Monetary Authority of Singapore

SOUND PRACTICES TO COUNTER PROLIFERATION FINANCING

August 2018

Contents

1 Introduction

1.1 International efforts in countering proliferation financing ("PF") have intensified in response to the nuclear weapons programmes of Iran and the Democratic People's Republic of Korea ("DPRK"). On top of list-based targeted financial sanctions, the United Nations Security Council ("UNSC") has used activity-based financial prohibitions and economic/sectoral sanctions to augment the tools to combat PF. In addition, the Financial Action Task Force ("FATF") and the UN have issued various reports highlighting PF typologies and the techniques used by proliferators to evade sanctions.

1.2 Addressing PF risk is a priority for the Monetary Authority of Singapore ("MAS")[1] and an integral part of Singapore's efforts to safeguard the integrity of our financial centre. To this end, financial institutions ("FIs") play important roles as gatekeepers. MAS requires senior management of FIs to set the tone from the top, and to put in place adequate control measures to mitigate this risk.

1.3 MAS conducted a series of thematic supervisory visits to selected banks between December 2017 and May 2018. The discussions were focussed on (i) understanding how banks ensure the effectiveness of framework and controls for countering PF, (ii) approaches to identify and monitor higher risk customers and transactions, as well as (iii) governance oversight, risk awareness, staff accountability and communications in relation to sanctions risk detection and mitigation. The discussions also centred around common typologies (referred in the box below, with some related red flag indicators at the Annex) and the need for banks to be vigilant in detecting sanctions evasion.

1.4 This paper[2] does not create new obligations on FIs and is intended to clarify how effective PF risk management and compliance with existing legal obligations can be achieved in light of evolving typologies. It summarises the key findings from the recent MAS thematic supervisory visits on countering PF, and elaborates on sound practices observed, for FIs to use as benchmarks to enhance their existing controls and practices. Case studies have also been

[1] The MAS has issued regulations pursuant to section 27A of the MAS Act to discharge Singapore's obligation to comply with UNSC Resolutions ("UNSCRs"). These regulations include MAS (Sanctions and Freezing of Assets of Persons – Iran) Regulations 2016 and MAS (Sanctions and Freezing of Assets of Persons – Democratic People's Republic of Korea) Regulations 2016. These regulations apply to all banks and other financial institutions ("FIs") regulated by MAS, and are aligned with the FATF Recommendations. MAS has also provided guidance to FIs through regular engagement and in the Guidelines to the MAS Notices on the Prevention of Money Laundering and Countering the Financing of Terrorism ("MAS Guidelines").

[2] This paper supplements the existing MAS Guidance on Proliferation Financing. FIs should also refer to FATF's 2018 "Guidance on Counter Proliferation Financing – The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction". The AML/CFT Industry Partnership ("ACIP") paper on Legal Persons - Misuse Typologies and Best Practices (May 2018) is also provides relevant best practices and recommendations to improve detection of misuse of legal persons or shell companies typologies, which are commonly used to evade PF-related sanctions.

used throughout the paper, to illustrate and provide context on how the banks we visited had enhanced their controls or were effective in the detection and mitigation of sanctions risks.

1.5 While this paper refers mainly to banks, the sound practices described, with the appropriate modifications, would similarly be relevant and applicable to other FIs. FIs should adopt these sound practices where appropriate, giving proper regard to the risk profile of their business activities and customers. The described controls are not intended to be exhaustive.

<u>Some common typologies</u>

(i) Use of shell companies set up by foreign beneficial owners with little or no substantial business operations in Singapore. These foreign beneficial owners typically hold multiple shell companies, including Singapore incorporated ones, with Singaporean nominee director(s). These nominee directors may be used to open bank accounts, which are then used for pass-through transactions or for layering payments.

(ii) Use of Singapore operating companies, including those which are long-established, to trade with sanctioned entities, with transactions layered through front companies and accounts held in third countries. Some companies have also established a separate operating legal entity to ring-fence these illicit business relationships.

(iii) Use of indirect routes, transhipment through third countries and disabling of vessels' automatic identification systems to mask the conduct of sanctioned activities.

