Dow Jones Risk & Compliance

CELENT

Neil Katkov, PhD

Achieving Global Sanctions Compliance: Challenges and Solutions

August 2011

A member of the Oliver Wyman Group

Content

3 Executive Summary
5 Survey Background
5 Leveraging Dow Jones Risk & Compliance's Expertise
6 Introduction
6 Special Challenges—The Arab Spring
8 Compliance Operations, Technology and Data at Large Global Banks
11 Cost of Watchlist Operations
11 The Tangled Web of Compliance
13 Current Compliance Practices
13 Centralization of Operations and Systems
14 Limits to Centralization: Know Your Customer
15 Challenges of Sanctions Compliance
16 Operational Issues
17 Complexity of Systems
18 Data Issues
20 Risks of Decentralized Watchlists
21 Emerging Best Practices in Sanctions Compliance
21 Enterprise-Wide Operations and Systems
23 Enterprise-Wide Data
23 Special Challenges—Non-Latin Scripts
25 Best Practices in Watchlist Management
26 Fitting the List to the Task
26 Enhanced Compliance Databases
27 Optimized Sanctions Watchlists
29 Looking Forward
30 Leveraging Celent's Expertise
30 Support for Financial Institutions
30 Support for Vendors
31 Related Celent Research

Executive Summary

This report provides an independent analysis of the challenges and best practices in managing customer and transaction screening processes—"watchlist filtering"—for sanctions compliance, transaction monitoring and customer due diligence at large financial institutions. The study aims to bring forth issues related to achieving efficiency and consistency across complex, distributed compliance operations at major global banks, across geographic and line-of-business divisions.

The study focuses in particular on sanctions compliance, which is the area of AML compliance that is most dependent on watchlist data, especially data from regulatory watchlists. Indeed, from the technology point of view, sanctions compliance might be said to be primarily an issue of effective management and exploitation of data.

This report is based on Celent's own observations of the state of sanctions compliance, as well as conversations with some 15 large banks in North America, Europe and Asia. Findings include:

- The cost of maintaining sanctions compliance is only escalating. The home markets of many of the large global banks—the US, UK and EU countries— have active regulators that require banks to adhere to the latest developments in technology and operations, sending new spending into the millions annually.
- Celent estimates that for firms managing watchlists internally, this cost alone averages some US$1.5 million annually at a large financial institution.
- To keep costs in check and improve operations, large banks are organizing centralized operations and technology platforms that perform sanctions compliance across multiple business lines of the bank.
- Some banks feel they have watchlist management under control, while others see it as a burden incurring significant cost, effort and specialized expertise. Based on our conversations with banks, Celent believes that even firms that are now managing their watchlists internally will tend to move to commercial watchlist management services.

- Alternatively, a bank may source watchlists from a commercial watchlist provider that has these capabilities already built into their product, saving the bank from reinventing the watchlist wheel. For financial institutions with more decentralized sanctions operations, the ASP or browser-based delivery option of the commercial watchlist providers also enables distributed access to this uniform data by users across business lines and geographies.

Survey Background

Dow Jones Risk & Compliance commissioned this study and worked in conjunction with Celent on the formal survey to question banks in North America, Europe and Asia. The survey, focused on the top tier firms in each region, was conducted in June and July 2011 with 15 banks participating.

Leveraging Dow Jones Risk & Compliance's Expertise

Dow Jones Risk & Compliance is recognized for providing critical sanctions data, independently verified for accuracy and timeliness, to financial institutions and regulated firms globally. Sanctions data is updated and maintained on a follow-the-sun basis by a dedicated team of experts in five key centres around the world. In addition to sanctions data formatted for client screening, Dow Jones has developed a robust third-generation data structure, designed specifically for tight integration into transaction filtering applications and proven to significantly reduce screening volumes.

For more information see www.dowjones.com/riskandcompliance.

Introduction

Sanctions compliance and the area around watchlist screening has over the past several years become one of the primary hotspots in anti-money laundering (AML) compliance. As regulators put more pressure on financial institutions to ensure strict compliance with embargoes, banks must be able to show that they are taking reasonable, adequate and effective measures. For large financial institutions operating across multiple lines of business and many global locations especially, the consistent application of compliance standards across departments and jurisdictions is becoming an important goal. In addition to the regulatory risk, inadequate enterprise-wide sanctions compliance may also expose a financial institution to reputational and commercial risk.

Achieving consistency in global sanctions compliance involves standardizing operations, technology systems, and perhaps most essentially the compliance data—watchlists—that drives sanctions filtering. This study will examine the challenges involved in achieving global sanctions compliance, and the approaches that major global banks are taking to overcome these challenges.

Special Challenges—The Arab Spring

The popular uprisings and ensuing civil conflict in Egypt, Libya, Syria and elsewhere in early 2011 serves as a potent reminder of the need for agility in sanctions compliance. Celent's recent conversations with banks indicated that the incidents in the Middle East have driven an increase in countries for which regulators are requiring escalated diligence, which is having a measurable impact on compliance operations. Even when dealing with entities that are not on sanctions watchlists, banks must exercise care in determining who to do business with in these sensitive regions. This is a significant challenge to banks with business operations in the Middle East, or simply banks with a global footprint.

The turmoil and heightened regional tensions caused by the Arab Spring has resulted in a flurry of sanctions activity by the US, UK and EU, as seen in Table 1 below, as well as large scale additions to sanctions watchlists. According to Dow Jones Risk & Compliance, Q1 of 2011 saw over 1,100 updates to international sanctions lists (including nearly 80 new Libyan entities), a nearly 45% increase over updates in

the same period in 2010. Banks are uploading regulatory watchlists two or three times a week, at least double that of the past. This has naturally resulted in banks experiencing higher volumes of alerts in their sanctions filtering, and putting some pressure on their sanctions compliance operations.

The heightened pace of watchlist updates also demands increased agility by banks in keeping up with these changes to the regulatory lists. The need for efficient, consistent and timely management of the watchlist data that powers sanctions compliance is a central theme of this study.

