

# Sanctions Screening - the quest for efficiency and effectiveness



more efficient  
more effective



## CONTENTS

---

03 INTRODUCTION

04 THE 2010 FINANCIAL CRIME THREAT

05 THE REGULATORY MINEFIELD

06 THE OPERATIONAL STRUGGLE

08 TAKING AN INTELLIGENT APPROACH TO SANCTIONS FILTERING

10 CONCLUSION

## INTRODUCTION

---

When it comes to filtering payments against sanctioned entities, banks today are finding themselves in a catch 22. As with most other forms of crime, sanctioned entities are averting prevention methods through increasingly more sophisticated approaches, designed to keep their misconduct firmly under the radar. While banks are also advancing their own strategies to detect illegally moving money, simply preventing it from being laundered isn't the only challenge they face. The following list names just a few of the challenges facing banks today when it comes to sanctions screening:

- The rise of organized financial crime
- The threat of higher fines & higher profile penalties
- Increased regulatory demands
- Disjointed & ambiguous regulatory approaches
- Increased volumes that need to be scanned
- The need to manage multiple sanctions lists
- Restrictions of reduced or limited budgets
- Communication breakdown between bank subsidiaries & departments
- Inefficiencies in payments filtering operations
- The risk of human error in payments filtering

The issues listed above are all inter-linked. As the sanctions environment presents new and increasing threats, the regulators have to clamp down further with more stringent demands and higher fines. This means tougher regimes for banks to follow and a subsequent vast operational burden. This report will explore these challenges in greater detail, before looking at how banks can best address them by increasing both their efficiency and their effectiveness.



## Fine lines in the system can allow criminal behavior to slip through the net.

### THE 2010 FINANCIAL CRIME THREAT

---

While September 11th was certainly the catalyst for the highly regulated environment we find ourselves in today, new criminal and terrorist activity reinforce the fact that financial crime is a persistent, global problem. Authorities are still trying to work out how Nigerian Umar Farouk Abdulmutallab, who was charged with trying to blow-up a transatlantic jet on Christmas Day 2009, was able to fly. He wasn't listed on the no-fly lists, but just one month earlier he had been added to a watch list kept by the U.S. National Counterterrorism Center. This is just one example of how fine lines in the system can allow criminal behavior to slip through the net.

In banking it's a similar story, which is why sanctioned entities are still using banks to illegally transfer money from A to B. A good example is how British bank Lloyds and Swiss banking group Credit Suisse aided the illegal transfer of Iranian money into the U.S. State-owned Iranian banks Saderat and Melli had been sanctioned by the U.S. due to their ties to terrorism and nuclear proliferation, respectively. However, the rogue banks had been able to infiltrate the U.S. financial system for years through Lloyds and later through Credit Suisse. The banking giants were able to do this by creating new SWIFT payments messages, which eliminated any reference to the sanctioned Iranian entities. Their punishment? A \$350 million fine for Lloyds and a \$536 million fine for Credit Suisse – not to mention the cost of severely damaged reputations.

In the case of Credit Suisse, these sanctions violations spanned an entire decade. This indicates that – even though such cases don't come to light every day – we probably only know about the tip of the financial crime iceberg.

The fact that money laundering is a very serious criminal activity is reaffirmed by the Europol Organised Crime Threat Assessment, disclosed in October 2009. The report ranks money laundering as one of the six most significant criminal sectors and acknowledges how regulation has forced criminals to smuggle cash across several jurisdictions in order to place it securely and accessibly. It also notes how organized crime invests into cash-rich legitimate business, camouflaging crime profits within the flow of cash generated by these legitimate activities and falsifying their accounting accordingly. Moreover, financial crime activity today is most commonly made through a high volume of low value transactions in order to go unnoticed.

Regulation has undoubtedly made a very positive impact in the prevention of financial crime – not just in relation to terrorism, but other criminal activity such as drug trafficking, people trafficking and intellectual property theft. However, as noted by Celent analyst, Dr. Neil Katkov, AML programs required by regulators in the U.S. and many other countries are a headache for banks. Now, as regulators increase pressure by emphasizing that the risk-based approach used to monitor suspicious activity is not sufficient for sanctions, the headache is set to get worse.

Immense transaction volumes now need to be scanned against dozens of ever-changing watch lists, containing tens of thousands of sanctioned entities.