2 Effective framework and controls for countering PF risks

2.1 Banks should remain vigilant to the risks of establishing or maintaining business relationships with representatives, nominees or companies, including front or shell companies, which are used to circumvent the UNSC Resolutions ("UNSCRs"). To achieve this, a bank's counter-PF programme should keep pace with changes in regulatory requirements in Singapore, relevant UNSCRs, as well as unilateral sanctions imposed by other countries where they are relevant to the banks' operations.

2.2 Controls should incorporate, on a timely basis, red flag indicators related to emerging sanctions evasion typologies. Such indicators and typologies could be distilled from suspicious transactions reports ('STR")s filed, credible sources for adverse news, information from regulators/law enforcement agencies, and relevant reports from the UN, FATF and other relevant bodies.

Structured Framework to Uplift Controls

2.3 *Key findings:* Most banks that MAS examined have in place a process to perform timely gap analysis of policies, procedures and controls against regulatory changes as well as unilateral sanctions where relevant to the banks' operations. There is room to enhance this practice to better detect sanctions evasion typologies.

Box Story: Examples of controls enhancements to detect sanctions evasion

- *Some banks have enhanced trade finance controls to ensure greater scrutiny of and due diligence on shipping documents, taking a risk-based approach. Enhanced due diligence, such as independent verification of shipping routes and tracking of shipping voyage, is required for transactions involving ports and destinations that pose higher sanctions evasion risk, or involving indirect routes to destinations.*
- *Some banks have also reviewed existing customer due diligence ("CDD") controls to ensure that these controls remain robust and would enable banks to detect front and shell company typologies.*
- *Most banks have, using a risk-based approach, strengthened their CDD controls to include counterparty due diligence checks to better detect indirect sanctions risks.*

2.4 Most banks have articulated in their policies, zero tolerance for sanctions-related activities and have prohibited any direct or indirect dealings with sanctioned entities or countries. Some banks have however not sufficiently made specific, consequential controls enhancements to enable early detection of PF risks via front companies or nominees, though such typologies were highlighted in various expert reports or from the banks' own internal investigations into higher risk customers and their transactions.

2.5 As a good practice, some banks have a structured process, when STRs are filed, to conduct a post-mortem review[3] of controls on a risk-based approach. Specific to STRs filed on PF risks, such a review enables banks to:

(i) identify evolving money laundering ("ML")/terrorism financing ("TF")/PF typologies;
(ii) self-discover control weaknesses; and
(iii) determine enhancements to internal controls and processes to better detect such risks going forward.

2.6 MAS has observed that following such post-mortem reviews of STRs, some banks enhanced the criteria for triggering a review of CDD information, which helped them to better detect shell/front company typologies.

<u>Box Story: How banks have used post-mortem reviews to enhance controls</u>

Case Study A

A bank was alerted to adverse information, which indicated that one of its customers was allegedly involved in PF activities. Based on the bank's records, this customer was in the business of real estate management, with a residential address listed for the business. The bank's transaction monitoring system had previously detected transactions which were not in line with the customer's declared activity. However, these alerts were closed based on the customer's explanation that the company had ventured into a new oil trading business, without obtaining further corroborative documents or conducting CDD review on the customer's new business lines.

After filing an STR, the bank conducted a post-mortem review and enhanced its controls:

(i) CDD refresh and customer risk assessment must be triggered when customers have a significant change in business activity;
(ii) Screening checks must be conducted on the customer's counterparties; and
(iii) Enhanced guidance on when corroborative evidence is required, when reviewing transaction monitoring alerts.

Case study B

One Singapore company was initially set up by a foreign national, who was listed as the company's shareholder and director. Shortly after account opening with the bank, the shares and directorship were transferred to a Singaporean, before the suspicious PF activities

[3] Performed by staff of sufficient independence and experience.

commenced, including transacting with companies that were known DPRK financial facilitators. The bank filed an STR.

The post mortem review conducted by the bank noted that there were indications that the Singaporean was merely a nominee director and that the foreign national continued to be the beneficial owner and ultimate controller of the company. For example, the foreign national was the one replying to queries received from a bank on the company's account, and the foreign national was an authorised internet banking user in the company. The Singaporean nominee director appeared to be unaware of the company's dealings when queried by the bank. Following further checks, the bank found out that this same Singaporean was the nominee director and shareholder of multiple other shell companies linked to the same foreign national.