Table 1: Sanctions list changes in Spring 2011

Country	Sanctions target
Canada	Syrian government officials
EU	Libyan Khadafi regime entities
EU	Syria
EU	Iran (multiple actions)
UK	Syrian entities
UK	Libyan entities
UK	Belarus entities
UK	Al-Qaida and Taliban Sanctions
US	Iranian entities (multiple actions)
US	Syrian, Korean, Chinese, Belarus entities
US	Army of Islam

Source: moneylaundering.com

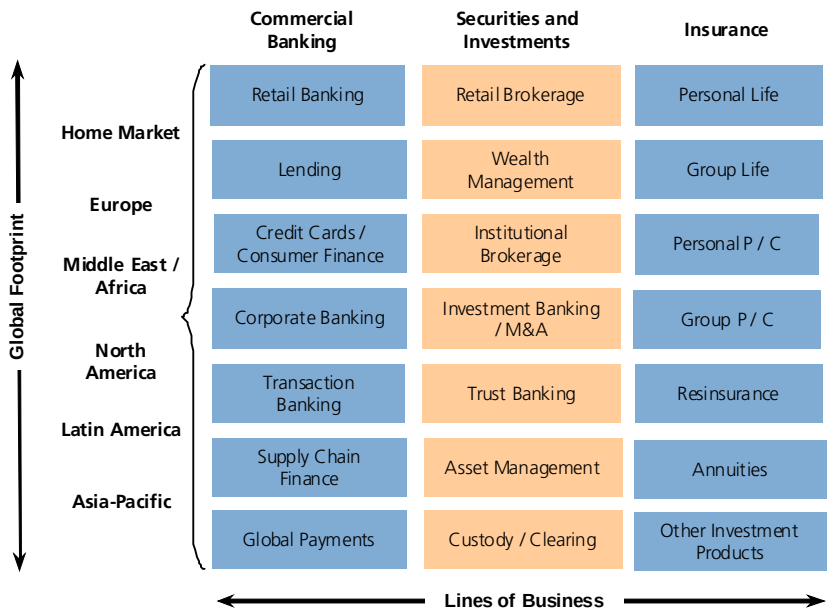
Compliance Operations, Technology and Data at Large Global Banks

AML compliance at large financial institutions is complex, in terms of operations, technology systems, and data. This complexity arises naturally from the wide range of businesses and regions in which these institutions are active. AML compliance across a large bank's entire enterprise may involve 200, 750 or even 1,000 staff. A major theme within large banks today is centralizing and standardizing compliance organizations, in order to bring this burgeoning complexity under control.

A snapshot of the makeup of large banks is useful in reminding us just how extensive these organizations are, and the broad range of services and geographies compliance must cover.

- **Lines of business (LoB).** Large financial institutions are active across the entire range of financial services, from commercial banking to securities and investments. A number of European and Asian financial groups especially also run insurance businesses, making them true universal banks. Even a brief rundown of the major LoBs within these organizations suggests the enormity of their operations:
  - Commercial banking: retail banking, credit cards, consumer finance, corporate banking, transaction banking, trade finance, global payments.
  - Securities and investments: retail brokerage, private banking / wealth management, institutional brokerage, investment banking, trust banking, asset management, custody and clearing services.
  - Insurance: personal and group life, personal and group property / casualty, fixed and variable annuities, other investment / savings products.
- **Regions.** The large global banks of Europe and the US maintain operations in 50, 75 or even 100 countries across EMEA, Asia and the Americas. The large Asia-Pacific banks have also been building out their international networks, which may extend to 30 or 40 countries (see Figure 1 on page 9).

Figure 1: Business and regional footprint at large global banks



Source: Celent

AML compliance at large institutions must span all these lines of business, and all the countries in which they operate. The complexity doesn't stop there, however, as compliance itself comprises numerous operations across the front, middle and back offices.

- **Compliance operations.** AML compliance extends across the entire life cycle of a client, from initial onboarding at account opening, to ongoing monitoring of transactional and non-transactional activity, to periodic reviews of the existing client base.
  - AML compliance in the front office focuses on know your customer (KYC) activities, such as due diligence and risk profiling of new customers. Compliance in the front office is typically the responsibility of the line of business, for example retail banking.
  - Middle office compliance is largely concerned with ensuring external counterparties to transactions are safe to do business with. This includes the critical area of sanctions compliance: monitoring international payments to ensure counterparties are not on any sanctions lists.

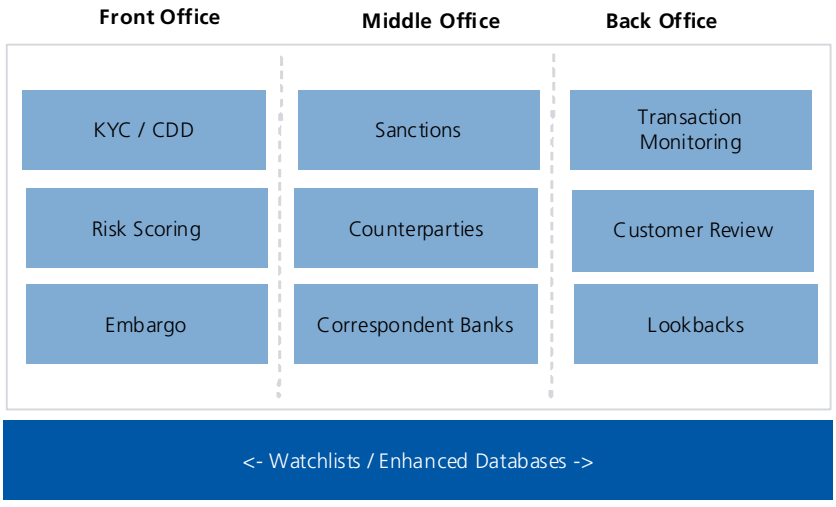
– Back office compliance is responsible for the ongoing monitoring of account activity in order to detect suspicious behavior that may indicate money laundering or other financial crime. Back office analysts also conduct periodic reviews of the customer base to ensure the bank is not doing business with sanctioned entities.

Each area of AML compliance requires technology and data to support compliance operations.

- **Technology systems.** Compliance systems in AML include onboarding and identity verification systems at account opening, transaction monitoring and watchlist screening software for ongoing account activity and customer review, and sanctions filtering systems for real-time domestic and international payments. Finally, effective case management systems are needed to enable compliance analysts to investigate and if need be report on suspicious activity.
- **Data.** Compliance data is integral to AML compliance processes. Watchlists and enhanced compliance databases are used across every stage of AML compliance, from initial account opening, to ongoing monitoring of transactions and periodic review of the customer base, to screening international payments for sanctions purposes.

