ICO

IRISH COMPLIANCE QUARTERLY

Winter 2017

AML CULTURE

MANAGING FINANCIAL SANCTIONS RISK

THE VOICE
Compliance Issues & Topics

PSD2
The Game Changer for Payments

ACOI CONFERENCE 2017
Compliance & Your Reputation

ACOI
Conferring 2017

COVER STORY

Ed Sibley

THE DIVERSITY & CULTURE CHALLENGE

MiFID II
CPC Addendum

THE ART OF MEDIATION

ACOI
The Association of Compliance Officers in Ireland

Managing Financial Sanctions Risk

The imposition of sanctions on a business can be catastrophic and it is incumbent on businesses, particularly those in the financial services industry to understand their actual risk and be clear of the expectations of the regulators when it comes to ensuring what they do to mitigate the risk is appropriate and effective.

Sanctions are considered an alternative to military force with the purpose of curtailing certain activities such as terrorism, military activity or human rights violations. They are restrictive measures implemented by international bodies such as the European Union (EU), the United Nations (UN), HM Treasury and the US Office of Foreign Assets Control (OFAC).

"Whether you represent a large scale international bank or a smaller scale local business, there is nowhere to hide from the Sanctions regime. "

Whether you represent a large scale international bank or a smaller scale local business, there is nowhere to hide from the Sanctions regime. Making sure you are not associated with names on the sanctions lists or sanctioned countries is critical. The sanctions lists are made up of names of individual people, company names and other entity names such as charities and terrorist organisations, etc. As the Central Bank of Ireland (CBI) states: "All natural and legal persons are obliged to comply with financial sanctions and can do so by monitoring the EU and UN lists and taking appropriate action as required (https://www.centralbank.ie/regulation/how-we-regulate/international-financial-sanctions). You don't want a sanctioned individual or entity as your customer, you don't want to process a payment for them, you don't want to make funds available to them – a bank loan, an insurance policy pay-out, lodging funds into an account for them, paying them for services carried out, etc. These are all prohibited and can result in significant penalties for your organisation. In addition to fines, breaching Sanctions regulations can result in significant reputational damage, criminal proceedings, financial loses, and sanctioning. If you do come across sanctioned individuals/entities, you need to make sure the appropriate procedures are in place for managing the risk, i.e. freezing funds and reporting to the relevant authorities.

What can you do to manage your exposure?

Automated solutions are a key consideration in the identification of sanctioned names on an ongoing basis and while automation is not in any way a legal requirement, in higher-volume environments it may be the only practical solution. Automated sanctions screening can be defined as the use of a technology solution to compare customer names and/or payment information against sanctions lists with the purpose of finding sanctions related activity. The level of automation can range from a user typing the name into the system for comparison against the sanctions lists, to names being automatically passed from your customer system to the screening system for automated checking.

Screening solutions are typically designed to look for possible matches, they are not focused solely on exact matches - this allows for variations in name spellings, typos, use of initials, etc. When a possible match is identified, this will require manual investigation to determine if it is an actual match or whether it can be discounted as a 'false positive'. For example, after investigation the following might be discounted due to a different date of birth or country of residence - Jared Ahmad V's Jarad Ahmad.

As mentioned, no regulator to date has mandated automated screening, it is left up to the individual organisations themselves to determine the appropriate approach to managing sanctions risk. The regulators do provide varying levels of guidance in relation to the use of automated screening solutions, the following are some key themes and expectations:

If you are going to do it, then do it properly;

- **OFAC** – "If your bank does not block and report a transfer and another bank does, then your bank is in trouble" (OFAC Regulations for the financial community 2012);

Know and understand what you are doing;

- **Financial Conduct Authority (FCA)** – "Many banks did not understand how the systems they used had been calibrated and at what thresholds 'fuzzy matching' had been set. We expect banks to understand the systems they use to ensure they mitigate risk as intended." (FCA - How small banks manage money laundering and sanctions risk Update November 2014);

Ensure that the system has been fully tested at the outset and that assurance testing is conducted on a regular basis;

- **CBI** – "the Central Bank expects that firms conduct regular IT assurance testing" (2015 - Report on Anti-Money Laundering/Countering the Financing of Terrorism and Financial Sanctions Compliance in the Irish Banking Sector).
- **Department of Financial Services NY (DFS)** – "shall include the following attributes …[…] …end to end pre and post implementation testing of the Watchlist Filtering program" (Part 504 Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications).

Fuzzy matching should be implemented (i.e. methods of non-exact matching);

- **Joint Money Laundering Steering Group (JMLSG)** – "It is important to consider "fuzzy matching", as names might be missed if only exact matches are screened" (JMLSG – Part 3 Chapter 4).