## THE REGULATORY MINEFIELD

---

Whether a financial institution is regional or global, today there are multiple and varying jurisdictional requirements to adhere to. The U.S. Treasury's Office of Foreign Asset Control (OFAC) still bears the sharpest teeth in terms of fines and geographical reach. It has the right to act wherever there is U.S. involvement and therefore even non-U.S. banks fall into its jurisdiction. In August 2009, for instance, the Australia and New Zealand Bank Group received a large fine from OFAC for violations of the U.S. Sudanese Sanctions Regulations and the Cuban Assets Control Regulations. Economic, trade and financial sanctions, however, are also imposed by other governments as well as the UN. This means the compliance task is vast in nature, making it increasingly difficult for banks to avoid penalties.

While the Financial Action Task Force (FATF) has created an international standard for the risk assessment of both cross-border and domestic transfers, individual country approaches still mean that AML regulation is a fragmented landscape. The European Union (EU) is a prime example of this. Its Economic and Financial Affairs Council (Ecofin) will work to establish common regulatory and supervisory standards and practices. It will therefore investigate each member state's AML practices. While this will help create further standardization, without a central EU sanctions reporting body in place, true uniformity cannot be achieved. For instance, if a bank in Italy violates a sanction in Italy, it will report to the Bank of Italy. However, if the same bank violates a sanction in the UK, it will report to the Bank of England.

A similar argument could be made for other regions. In Asia, the Asia/Pacific Group on Money Laundering consists of 40 members committed to implementing the FATF's international standards for anti-money laundering and combating financing of terrorism. However, each member country will have its own sanctions lists and its own reporting bodies. In South America, the Financial Action Task Force of South America consists of ten member countries. This group has been set up to develop and implement a comprehensive global strategy to combat money laundering and terrorist financing as set out by FATF.

These collaborative governance efforts are certainly a step in the right direction – they suggest that most countries around the world are turning to the same page. But what they don't do is solve the issue of the complex compliance mesh for banks – many of which have to recognize FATF standards as well as comply with country-specific requirements. The result is a continual struggle to keep up with the regulations, which compounds the challenge to understand them in the first place. In many cases, the regulatory direction given to banks about what they can and can't do isn't clear cut. It's open to a degree of interpretation, which will differ according to the risk adversity of each institution.

Perhaps even worse than this complexity and ambiguity, however, are the immense transaction volumes that now need to be scanned against dozens of ever-changing watch lists, containing tens of thousands of sanctioned entities.

If banks can reduce false positive alerts, they can substantially drive down costs and use their resources in a more productive way.

## THE OPERATIONAL STRUGGLE

---

In support of tougher regulation and as a result of the globalization of the payments landscape, many ACH transactions that were once considered domestic may now be deemed international. In September 2009, the National Automated Clearing House Association (NACHA) in the US introduced a rule to ensure that more types of payments are scanned. In Europe, the Single European Payments Area (SEPA) scheme also means that banks need to scan increasing volumes of payments – not just cross-border SWIFT messages.

For many banks the volume of domestic payments is between 10 and 100 times greater than the number of cross-border ones. If banks only extend their scanning operations to foreign domestic payments traffic, this will still mean a considerable increase. For many, it could result in hundreds of thousands of additional payments that need to be scanned each day. Even with highly scalable and robust infrastructure in place to automate this, coping with such volumes will require a small army of operations employees to process the payments alerts. It will also lead to spiraling costs.

This model is simply not a sustainable one. Banks view payments filtering activities as a regulatory purpose rather than one that drives business growth, so compliance budgets are stretched at the best of times. Again, we have a catch 22. For banks to drive down the cost of compliance, they run the risk of being less sensitive to potential data matches to sanctioned entities and less thorough. If they choose the most sensitive and effective screening route, they risk negatively impacting their bottom line.

As an example of this conundrum, risk-averse global financial institutions will often scan hundreds of thousands of payments on a daily basis. Of these, their filtering systems will typically identify between 3% and 6% as payments that appear to be high risk. Following further investigation, which in some cases will be carried out by team of over 200 people, 98% of payments originally identified as high risk could turn out to be false positives. An institution scanning 200,000 payments daily could therefore have over 11,000 false positives to deal with every day. If banks in similar predicaments can reduce these false positive alerts, they can substantially drive down costs and use their resources in a more productive way.

Unfortunately, in many cases when banks take measures to reduce the volume of false positives, it comes at the expense of effectiveness. This is because the only way to reduce the hit rate is to increase the thresholds or narrow the search. For example, many banks set their filtering systems to alert payments that have a minimum 80% to 90% match to a sanctioned entity. Increasing the percentage of the match algorithm will enable more payments to slip through the net. This opens up banks to greater risk at a time when operational risk is being tightened. Alternatively, in a bid to achieve straight-through-processing, some banks may only scan parts of the transaction, such as the originator and beneficiary fields. The problem is that this means they run the risk of missing true positive hits elsewhere in the message.