Compliance data is in fact the only technology that is needed across the entire cycle of AML compliance (Figure 2 on page 10).

Figure 2: Compliance technology in the front, middle and back office

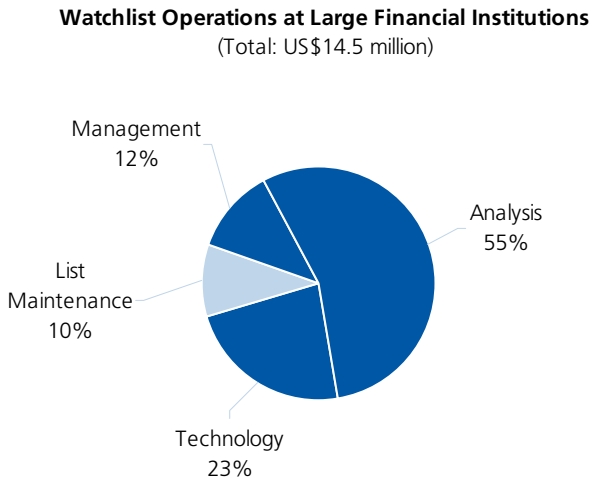


Source: Celent

Cost of Watchlist Operations

As shown above, compliance data is used across a variety of LOBs and functions, making it difficult to estimate costs involved with watchlist operations across the entire, distributed enterprise. Focusing on the more centralized middle and back office functions of sanctions compliance, transaction monitoring, and case analysis, Celent estimates that the cost for watchlist operations at a large financial institution averages US$14.5 million annually. More than half of this, or nearly US$8 million, is associated with analysis of alerts. For those large banks that update, consolidate and maintain watchlists internally, Celent estimates list maintenance costs at nearly US$1.5 million annually (see Figure 3 on page 11). While list maintenance is not the largest piece of the cost pie, it is nonetheless a fairly significant expense.

Figure 3: Cost of watchlist operations in the middle and back office



Source: Celent

The Tangled Web of Compliance

The multiple businesses and regions in which large financial institutions operate give rise to a complicated and fragmented compliance ecosystem. Regulatory considerations add a further layer of complexity.

Large banks maintain group compliance standards. These enterprise-wide standards must invariably be based on the compliance regime in effect in the bank's home market, because the home market regulators consider the bank's entire operations under their purview, including foreign market operations. At the same time, the local branches of banks must comply with the AML regulations in effect in each country

in which they operate. Moreover these local market compliance requirements can be quite specific and granular. Finally, financial institutions operating globally are concerned with complying with the AML regulations of the US and their specific requirements for foreign correspondent banks and international payments, which in effect bring virtually all international payments in US dollars under the scrutiny of US regulators. A similar concern exists with British pounds and Euros.

These overlapping regulatory considerations add further complexity as large global financial institutions must develop compliance policies, reporting lines and operations that cover these multiple regulatory layers. In the area of sanctions compliance specifically, the task is exacerbated by the need to screen payments against numerous international and local watchlists.

The extensive AML compliance operations large global institutions must maintain across lines of business, geographies and regulatory regimes creates an intricate and decentralized compliance framework. The following section will take a look at how banks have been working to organize and simplify these tangled webs of compliance.

Current Compliance Practices

In order to establish effective compliance across their wide range of business lines and far flung global locations, large financial institutions have been working to standardize and centralize their compliance processes. These efforts span the areas of operations, technology systems, and compliance data.

Centralization of Operations and Systems

In terms of operations, large banks are organizing their AML compliance into centralized middle and back office operations that monitor activity and perform customer due diligence investigations across multiple business lines of the bank.

In terms of technology, banks are attempting to reduce the number of software systems they use. Banks that previously operated many separate systems across their various lines of business are standardizing on a more restricted technology base. While centralizing on one single software platform may be an ultimate goal, the historical and operational differences between lines of business as different as commercial banking and brokerage make this impractical. Currently most banks are at the stage of limiting themselves to two or three systems both on the monitoring side and on the watchlist screening side. Ideally the output of these different systems will be fed into a centralized case management system to enable coordinated, enterprise wide investigation and reporting, but again this is an elusive goal for most banks.

To reduce complexity in compliance across multiple countries and regions, banks have been establishing compliance hubs to centralize compliance operations and technology across a region. A bank taking this approach will typically maintain three or four hubs globally, perhaps one each in North and South America, in Europe and in Asia. These compliance hubs will often be colocated with other hubbed operations and systems of the bank. Although technology and some operations functions may be thus centralized, the bank will of course also have a local AML compliance unit in each country. The question then becomes to what extent compliance operations can be centralized, and which functions must remain locally executed.

Limits to Centralization: Know Your Customer

Celent's conversations with numerous banks make it clear that among the compliance functions most resistant to centralization, whether across business lines or geographies, are those involving customer identification and due diligence: the area of "know your customer." To begin with, the initial onboarding of a customer is carried out by the line of business, which establishes its own criteria for accepting customers from the business point of view. This means the line of business will also often collect the compliance information, including performing identity checks and watchlist scans.

Moreover, each line of business may take a different approach to the customer due diligence process. For a mass retail account, a bank might only perform an identity check and OFAC scan. For wealth management accounts, more extended due diligence will be called for, and banks may utilize enhanced databases, PEP checks and negative news checks. The AML compliance back office may provide support for enhanced customer due diligence for cases difficult to resolve in the front office. For corporate accounts, banks may in addition search a variety of public records to check for the existence of malfeasance. In addition more jurisdictions are requiring banks to identify the ultimate beneficial owners of a corporate account. The approach might also vary by region; for example a risk-based approach might be employed to focus on risks posed in certain "hotspot" jurisdictions.

As a result, banks will often have customer due diligence units set up within each line of business. To bring a degree of standardization and consistency to the fragmented KYC processes across the various business units and geographies, best practice large banks are putting in place enterprise wide KYC systems to automate the basic screening process. Ideally these systems will utilize centrally coordinated watchlists and a standard name matching technology that screens customers against regulatory lists and PEP or other enhanced databases, as well as against the bank's own internal lists.

