introduced the designation of "politically exposed persons" (PEPs) when Nigerian dictator, Sani Abacha orchestrated the systematic theft of assets from the Nigerian central bank with his family members and associates.

Graph 1 **Global Sanctions Regimes**




[1]Central African Republic
[2]Democratic Republic of Congo

Source: U.S. Treasury Department
Credits: Jonathan Masters, Julia Ro

PEPs emerged later in FATF, Section 312 of the USA PATRIOT Act, the EU Fourth Directive and the Wolfsberg Group. In the absence of a global definition for PEPs, most countries base their definition on the 2003 FATF standard.

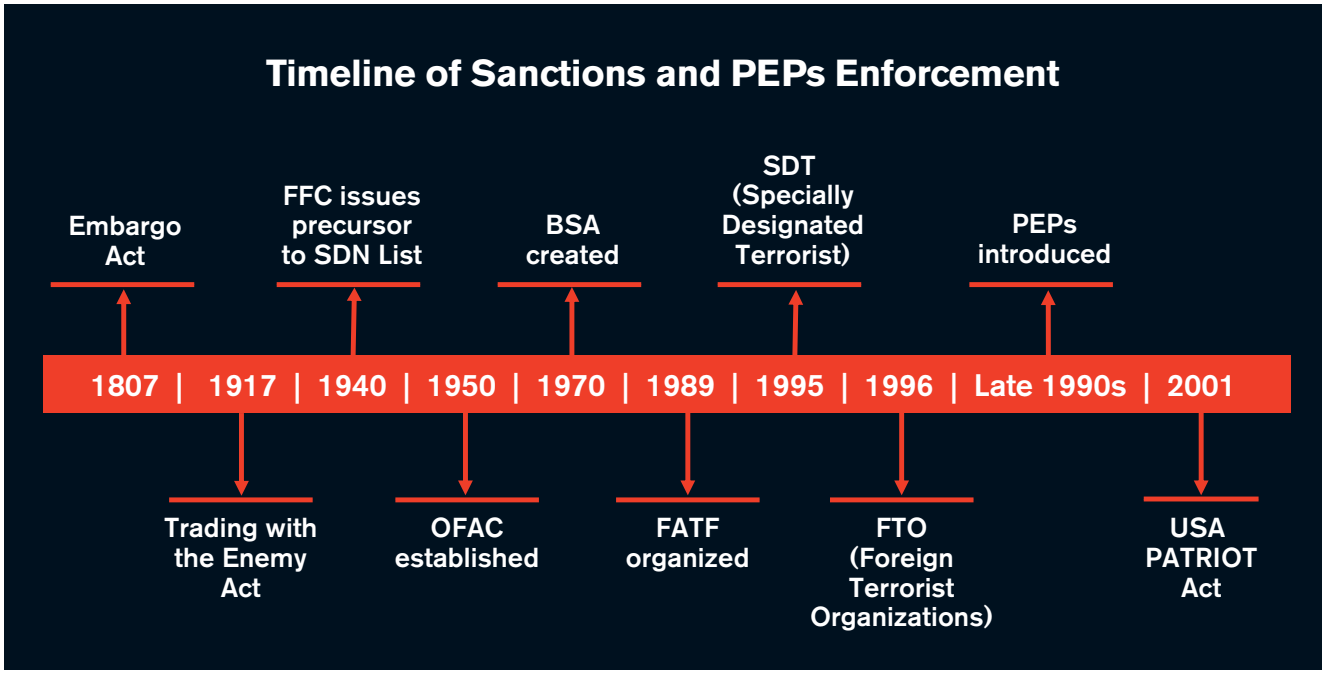
## 9/11: A turning point in AML and compliance

The terrorist attacks of 9/11 set the course of the U.S. and global response for the next decade. Title III of the USA PATRIOT Act dramatically changed the requirements of the BSA to address the critical emerging issue of terrorist financing. The act also provided a platform for other AML-related requirements including know your customer (KYC). Acceptance of an organized and detailed approach to customer identification, comprehensive customer due diligence (CDD) policies and procedures, and the expansion of CDD to enhanced due diligence (EDD) are now considered the cornerstone of a strong BSA/AML compliance program. The most effective programs start at the onboarding process and include a strong culture of compliance that infuses every level of an organization from board members and senior managers to investigations staff. Because of continuous changes in regulatory requirements, education and training play an important role in the success of an institution's AML efforts.

In the post 9/11 regulatory environment, OFAC's sanctions on terrorism and weapons of mass destruction were amended and updated. The lists of individuals and entities were expanded and updates to the list were more frequent. Similarly, U.N. and EU sanctions programs were also expanded. These changes have led compliance departments to pursue greater and more frequent screening on individuals and entities as well as to look specifically for terrorist financing.

Although subject to scrutiny pre-9/11, PEPs have gained greater attention in the past 10 years due to the increased importance of foreign corruption issues. The Riggs Bank case remains an infamous reminder of how foreign corruption proceeds were easily laundered in the U.S. More recent political turmoil in the Middle East has once again shed light on foreign corruption and large fortunes placed offshore by ousted political leaders. FATF guidance implies that if a person is a foreign PEP they are also a domestic PEP in their own country. Whereas the original practice was to screen only foreign PEPs, world events have highlighted the importance of also screening domestic PEPs. Most of the FATF member countries now treat foreign and domestic PEPs with heightened scrutiny—screening at account opening followed by enhanced monitoring for ongoing due diligence. Technology is the grand enabler for comprehensive screening. Ongoing monitoring and keeping up with changing sanctions cannot be done effectively without the use of technology.