“Bank operations are really facing an uphill battle when it comes to sanctions screening. The need to increase efficiencies and drive down costs is greater than ever, but this becomes almost impossible in light of added pressure from the regulators. To cope with this, banks are going to have to take smarter approach to suspicious activity monitoring and payments filtering – improving both accuracy and productivity at the same time.”

Shaun O’Leary LLB, head of Risk and Regulation, Temple Risk Partnership

True positives continue to be a key focus area for compliance departments, with many seeking the help of auditors to apply academic rules to filter out the matches. However, they are still missed – even with the most diligent approaches – because the art of payments filtering is not a black and white one. Furthermore, there are many aspects of each payment to investigate, all of which might indicate risk with the transaction.

This adds further to the operational burden, which has also been impacted by the new payments landscape. Mobile, contactless and person-to-person payments have all made strong traction in recent years. Gartner has predicted that the mobile payments industry will experience steady growth and that by 2012 the number of mobile payment users will reach more than 190 million. This represents more than three percent of total mobile users worldwide, attaining a level at which it will be considered mainstream.

While these new channels present favorable business opportunities, they also bring a new wave of sanctions screening implications to contend with. For example, Austrac, the Australian financial crime regulator, imposed a deadline on PayPal last year to tighten up its procedures for managing money laundering and terrorism financing risks. This was in light of PayPal’s failure to implement adequate know-your-customer mechanisms for transactions under the A\$1,000 threshold. Such payments, which are low value in nature and often don’t even transact through banking systems, are prime for remaining elusive to filtering efforts.

## Banks can be more effective and efficient when screening against sanctions.

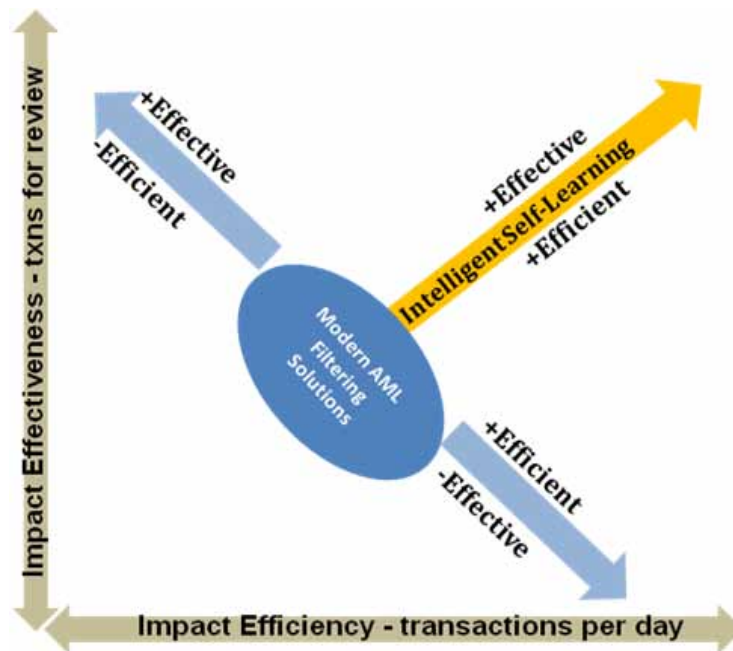
### TAKING AN INTELLIGENT APPROACH TO SANCTIONS FILTERING

Considering the rudimentary payments filtering techniques used by banks a decade ago, great advancements have been made. AML and sanctions screening today feature much higher on the priority lists and the financial landscape is generally more risk-averse. However, when compared to the real-time and highly robust capabilities found in many front office systems, compliance still has some way to go. All too often banks need to apply a high proportion of manual resource to their sanctions filtering operations, as a result of technology that doesn't fit the bill and simply can't scale appropriately.

While many institutions are achieving compliance, it doesn't necessarily mean they're doing this well. In Europe, the transposition of the 3rd AML Directive appears to have been successful, with all but two countries having implemented this. However, it's likely that most banks in these countries will still have relatively weak and inflexible systems in place – resulting in high costs and complexities. Unsurprisingly, last year the U.K.'s Financial Services Authority called for improvements to be made to sanction screening systems and controls. It also claimed there was not sufficient understanding of sanctions regulation or the importance of both suspicious activity monitoring and payments filtering. As we move further into this new decade, many banks will therefore be looking to redress their strategies.