Challenges of Sanctions Compliance

Sanctions compliance is emerging as perhaps the most sensitive area for AML compliance for large global banks. The reason is straightforward: an outgoing payment is the point at which funds may potentially be moved to a criminal or terrorist entity, or an entity associated with a country against which home market regulators have established an embargo. As international tensions increase with countries such as Iran, regulators are placing intense scrutiny on how banks are ensuring compliance in this area. For banks with far-flung operations worldwide, home market regulators are also concerned with how banks achieve consistency in sanctions compliance among all the countries in which they operate.

For compliance officers, sanctions operations and the systems that interface to SWIFT and other payments gateways is practically a matter of life and death, at least professionally speaking. Even a brief failure—or a delay in processing transactions—would be an embarrassment if not a regulatory risk. Therefore the reliability of the sanctions filtering systems and the efficient processing of payments is of upmost concern.

Sanctions compliance differs from other areas of AML compliance in two essential ways. First, the screening of payments information and decisioning of any alerts must be carried out in real time, before the transaction is released through the payment gateway. Second, sanctions compliance involves transactions with cross-border entities, making the scope of compliance international by definition, and so necessitating the use of international regulatory lists based not only on where the payment is originating from, but also the jurisdiction to which the payment is being made.

Due to the large number of sanctioned entities—some 5,000 names on the US Treasury's OFAC list alone—sanctions compliance requires the use of automated screening technology at any institution regardless of size. At large global banks, the filtering systems are extremely specialized and capable of processing high volumes of wires. Functionality includes workflow to support an analyst in investigating an alert to make a determination of whether the matched name is indeed a true hit on a regulatory watchlist, and if so to block the payment from being made. These filtering systems should also include business rules to

identify payments going to specific jurisdictions, or payments made in specific currencies such as the US dollar or British pound, and applying the appropriate regulatory watchlist to the transaction.

On the other hand, sanctions compliance is quite specific in its purpose: to block payments from being made to embargoed entities. Therefore, sanctions filtering need only screen a transaction against the pertinent regulatory lists. While some banks may decide to take a broader approach and screen against large commercially available enhanced databases or PEP lists, in order to be compliant from a regulatory perspective this is not required. Indeed, to improve the efficiency of the onerous sanctions filtering process, there is a trend among large banks to scale back from the use of very large name databases in favor of lists containing only those entities on the sanctions watchlists.

Banks are finding that the cost of maintaining sanctions compliance is only escalating. The home markets of many of the large global banks—the US, UK and EU countries— have active regulators that require banks to adhere to the latest developments in technology and operations. This requires banks to invest millions in technology, and because technology and operational approaches are constantly evolving, further investments are required on an ongoing basis, in addition to running costs.

In addition to cost issues, the multiple business lines and regions in which large banks operate present significant challenges in the area of sanctions compliance as well. Here we will focus on operational issues, sanctions filtering systems and the compliance data itself that powers sanctions compliance efforts.

Operational Issues

As described earlier, the organizational complexity of large global banks presents a challenge to the deployment of AML compliance operations and systems. The regulatory complexity of operating in dozens of jurisdictions globally means that banks' compliance operations must encompass a bewildering array of local regulations and in many cases local watchlists.

This may mean that a multinational financial organization supports local compliance units in each jurisdiction with the tools to perform watchlist checks or sanctions screening. This results in a decentralized model in which these critical functions are performed locally, with lit-

tle practical oversight by the home office. This leaves the institution open to regulatory risk if the local branches are not scrupulous in fulfilling compliance requirements.

As a result, large banks are furthering their efforts to centralize watchlist and sanctions operations, progressively running more local lists at the central facility as well as possibly sanctions operations. Preparing local lists from the data perspective requires considerable effort, but a bank may put as many as 15 local lists or more on the central system at one go in such an upgrade. Maintaining the watchlists centrally also supports quality control in terms of keeping up with list updates in a timely manner. For the commonly used international watchlists, central processing also ensures that each jurisdiction's transactions are being checked against the same uniform lists.

Complexity of Systems

In order to cover the various lines of business and regions in which they operate, large banks have implemented multiple sanctions filtering systems. In fact, a number of banks have managed to standardize on one software system for much of their payments filtering. Even so, siloed business lines and operations across multiple geographies have required these banks to implement numerous instances of their system of choice.

In Europe, for example, banks may implement separate instances of sanctions filtering software to cover SWIFT payments, cross-border payments that involve gateways other than SWIFT, trade finance, and SEPA payments. In addition, the same bank may install instances to handle North America, Latin America, and Asia Pacific.

In order to limit the complexity of these multiple systems, some large banks are attempting to hub systems as much as possible. Thus a bank may locate multiple instances of a system, supporting 20 or more countries, in one data center. This approach simplifies, for example, the task of maintaining and upgrading the software.

From an operational standpoint, transaction volumes will vary significantly from region to region. A bank's home market may process 50,000 to 250,000 wires per day, while some of the same bank's overseas operations may only have several hundred transactions per day in some small markets. Clearly, different operational approaches are required for markets of such varying sizes. Here too, hubbing systems for multiple countries will allow the provision of automated sanctions filtering for small markets at a less prohibitive cost and effort than if installed

locally. Ideally, any local watchlists will also be run through the centralized system. However in practice large banks are still relying on local operations for sanctions compliance in many markets.

Data Issues

Sanctions compliance is the area of AML compliance that is perhaps most directly dependent on data. Simply put, sanctions filtering involves matching the data in payments messages to the data contained in watchlists. As banks increasingly move to limit their sanctions databases to regulatory watchlists, as opposed to the much broader data sets in enhanced databases, sanctions compliance turns ever more closely on how the data in regulatory watchlists is managed and exploited. This close reliance on the data means that effective sanctions compliance relies on clean, well-managed and optimized watchlist data. But as the industry well knows, watchlist data presents myriad challenges in terms of data quality, complexity and maintenance.

- **Plethora of watchlists.** A basic issue with sanctions watchlists is that there are just so many of them. There is a fairly limited number of regulatory watchlists that are used de rigueur by most institutions operating internationally, including OFAC, the UN list, the EU lists and the UK's HMT list. For large banks operating in dozens of jurisdictions, however, the number of regulatory lists they must screen against might reach 50 or 100. Financial institutions also maintain internal black lists and white lists based on previous experience with customers. In addition, some banks choose to filter against a broader range of data, including other national lists such as those issued by law enforcement agencies, as well as the enhanced compliance databases provided by commercial watchlist providers (see Table 2 on page 18).