The USA PATRIOT Act extended AML program requirements beyond financial institutions to include casinos, broker/dealers, currency exchanges, certain insurance companies and mutual funds. It also identified some customer types with the potential for money laundering or terrorist financing as high risk, requiring more due diligence. These included charities, nongovernmental organizations (NGOs), nonresident aliens (NRAs), foreign embassies/consulates and nonbank financial institutions. The expansion of AML regulatory requirements meant increased regulatory oversight and penalties administered by U.S. governmental agencies, both federal and state and their EU equivalents.



## The growing role of technology

Early interdiction software evolved from a need to identify bad actors. It searched transactions for names that matched those listed on the OFAC SDN list. The process became more complicated as the number of entities on the list grew and the EU and U.N. introduced other government sanctions lists. While interdiction software was not mandatory, it facilitated compliance with growing regulatory requirements for international sanctions.

Times have changed. Rapid developments in financial information, technology and communication allow money to move anywhere in the world with speed and ease, creating a host of new challenges. Regulatory requirements and compliance mandates continue to grow while bad actors and rogue nations craft new ways to circumvent systems and processes designed to detect their illicit activities. Frequent changes to sanctions lists, poorly formatted data, misspellings, aliases and exponential growth in third-party reference lists make it impossible for institutions to keep up without using technology.

An entire industry has developed around providing what has come to be known as BSA/AML software. Automated systems have become a necessity to not only keep pace and comply with the changes in regulatory requirements, but to effectively manage risk across the enterprise especially when dealing with large volumes of customer information and transactions. KPMG's 2014 Global Anti-Money Laundering Survey bears this out. It cites expenditures on transaction monitoring systems as the largest contributor to banks' escalating cost of AML compliance. The increasing cost of compliance has given rise to hosted platforms and Software as a Service (SaaS). Institutions are embracing these options with greater confidence in the security controls to protect their customer data. Lower total cost of ownership, rapid deployment and business continuity are some of the key benefits to be realized.

The complexity of screening customers and transactions against a variety of government sanctions lists, third-party reference databases of PEPs and negative media has only increased the use of list management services. These services facilitate seamless integration with filtering engines and eliminate the time-consuming, labor-intensive process of managing multiple lists.

In today's environment, data quality and the ability to process enormous amounts of data with speed and accuracy are critical to an AML program's success. Technology increases efficiency by eliminating labor-intensive manual procedures and frees up resources to focus on other issues. Since keeping up with regulatory and world events are critical, compliance professionals should look for systems that employ continuous KYC, which hinges on a system's ability to handle the scale, scope and uncertainty of massive, unstructured data, and provides a hedge against risk. System models that support this approach bring innovation to the screening process with the use of machine learning and artificial intelligence (AI) to map millions of data points to identify hidden risk.

Data visualization, advanced analytics and robust research tools that convert information to actionable intelligence are emerging as "must-haves" in an AML platform. Other important technology features include:

- Pattern recognition—to detect approximate classes, clusters or patterns of suspicious behavior either automatically (unsupervised) or to match given inputs.
- Neural networks—to learn suspicious patterns from samples and to be used later to detect them.
- Link analysis—to evaluate relationships and connections between organizations, people and transactions.

The introduction of more sophisticated and powerful AML solutions that screen an institution's entire customer database daily for sanctions, PEPs and negative media without generating an unmanageable number of alerts and an explosion of false positives should be good news to compliance professionals. After all, too many false positives seem to be the proverbial thorn in every compliance manager's side, which is why they were identified as one of the top compliance challenges in the Dow Jones 2015 Global Anti-Money Laundering Survey results. However, compliance professionals must keep more than eliminating false positives in mind when evaluating AML vendor solutions. It is important to understand the structure of your bank, reporting requirements for senior management and what technical solutions will get through the bank's compliance program. AML systems must be able to keep pace with changes in regulations and bank policies, identify and prevent reputational risk, and most importantly, demonstrate to regulators that adequate controls are in place.

The convergence of business and technology is bringing greater collaboration with information technology (IT) professionals to respond to regulators' scrutiny on model validation, data integrity and effective automation planning. This is critical as penalties imposed from enforcement actions now extend beyond the institutions themselves to the individual level as officers and directors of banks are being held accountable for deficiencies in AML programs.

## Conclusion

Based on past history it is likely that governments, including the U.S., will continue to use sanctions as a first response to geopolitical issues. As global events shape the world stage, AML challenges will continue to grow in complexity. To meet these challenges head on, technology is a must. The best compliance programs will start with strong corporate governance and include an enterprise-wide approach to sanctions and PEP risk, well-trained staff to manage compliance, and systems and controls that keep pace with cutting-edge technology.

*Carol Stabile, CAMS, senior business manager, Safe Banking Systems, Mineola, NY, USA, carol.stabile@safebanking.com*