

# Sanctions screening in Asia-Pacific – 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

07 SCREENING & THE NEW PAYMENTS LANDSCAPE

08 TAKING AN INTELLIGENT APPROACH TO SANCTIONS FILTERING

10 CONCLUSION

## INTRODUCTION

---

When it comes to filtering payments against sanctioned entities, banks in Asia-Pacific (APAC) – many of which are only just putting AML measures in place – are finding themselves in a catch 22. As with most other forms of crime, sanctioned entities are trying to avoid detection through increasingly more sophisticated approaches, designed to keep their misconduct firmly under the radar. Banks in APAC are also advancing their own strategies to detect illegally moving money, although 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:

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

The issues listed above are all inter-linked. As the sanctions environment in APAC presents new and increasing threats, the regulators are turning their attention to this region with stringent demands and high 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 reinforces 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 in APAC is reinforced by an Interpol paper entitled, 'Alternative remittance systems distinguishing sub-systems of ethnic money laundering in INTERPOL member countries on the Asian continent'. The report states that illicit proceeds, which are later laundered, are produced by criminal activity in the area, particularly from the drugs trade. Central Asia, the Golden Triangle, and the Golden Crescent are major centers for the manufacture of heroin, opium, marijuana, and methamphetamine. The report also notes that criminal income is also generated by Asian-oriental organized criminal involvement in prostitution, human traffic, gambling, kidnapping, extortion, and drug trafficking. The report suggests that one of the reasons for the money laundering boom is the lack of regulatory controls and legal provisions in some of the territories.

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 local, regional or global, today there are multiple and varying jurisdictional requirements to adhere to – and APAC is no exception. Here, 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.

OFAC has put pressure on local regulators in APAC to tighten up their AML regimes, and many have responded to this. Some have required financial institutions in the region to undertake self-assessment exercises and conduct focused regulatory examinations, which have served to reduce penalties dealt in several cases. However, OFAC's dominance in the region often over-rides the domestic authorities in APAC, with many firms choosing to prioritize its requirements over local ones.

The Financial Action Task Force (FATF) aims to address AML inconsistencies across the globe and has created an international standard for the risk assessment of both cross-border and domestic transfers. The Asia/Pacific Group on Money Laundering consists of 40 members committed to implementing the FATF's standards. However, individual country approaches make AML regulation highly fragmented. The result is a continual struggle to keep up with the regulations, which compounds the challenge of understanding 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 therefore 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

---

We're seeing new requirements – across the globe – for banks to scan cross-border payments as well as domestic traffic. 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.

For banks in APAC, operational challenges are also caused by language differences. Most sanctions lists are in English, which means that names in local APAC languages should technically be translated into their English equivalents and then scanned. In Japan, the Ministry of Finance sanctions lists contains details in Kanji and Katakana as well as in English, so the banks themselves don't have to do this.

While the translation of names on the watch lists is beneficial for Know Your Customer (KYC) purposes, for payments filtering, it means there will be more names to scan and more possible matches to sanctioned entities. Banks will therefore have to follow up more payments for further investigation – costing them time and money.

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 each day. 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, opening up banks to greater risk. 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. This means they run the risk of missing true positive hits elsewhere in the message.

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.



“Increased pressure from regulators to improve sanctions filtering and the need to drive down costs through greater efficiencies, means banks will need to rely on filtering tools that save time. In parallel they need to ensure that resources are being used to prevent violation of sanctions. Filtering systems that reduce false positives in screening payments will be critical for large banks seeking to optimize productivity and gain the most accurate results.”

Dr. Neil Katkov, senior vice president at Celent

## SCREENING & THE NEW PAYMENTS LANDSCAPE

---

The operational and regulatory issues surrounding sanctions screening are further impacted by the new payments landscape. Mobile, contactless and person-to-person payments have all made strong traction in recent years, especially in APAC. 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 instance, there is currently very little AML governance over the expanding pre-paid cards market.

Technically, it is the onus of the organization that the payment is initiated through to carry out the necessary KYC checks. Telcos, for example, should have conducted KYC on each customer, which means that they don't need to scan each and every mobile payment. Interestingly, 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 KYC 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.

Worker remittances – a large and still-growing market – further complicate matters. The informal, and sometimes illegal, ways that money is moved around the globe continue to bypass any form of regulation. Mobile payments, which are heavily targeted at the unbanked, provide another cross-border capability for remittances. At the same time, they also create the perfect environment for money laundering and terrorist financing.

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

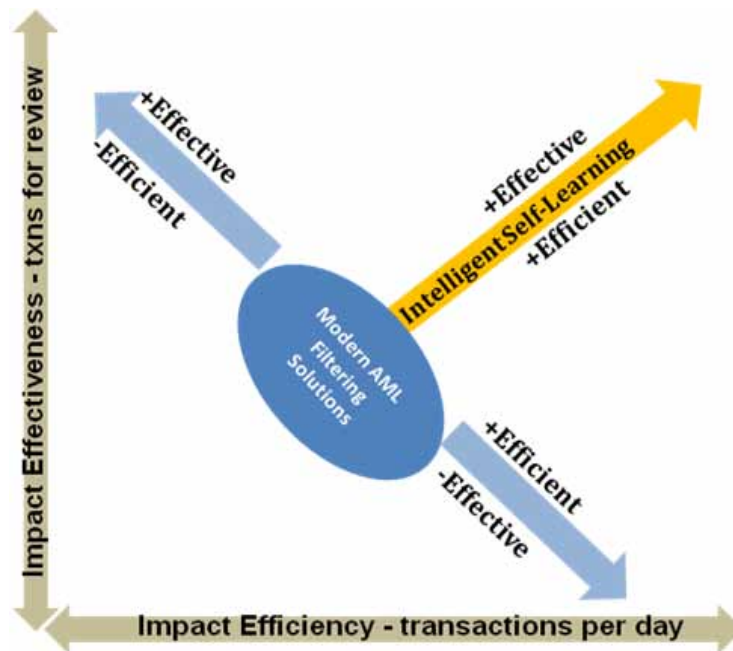
### TAKING AN INTELLIGENT APPROACH TO SANCTIONS FILTERING

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 APAC 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 in APAC are now achieving compliance, a large proportion still have relatively weak systems in place – as has been noted by FATF. As we move further into this new decade, many banks – particularly those looking to expand their regional footprint – 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 in APAC 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 which 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 in APAC 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