Table 2: Taxonomy of AML Compliance Data

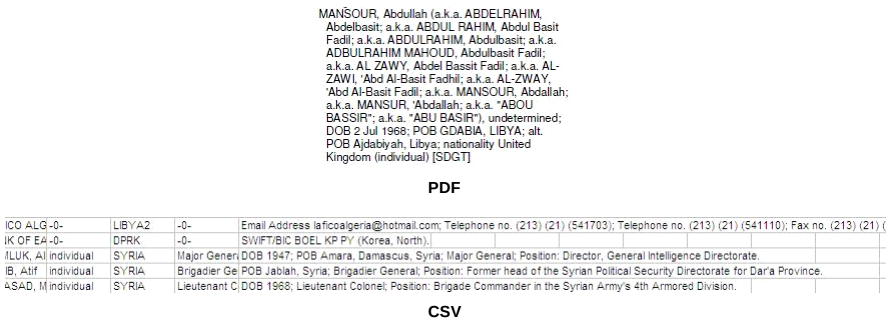
Sanctions Watchlists	Enhanced Databases	Internal Lists
OFAC	PEPs / associates	Black lists
UK HMT	EDD lists	White lists
EU	Corporate lists	Other internal lists
UN	Adverse media	
Other jurisdictions	Public records	

Source: Celent

- **Unoptimized watchlist data.** Even limiting the field to the sanctions watchlists which strictly speaking are the target of sanctions compliance, data management can be onerous. As can be seen from Figure 4 on page 19, watchlists simply are not optimized for automated data processing. In recent years, a number of regulators including OFAC and the UK's HMT have issued their lists in various electronic formats including plain text, delimited CSV files and Excel. However a flat file is only as useful as the data fields it contains, and the OFAC files for example still contain catch-all data fields. Effective use of this information requires parsing the data in these fields for automated filtering.

  More over, the content of the different file format versions of watchlists may not be uniform. For example, the CSV version of the OFAC list provides biographical information missing from the PDF version. Not all lists publish incremental updates, leading to version control issues. Some entities in the current PDF list may not be present in the current CSV version and vice versa. Finally, some lists do not even clearly identify what changes have been made in a list update. Because the regulatory bodies that produce these lists do not provide clean and consistent files, it falls upon the financial institutions to manage the lists to ensure they have the full data set at any given time, in order to be in compliance.

Figure 4: OFAC SDN list: PDF and CSV versions



MANSOUR, Abdullah (a.k.a. ABDELRAHIM, Abdelbasit; a.k.a. ABDUL RAHIM, Abdul Basit Fadil; a.k.a. ABDULRAHIM, Abdulbasit; a.k.a. ADBULRAHIM MAHOUD, Abdulbasit Fadil; a.k.a. AL ZAWY, Abdel Bassit Fadil; a.k.a. AL-ZAWI, 'Abd Al-Basit Fadhil; a.k.a. AL-ZWAY, 'Abd Al-Basit Fadil; a.k.a. MANSOUR, Abdallah; a.k.a. MANSUR, 'Abdallah; a.k.a. "ABOU BASSIR"; a.k.a. "ABU BASIR"), undetermined; DOB 2 Jul 1968; POB GDABIA, LIBYA; alt. POB Ajdabiyah, Libya; nationality United Kingdom (individual) [SDGT]

PDF

ICO ALG -0-	LIBYA2	-0-	Email Address laficoalgeria@hotmail.com; Telephone no. (213) (21) (541703); Telephone no. (213) (21) (541110); Fax no. (213) (21) (
IK OF EA -0-	DPRK	-0-	SWIFT/BIC BOEL KP PY (Korea, North).
ILUK, Al individual	SYRIA	Major Gener	DOB 1947; POB Amara, Damascus, Syria; Major General; Position: Director, General Intelligence Directorate.
IB, Atif individual	SYRIA	Brigadier Ge	POB Jablah, Syria; Brigadier General; Position: Former head of the Syrian Political Security Directorate for Dar'a Province.
ASAD, M individual	SYRIA	Lieutenant C	DOB 1968; Lieutenant Colonel; Position: Brigade Commander in the Syrian Army's 4th Armored Division.

CSV

Source: OFAC

- **Free-for-all payments messages.** The data that is to be matched to the watchlists, that is the payments messages, are similarly not optimized for automated sanctions filtering. SWIFT, the closest thing there is to a global standard in payments, has numerous message types, and multiple data fields within each message where payment instructions may appear. As a result the entire message must be scanned and parsed in order to ensure a thorough screening. Even if a

bank managed to standardize its own outgoing payments, incoming payments originating from banks worldwide will continue to present a formidable variety of formats.

Risks of Decentralized Watchlists

While regulators do not always provide financial institutions with watchlists that are optimized for automated sanctions screening, they of course require banks to thoroughly and accurately match customers, counterparties and payments against the names in these lists. Banks that use multiple sanctions watchlists, and moreover use these lists in many different LoBs and jurisdictions globally, face a challenge in ensuring that their lists are updated and uniform in content and completeness across these dispersed compliance operations.

Banks that rely on different LoBs or branches in local jurisdictions to source and maintain the watchlists they use expose themselves to regulatory risk. Home country regulators are increasingly emphasizing the importance of standardized, consistent compliance processes across a bank's various businesses and global locations.

Lists sourced from different vendors—as well as lists maintained internally by different LoBs or branches—will inevitably differ in completeness of content, format, degree and type of enhancements to the data, and update schedule. This fact alone makes it difficult for a financial institution to demonstrate to a regulator that they are utilizing standardized and consistent processes and data across their operations.

In concrete terms, running these different versions of lists through a sanctions filter will deliver different results. A name might trigger an alert when matched against one list, while not triggering an alert when run off a different list. The name itself might not be in the second list, or the precise content of the entry may differ. This is of course also true for watchlist screening for CDD and transaction monitoring. Such discrepancies will be difficult for regulators to accept.

To ensure consistent and uniform results in watchlist screening across the enterprise, therefore, financial institutions should undertake centralized list maintenance, and enable distribution of these standardized lists to their various business units and branches. A number of global banks are aware of this issue and are building capabilities to do so. Of course, outsourcing this task to a managed service is also an attractive option, in that it would free up internal resources to focus on compliance itself, and potentially reduce costs involved with list maintenance.