Consequently, the bank included changes in directors, beneficial owners as well as authorised signatories of accounts as an indicator for triggering CDD reviews. This enables the bank to be vigilant to unusual changes in account ownership and put in place mitigating measures where appropriate.

Sound Practices

- Banks have included new sanctions evasion typologies in the UN Panel of Experts reports, from other credible sources or in information provided by MAS and other relevant authorities, as triggers to identify and address control gaps.
- Banks have in place a risk-based process to conduct post-mortem reviews of STRs filed, to identify and address control gaps.
- Banks have enhanced controls to take a risk-based approach to trigger review of CDD where there are changes in beneficial ownership, directorship or authorised signatories of accounts.

3 Identification of higher risk customers and monitoring transactions

3.1 *Key findings:* MAS found that most banks have enhanced their CDD frameworks and controls to enable timely detection of a sanctions nexus, such as pass-through transactions or indirect trade transactions with sanctioned entities/countries using front/shell companies.

3.2 Some banks have enhanced their CDD checks for higher risk categories of customers, including non-borrowing customers, by obtaining additional information on the customer's business counterparties (such as information on buyer, supplier, vessel and shipping route). These data points help the banks to better assess whether the customer presents any specific sanctions-related risks and take the necessary mitigating or enhanced control measures.

3.3 Most banks have identified PF-related risk indicators to identify customers and their transactions for enhanced due diligence. For example, for trade finance transactions, banks conduct enhanced checks on transactions involving ports and/or goods which pose higher PF risks. Checks to mitigate PF risks include, inter alia, verifying the physical movement of vessels/goods and requiring corroborative documentary evidence for higher risk customers and transactions. Through enhanced vigilance, one bank successfully detected ship-to-ship transfers of oil for the DPRK, even before this typology was known publicly and filed STR.

<u>Box Story: Detection of ship-to-ship transfers</u>

A bank has in place existing controls to conduct Lloyd's List Intelligence ("LLI") and International Maritime Bureau ("IMB") checks on certain shipments involving ports of high sanctions risks. For a particular transaction, the checks indicated that the vessel veered close to the territorial waters of a sanctioned country, a few days after it was loaded with oil cargo. Subsequently, IMB was unable to verify the discharge of cargo at the port listed on the bill of lading provided. The bank filed an STR, and terminated the transaction. Relationship with the customer was also exited.

3.4 Some banks have a dedicated sanctions surveillance team responsible for identifying emerging sanctions evasion typologies, as well as specific customers which could pose PF-related sanctions risks. Such surveillance is typically conducted through reviewing intelligence from various sources, such as information from regulators and law enforcement agencies, adverse news and investigative reports. As a follow up, the surveillance team would trigger a comprehensive bank-wide review, either on a thematic portfolio or customer-specific basis, to assess the risks to the bank and the mitigating controls required.

3.5 As the sanctions nexus may typically not be obvious at the point of onboarding, most banks are proactively reviewing higher risk customer segments to address sanctions evasion concerns. These reviews use various risk factors and customer profiles to address sanctions evasion typologies, including the following non-exhaustive examples:

(i) Customers that previously had dealings with individuals/entities of proliferation or PF concerns[4]. This could include, for instance, customers known to have previously entered into business or joint ventures in countries subject to UNSC sanctions;
(ii) Customers exhibiting potential shell/front company characteristics – this could relate to: (a) dormant company accounts which suddenly become active; or (b) companies with legitimate transactions which were subsequently diverted to support sanctions evasion; or (c) abrupt or unexplained changes in directorship, beneficial owners or authorised signatories;
(iii) Correspondent banking relationships involving higher risk banks bordering sanctioned countries, which are more susceptible to being used to circumvent PF-related sanctions; or
(iv) Customers involved in wholesale trading, brokering or intermediary company, carrying out business inconsistent with normal business or significant changes in business activities.

Such reviews, when well executed, help banks to have a stronger understanding of the PF risks within their business, for commensurate mitigating measures/controls to be instituted.