Former president of Zimbabwe, Robert Mugabe, (pictured below on the left), encouraged the violent seizure of white-owned land from 2000 onwards. Food production was severely impacted, leading to famine and drastic economic decline in Zimbabwe which ultimately resulted in international sanctions.

How do you avoid the fines and consequences?

Understanding your risk is fundamental to ensuring your overall approach to managing sanctions is appropriate and will stand up to scrutiny by both internal auditors and external regulators. A Board mandated Sanctions framework including a Sanctions policy, Standards and a completed Sanctions Risk Assessment are essential for defining your sanctions strategy. This process of documenting your sanctions risk will solidify your requirements and determine whether an automated screening solution is a necessity; this can support the business case to secure necessary budget for implementing and maintaining a solution.

Implementing any technology solution can be a daunting process, adding Sanctions into the mix can seriously heighten the pressure but standard project rules still apply – ensure the right resources are in place, requirements are documented, a project plan is in place, and the risks are identified and managed closely, etc. Specifically, for a sanctions screening solution there are some unique requirements which must be considered, these include:

Sanctions Lists – What lists will you screen against? Where will you source them from, how frequently will list updates be made to the system, what controls will be in place to ensure the lists are complete and up to date on an ongoing basis? Can an internal black list be implemented on the system?

System Tuning and Fuzzy Matching Capability - How do you know the system will be effective at matching before you buy? What testing can you carry out? What are your expectations of matching levels – would you expect for example a match between "Charles Taylor" and "Charles T" to generate a report for manual review? How easy is it to tune the system on an ongoing basis? What level of false positives might you expect the system to generate? These must all be aligned to the internal risk appetite.

Case Management functionality - Can the rationale for the decision regarding the potential match be adequately recorded and is there an effective audit trail? Can a '4 eye process' be implemented allowing two people to add comments/ record actions if required? What management information reports are available on the system?

Resourcing - Who will be the business owner – regulators will expect the compliance/AML function to have clear lines of responsibility (and understanding) albeit the IT function may be responsible for the day to day running of the system.

System reliability & performance – How reliable is the system given the real-time requirements of payment screening and customer onboarding? What service level agreements are in place with IT for issue resolution? Has the business continuity plan been formally approved? Will the system cater for larger peak volumes of traffic (for example increase in payments being sent over Christmas period)? Has someone been assigned the role of relationship manager responsible for liaising with the software vendor on a regular basis?

> ***"To date there have been many fines and reprimands issued to banks and companies regarding failings in their management of sanctions risk. These have predominantly been issued by OFAC but the FCA has also been active ."***

To date there have been many fines and reprimands issued to banks and companies regarding failings in their management of sanctions risk. These have predominantly been issued by OFAC but the FCA has also been active. An example of a non-bank fine is the case of an American seed company which settled a potential civil liability for alleged violations of the Iranian transactions and sanctions regulations. They apparently violated the relevant regulations "by indirectly exporting seeds, primarily of flowers, to two Iranian distributors on 48 occasions" which resulted in a $4.3m fine (https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20160913_panam.pdf). In addition, a recent bank fine was a $2.4m settlement by a bank a for processing 159 transactions for or on behalf of corporate customers that were owned 50 percent or more, directly or indirectly, by a person identified on the OFAC list of Specially Designated Nationals and Blocked Persons (the SDN List) (https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20160208_barclays.pdf).

The following includes an overview of the themes and important lessons for firms emanating from the fines to date:

- Any attempt or help to circumvent Sanctions regulations will result in severe penalties.
- Timely remediation of issues is essential, the longer the delay in addressing the issues the higher the fine.
- Ensuring staff involved in the Sanctions review process are adequately trained is central to ensuring the risk can be managed properly - this goes beyond those staff investigating the screening system outputs and includes for instance staff responsible for account opening, setting up payment requests etc.
- Missing a match due to poor matching capability or poor tuning of the fuzzy matching capability can be a costly mistake.
- It is of limited value screening your customer if you are not also screening their related beneficial owners and relevant directors.
- Lack of adequate assurance processes to ensure systems and processes are working effectively will be detrimental – do not rely on assurances and testing carried out at the time of system implementation. Regular on-going assurance testing is a must.

Regardless of the scale of your business and the scale of the solution in place to manage your Sanctions risk, understanding your actual risk and being clear of the expectations of the regulators are key tools for ensuring what you do is appropriate and effective. In essence, keep your risk assessment current such that you are proactive rather than reactive to any necessary change.

Sarah Connolly, AML Business Unit Manager Ireland, SQA Consulting on behalf of the AML Working Group. ICQ