Emerging Best Practices in Sanctions Compliance

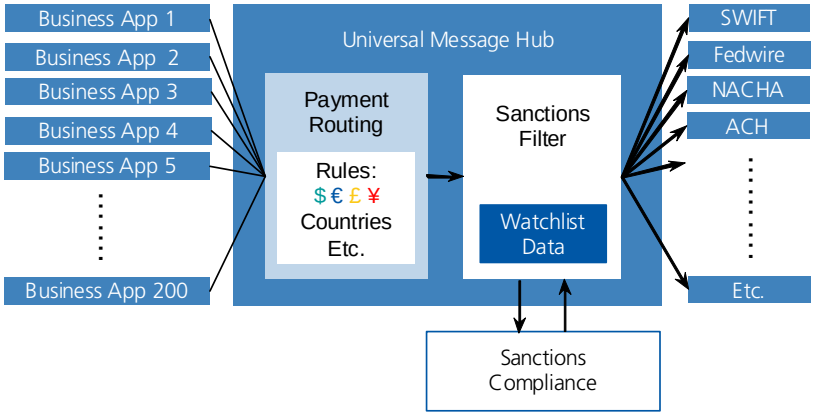
We have examined the challenges that large global financial institutions face in organizing effective sanctions compliance across the entire enterprise. How can these firms ensure that sanctions programs are being enforced uniformly between local, country-specific and centralized compliance operations, as well as across business units? This section will look at some of the evolving best practice approaches with which large banks are striving to overcome these challenges. Essentially, there is a clear movement towards implementing enterprise-wide sanctions compliance in terms of operations, technology systems, and watchlist maintenance.

Enterprise-Wide Operations and Systems

To achieve consistency in sanctions compliance across the enterprise, large banks are evolving towards centralized, standardized operations and technology platforms to handle sanctions screening across virtually all business lines and geographies.

Some best practices banks have already succeeded in standardizing on one technology platform for processing of virtually all payments that go through the bank. Such a platform would still be implemented in perhaps four hubs worldwide, for example in the home country, as well as in Europe, the US and Asia-Pacific. At a large bank, the payments platform might accept payments from over 200 business applications globally—including banking and brokerage related payments—and route them to the appropriate gateways and destinations worldwide. As part of the process, rules in the messaging hub determine which messages need to be filtered and against which lists. The messages are then sent through the sanctions filter and alerts dispositioned by centralized analyst teams. Such a setup might process 50 million messages per month. Such a centralized sanctions filter needs to have definitions for the fields in each type of transaction, including for complex securities transactions, as well as business rules to apply the appropriate international or country-specific lists to each transaction (see Figure 5 on page 22 for a conceptual depiction of such a system).

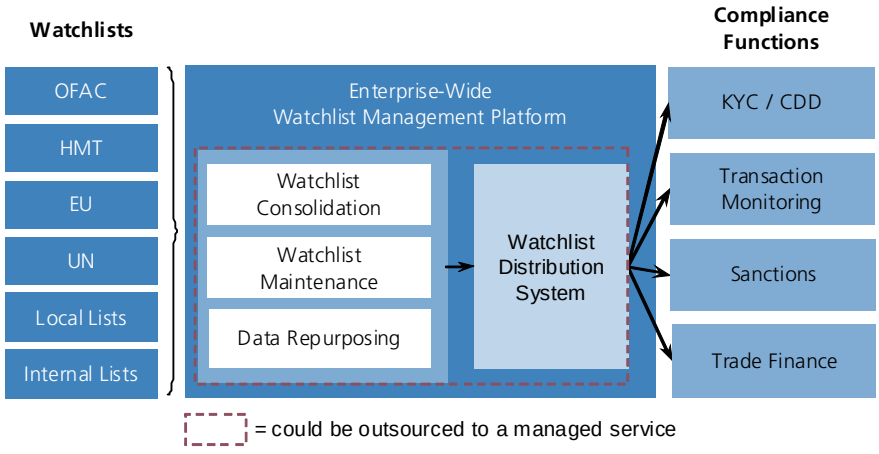
Figure 5: Enterprise-wide sanctions filtering



Source: Celent

Taking the centralization of watchlist screening further would involve building a platform to manage and deliver watchlists not just to sanctions compliance, but across all the areas involving watchlists in a centralized, standardized manner. Best practice banks are developing plans for centralized list management platforms to cover sanctions, customer due diligence / KYC, and transaction monitoring / AML, three major areas of watchlist operations that have historically been separate. The platform would compile all watchlist data centrally, then deliver it to the respective divisions such as CDD / KYC, AML and sanctions. This approach would also require an operations and systems capability to maintain the watchlists in a uniform and timely manner (see Figure 6 on page 22).

Figure 6: Enterprise-wide watchlist operations platform



Source: Celent

Alternatively, the watchlist maintenance and distribution could be outsourced to a service provider specializing in watchlist management.

Enterprise-Wide Data

Regardless of how centralized or distributed their compliance operations are, financial institutions need to ensure that the compliance data they use is configured to a uniform standard, both for efficiency and consistency in operations, and to reduce regulatory risk.

Banks take varying approaches to sourcing their watchlist data. Some banks, even large banks, use first-generation watchlist data; that is, the watchlists in the formats provided directly by the regulators. Due to the data inadequacies of raw government watchlists described earlier, banks must expend considerable effort in developing parsing capabilities, aliases for specific entities, fuzzy name matching, tokens, etc. to supplement the original watchlists in order to render them, in a word, usable. Considering that even the basic international watchlists between them contain over 20,000 entities, the effort required for this is considerable, and ongoing.

Alternatively, a bank may source watchlists from a commercial watchlist provider that has these capabilities already built into their product, saving the bank from reinventing the watchlist wheel. For financial institutions with more decentralized sanctions operations, the ASP or browser-based delivery option of the commercial watchlist providers also enables distributed access to this uniform data by users across business lines and geographies. Because regulators will want to see that the institution is properly utilizing the official watchlist, commercially sourced lists should include the original watchlist reference, in addition to the enhancements developed by the commercial provider.