When taking a fresh approach to sanctions screening, banks should take into account the regional cross-over of the regulatory landscape. A centralized regional or global payments filtering hub will help address this. It will also bring further lucrative benefits to the table, in terms of greater efficiencies, reduced operational risk and, ultimately, lower costs. In addition to centralization, the scalability of a bank's sanctions screening must also be called into question. Systems should now be able to accurately filter millions of payments messages each day, checking every field of each transaction against the watch lists. Given the speed at which funds can be moved, scanning must also be in real-time. Moreover, with each institution having slightly different regulatory requirements to adhere to and a unique organizational structure, sanctions screening technology must be tailored to each specific firm.

One tangible and straightforward way to gain positive results in sanctions screening, which few banks have yet realize, is to reduce the relentless volume of false positive alerts without impacting the level of filtering diligence and accuracy. This can be achieved by applying filtering technology that intuitively self-learns from users' previous actions. It is therefore able to recognize more payments that should in fact be passed that once might have been categorized as a positive by less sophisticated systems. Such a solution has been proven to reduce false positive alerts by more than 50%, while maintaining full compliance transparency and without narrowing the filtering net. Not only does this save costs by massively reducing manual checking and keeping alerts to a manageable amount, but it also decreases the compliance burden. It means that banks can be both effective and efficient when screening against sanctions



“Over the last two years we have reviewed a number of live AML systems around the world. The analysis from this was clear – there is one major factor restricting performance across the market. Looking at the diagram above, there are only so many parameters that can be changed on these systems. The impact of this change either improves efficiency at the cost of effectiveness or vice versa. Nothing has enabled the improvement of both at the same time with software solutions available today. This has been the conundrum that we have been working on solving at Logica.”

Tim Brew, market development director, Logica

## CONCLUSION

---

It's not often that the words 'innovation' and 'compliance' are included in the same sentence. However, the fact that sanctions screening effectiveness and efficiency are not mutually exclusive means that sanctions compliance has made a positive, innovative step forward. This is a timely advancement given that it's more important than ever for banks to contain the cost of compliance

Coupled with scalable, real-time flexible filtering solutions, this technique to reduce false positives allows banks to truly benefit through improved operations. This will enable them to avoid heavy penalties and protect their reputations, which for many banks is foremost in light of the industry's damaged profile.

Looking back at the list of sanctions screening challenges in the introduction, they certainly won't be eliminated any time soon. However, it's clear that the right sanctions approach combined with the right technology can certainly lessen their impact on banks today.



## CALL TO ACTION

Intelligent Self-Learning (ISL) Solution is an innovative new product that reduces false positive alerts in sanctions filtering by more than 50%, without reducing the accuracy or narrowing the net.

Let us demonstrate how ISL can help you.

Schedule an appointment: contact us at [globalproducts@logica.com](mailto:globalproducts@logica.com)

---

Logica is a business and technology service company, employing 39,000 people. It provides business consulting, systems integration and outsourcing to clients around the world, including many of Europe's largest businesses.

Logica creates value for clients by successfully integrating people, business and technology. It is committed to long term collaboration, applying insight to create innovative answers to clients' business needs.

Logica is listed on both the London Stock Exchange and Euronext (Amsterdam) (LSE: LOG; Euronext: LOG).

More information is available at [www.logica.com](http://www.logica.com)

This document is for general information purposes only and is subject to change without notice.

---

Copyright © 2010 Logica

All rights reserved. This document is protected by international copyright law and may not be reprinted, reproduced, copied or utilised in whole or in part by any means including electronic, mechanical, or other means without the prior written consent of Logica.

Whilst reasonable care has been taken by Logica to ensure the information contained herein is reasonably accurate, Logica shall not, under any circumstances be liable for any loss or damage (direct or consequential) suffered by any party as a result of the contents of this publication or the reliance of any party thereon or any inaccuracy or omission therein. The information in this document is therefore provided on an "as is" basis without warranty and is subject to change without further notice and cannot be construed as a commitment by Logica.

---

Logica  
Tel: +44 (0) 207 637 9111  
[globalproducts@logica.com](mailto:globalproducts@logica.com)

[www.logica.co.uk](http://www.logica.co.uk)

CODE 011 0310

AUSTRALIA / BELGIUM / BRAZIL / CANADA / CZECH REPUBLIC / DENMARK / EGYPT / ESTONIA / FINLAND / FRANCE  
GERMANY / HONG KONG / HUNGARY / INDIA / INDONESIA / KUWAIT / LUXEMBOURG / MALAYSIA / MOROCCO  
NETHERLANDS / NORWAY / PHILIPPINES / POLAND / PORTUGAL / RUSSIA / SAUDI ARABIA / SINGAPORE / SLOVAKIA  
SPAIN / SWEDEN / SWITZERLAND / TAIWAN / UKRAINE / UNITED ARAB EMIRATES / UK / USA