At the same time, however, financial institutions need to develop their own knowledge base of customers that they wish to either whitelist or blacklist based on their specific institutional experience with these entities. The development of such an internal database is an important tool in improving the efficacy and efficiency of the sanctions process. As a result, financial institutions need to manage both external, official watchlists and their internal lists in a coordinated fashion, and again uniformly across the enterprise.

Special Challenges—Non-Latin Scripts

For global banks, sanctions filtering must also grapple with the special issue of checking names in non-Latin scripts, such as Arabic, Cyrillic, Chinese and Japanese. This problem has given rise to a number of spe-

cialized companies offering solutions to assist financial institutions with matching names in these scripts to the Latinized versions of these names in the international regulatory watchlists on the one hand, as well as identifying non-Latin script names in some local regulatory watchlists, for example Japan's watchlist. Similarly, commercial watchlist providers are also facing increased demand for the ability to handle non-Latin scripts.

Aliases and alternate name versions are a challenge in any watchlist, but the common lack of standard Latin transcriptions for names in scripts such as Chinese, Russian and Arabic exacerbates the problem by creating many more possible transliterations.

A specific issue that has recently emerged as a special problem for banks is the Chinese Commercial Code (CCC), a method of transcribing each Chinese character into a 4-digit number. Sanctions compliance officers at global banks need to be able to correctly identify the Chinese name indicated by this code when used in payments messages in order to check them against regulatory watchlists. Regulators are focusing on this issue in part due to concern over transactions between Chinese and Iranian entities.

Financial institutions tend to be more or less concerned with this issue to the degree that they operate in China, Taiwan and Hong Kong. While some banks seem little bothered by CCC, others admit that as with other special scripts a serious effort is needed to develop capabilities to correctly transcribe CCC and avoid false positives. Considering that CCC could potentially occur in incoming payments messages as well, perhaps even as a technique to disguise the origin of the payment, the need to come to terms with CCC is likely to grow among banks anywhere.

Best Practices in Watchlist Management

Whether a financial institution maintains its compliance data internally or sources it from a commercial provider, we have seen that uniform watchlist data is essential to achieving enterprise-wide consistency in sanctions compliance. We have examined some of the developing best practices in operations and technology systems. Similarly, emerging best practices in watchlist maintenance include the following.

- Regulators are requiring banks to properly screen for wires against regulatory lists by using optimization techniques such as fuzzy matching, aliases and text parsing. As a result such enhancements are becoming an important part of watchlist management.
- Watchlist consolidation can reduce the number of alerts, thereby increasing efficiency of the sanctions filtering process. Indeed watchlist consolidation can increase the efficiency of watchlist maintenance itself. However in consolidated lists, as well as any repurposed watchlist, reference to the original watchlist record should also be included.
- Large global banks need to ensure they input updates to official watchlists in a timely manner. An effective list management approach is needed in order to stay abreast of updates to the official lists in multiple regions worldwide. This means watchlist management itself is essentially a global operation for multinational banks. The same can be said for updating the much larger data sets of the enhanced database providers.

In addition to the watchlist data itself, financial institutions should undertake regular reviews of the screening system to ensure it is up-to-date and effective, in particular to keep up-to-date with name changes in regulatory lists, and regularly calibrated (fine-tuned) to ensure it is returning appropriate results (enough accurate hits).

Fitting the List to the Task

A recurring theme in Celent's conversations with banks is the need to use lists appropriate for the compliance area at hand. Watchlist filtering requirements for sanctions compliance are quite different from those for customer due diligence and ongoing monitoring.

Customer due diligence at account opening as well as for ongoing monitoring generally requires the use of enhanced compliance databases. Sanctions filtering benefits from optimized lists containing only sanctioned entities. As efficient sanctions compliance becomes more urgent for banks, they are increasingly looking to optimize watchlists for sanctions filtering. Some banks are also using such optimized sanctions lists at account opening for embargo checks.

Enhanced Compliance Databases

A number of commercial watchlist providers, including Dow Jones Risk & Compliance, provide enhanced compliance databases which aim to be as complete as possible a listing of high risk identities. Enhanced databases contain information on 100,000s of entities, compiled from a wide variety of sources. As shown in Table 2 on page 18, these sources include news and other media, public records, as well as the government-issued sanctions lists.

Enhanced compliance databases are used by financial institutions to better understand the risk profile of their customers as well as external counterparties to transactions. Regulators may also require the use of enhanced databases such as PEP lists.

PEP lists are a specialized type of enhanced compliance database provided by the commercial watchlist providers that contain information on politically exposed persons, that is, current and former government leaders, politicians, elected officials, bureaucrats and others with connections to government. In addition, these lists may include relatives, business partners and other associates of the PEPs.

Enhanced compliance databases are generally used for customer due diligence at onboarding and during periodic customer review, as well as for ongoing transaction monitoring.

- **Customer due diligence.** The EU, UK and US all require banks to assess the risk profile of customers. As part of this process, many banks screen customers against the large enhanced database sets that contain profiles of 100,000s of entities. Scanning against these large data sets takes time, so for banks that open large numbers of accounts each day, this screening is often done on a batched basis. Batch screening is also used for periodic screening / review of existing customers.

  Some jurisdictions, such as the EU countries, require that banks determine if customers are PEPs, or associates or relatives of PEPs. This requires use of the enhanced compliance databases specifically compiled to address the PEP issue.

- **Transaction monitoring.** Financial institutions may also use enhanced compliance databases to screen names in transactions as part of ongoing AML transaction monitoring. Use of these databases in transaction monitoring enables the bank to screen their own customers against the latest data whenever they make a transaction, as well as to check external counterparties to transactions. To make the best use of enhanced compliance databases in ongoing monitoring, financial institutions must be scrupulous in uploading the latest version of these databases as soon as they are updated by the provider.

Optimized Sanctions Watchlists

Sanctions compliance requires filtering the message information in a payment in real time or near real time. Screening against the massive amounts of data in enhanced compliance databases is difficult in this environment, although some high performance watchlist filtering software products are able to meet this challenge. In addition, though, using the wide-net approach of enhanced databases for sanctions filtering can produce large numbers of false positives, putting a drain on analyst resources as well as threatening the very ability to process payments in a timely manner.

While an enhanced database may contain 100,000s of names, more banks are using lists purposed specifically for sanctions compliance with a much smaller data set of, say 20,000 - 50,000 entities. A more focused list will, ideally, enable faster, more efficient and more accurate sanctions filtering. As a result, banks have been moving to running

only official watchlists, supplemented by internal lists, for sanctions compliance, and seeking such optimized versions of the regulatory watchlists from commercial watchlist providers.

- **Sanctions Compliance.** Banks have sometimes taken a wide-net approach even to sanctions filtering, scanning payments against the very large PEP and other commercially provided databases. As they seek greater efficiency in the process, banks have been restricting the lists they use for sanctions compliance to the explicit regulatory requirement of ensuring payments involving sanctioned entities are blocked.
- **Embargo.** At the same time, banks must ensure they are not doing business with entities on regulatory watchlists. As a result, just as they must screen outgoing payments against regulatory watchlists, banks screen new as well as existing customers against these watchlists. In order to process new accounts quickly, some banks have taken the approach of using data sets containing only the regulatory watchlists—for example, a bank in Germany might use only the EU and OFAC lists—specifically to check for embargoed entities in real time at account opening. The bank may run this targeted real time check and the fuller, batched PEP / risk assessment check used for risk profiling / CDD off the same system.

As a result of these trends, the need for optimized sanctions watchlists is growing in both the sanctions filtering and customer embargo areas of compliance.

Looking Forward

Because watchlist data is used across the entire AML compliance cycle, maintaining this data is a particular challenge for large banks. This study has looked at how banks are tackling this issue through promoting enterprise-wide, global standardization of their processes, technology and data, with a focus on sanctions compliance. Some of the achievements described in this report have been quite remarkable. But by the banks' own admission, globally integrated and standardized sanctions compliance is still an ambition that has not been fully realized.

This means that we will see continued and ongoing evolution in processes and best practices in global sanctions compliance, as well as delivery through increasingly comprehensive enterprise-wide platforms.

While some banks feel they have the data management aspect under control, others see watchlist maintenance as a burden incurring significant cost and effort, not to mention the need to fulfill specialized requirements such as non-Latin scripts. List management is complicated and challenging; a watchlist management service can be part of the solution. Based on our conversations with banks for this study, Celent believes that firms that are now managing their watchlists internally will move to commercial watchlist management services.

Challenges will remain. Some of the pain points next on the horizon will be effectively integrating watchlist services with internally developed lists, as well as supporting the myriad local regulatory lists that large banks need to support their extensive regional operations.

The major challenge, though, will of course remain how to keep up with the pace of regulation, and on a global scale. AML regulation will not remain an issue of home market rule. Regulations will continue to fan out from the US, UK and EU to be adopted by jurisdictions around the globe. Issues such as ultimate beneficial owner (UBO) and enhanced diligence for regional hotspots are taking on a global scope. The ongoing march of global regulation will ensure that global sanctions compliance will remain an issue of concern.

Leveraging Celent's Expertise

If you found this report valuable, you might consider engaging with Celent for custom analysis and research. Our collective experience and the knowledge we gained while working on this report can help you streamline the creation, refinement, or execution of your strategies.

Support for Financial Institutions

Typical projects we support related to [insert report topic here] include:

Vendor short listing and selection. We perform discovery specific to you and your business to better understand your unique needs. We then create and administer a custom RFI to selected vendors to assist you in making rapid and accurate vendor choices.

Business practice evaluations. We spend time evaluating your business processes, particularly in [list several here]. Based on our knowledge of the market, we identify potential process or technology constraints and provide clear insights that will help you implement industry best practices.

IT and business strategy creation. We collect perspectives from your executive team, your front line business and IT staff, and your customers. We then analyze your current position, institutional capabilities, and technology against your goals. If necessary, we help you reformulate your technology and business plans to address short-term and long-term needs.

Support for Vendors

We provide services that help you refine your product and service offerings. Examples include:

Product and service strategy evaluation. We help you assess your market position in terms of functionality, technology, and services. Our strategy workshops will help you target the right customers and map your offerings to their needs.

Market messaging and collateral review. Based on our extensive experience with your potential clients, we assess your marketing and sales materials—including your website and any collateral.

Related Celent Research

Trends in Anti-Money Laundering 2011
Neil Katkov, PhD

IT Spending in Financial Services: A Global Perspective
Jacob Jegher

Enterprise Operational Risk, Compliance, and Governance Solutions: Towards a Convergence End Game
Cubillas Ding

Internal Fraud: Big Brother Needs New Glasses
Jacob Jegher

Insurance Fraud Mitigation Technology: Beyond Red Flags
Donald Light

Copyright Notice

Prepared by

Celent, a division of Oliver Wyman

CELENT

For more information please contact info@celent.com or:

Neil Katkov

The Imperial Hotel Tower
13th Floor
1-1-1 Uchisaiwai-cho
Chiyoda-ku, Tokyo 100-0011 Japan

+81 3 3500 3034

nkatkov@celent.com

North America

USA

200 Clarendon Street
Boston, Massachusetts 02116
Tel.: +1.617.262.3120
Fax: +1.617.262.3121

USA

1166 Avenue of the Americas
New York, NY 100136
Tel.: +1.212.541.8100
Fax: +1.212.541.8957

USA

Four Embarcadero Center, Suite 1100
San Francisco, California 94111
Tel.: +1.415.743.7900
Fax: +1.415.743.7950

Europe

France

28, avenue Victor Hugo
75783 Paris Cedex 16
Tel.: +33.1.73.04.46.20
Fax: +33.1.45.02.30.01

United Kingdom

55 Baker Street
London W1U 8EW
Tel.: +44.20.7333.8333
Fax: +44.20.7333.8334

Asia

Japan

The Imperial Hotel Tower, 13th Floor
1-1-1 Uchisaiwai-cho
Chiyoda-ku, Tokyo 100-0011
Tel: +81.3.3500.3023
Fax: +81.3.3500.3059

China

Beijing Kerry Centre
South Tower, 15th Floor
1 Guanghua Road
Chaoyang, Beijing 100022
Tel: +86.10.8520.0350
Fax: +86.10.8520.0349

India

Level 14, Concorde Block
UB City, Vittal Mallya Road
Banglalore 560 001
Tel: +91.80.40300538
Fax: +91.80.40300400

A member of the Oliver Wyman Group