<u>Box Story: Detecting the use of operating company for sanctioned activities.</u>

A long-established Singapore company with Singaporean beneficial owners was dealing in petroleum and related products. Over the past couple of years, it has been observed that its shareholding and directorships have slowly changed hands to foreign nationals, such that the original Singaporean owners now hold minimal shares. Instead, the foreign nationals have ultimate control over the business, and used the Singapore company's established name to broker illicit transactions to DPRK through third countries.

3.6 To be more comprehensive, some banks conducted retrospective reviews of wire transfer transactions, to identify customers that had previously transacted with individuals/entities of proliferation concern, for closer scrutiny and review. Some banks have also shared with MAS their intentions to leverage artificial intelligence and data analytics to complement their analyses. For instance, the risk indicators in relation to shell/front companies on their own may not be definitive indicators of wrongdoing by the customers. Data analytics have been used by some banks to identify higher risk customers that exhibit a combination of risk factors for further review. Data analytics have also been used to identify customers in higher risk countries, or with shared addresses for the banks' targeted reviews.

[4] As noted from e.g. bank's past interactions with the customer, the UN Panel of Experts' reports, etc.

MAS strongly encourages banks to continue their proactive measures to address emerging typologies and better detect and deter attempts at sanctions evasion.

3.7 Should higher risk customer reviews take an extended period of time to complete, banks are reminded of the risks posed by the transactions undertaken on behalf of those customers. Where banks have identified the customers who pose higher PF-related sanctions risks, appropriate controls should be put in place for risk mitigation. For instance, some banks have in place a control for ex-ante review of all transactions prior to completion of review of higher risk customers, to mitigate any further risk of facilitating direct or indirect[5] PF-related transactions through the bank. The banks would require the purpose and nature of the transactions, including beneficiary/originator of transactions, to be established, prior to execution by the bank.

<u>Box Story: Identifying shell company red flags for conduct of customer reviews</u>

A foreigner was listed as a director/shareholder of several companies, which maintained corporate accounts with a bank. This individual, was in the process of opening a new account with the same bank for another recently incorporated company. During the account opening process, the bank staff escalated the application for further review, given that this individual had multiple corporates listed under his name. Following the staff escalation, the bank conducted a review of all the other related accounts and noted that some accounts were funded by third parties from overseas. An STR was subsequently filed as the bank was unable to ascertain the economic purpose for the flows.

The bank initiated a wider review of its customer base, to identify companies with common beneficial owners, directors or signatories, for assessment (including transactional reviews). This review was further scoped using additional risk indicators such as companies without real business activities in Singapore as well as companies with low level of capitalisation.

Red flags observed

(i) Changes in directors, beneficial owners, or signatories within a short time from incorporation or account opening;
(ii) Use of common directors/shareholders, addresses/telephone numbers, and/or place of incorporation. In some instances, residential addresses are used in place of business addresses; and
(iii) Period of dormancy in account before commencement of unusual activities.

[5] A key prohibition for countries subject to activity-based sanctions under the UNSCRs.

Sound Practices

- Banks have sufficient resources to manage sanctions risks, including having dedicated resources towards sanctions risks surveillance and detection. Risk surveillance further takes into consideration, additional information sources, including credible investigative reports, to identify customers that have been linked to sanctioned entities or used to evade PF-related sanctions.
- Banks have conducted customer reviews, using a risk-based approach, to proactively identify PF-related links in its customer base. These reviews, which takes into consideration all material information on the customer, are conducted as new typologies or risk indicators emerge, that expose the banks to higher sanctions risk. Banks have put in place appropriate case management controls for these higher risk customers, to mitigate risks.
- Banks have enhanced their Know-Your-Customer assessment to include information on counterparties (i.e. information on key suppliers and buyers, vessels and shipping routes), even for non-borrowing trading companies. Where sanctions-related red flags are noted, banks perform further due diligence on these counterparties to augment the bank's understanding of the customer's business profile and sanctions risk assessment. Such information would enable the bank to better identify anomalies in the customer's transactions.
- Banks have identified a list of sanctions risk indicators for trade transactions and/or put in place appropriate transaction trigger thresholds for enhanced due diligence checks.
- Banks perform consolidated account monitoring across customer's accounts, to be vigilant to activities intended to circumvent sanctions prohibition.
- Banks conduct retrospective reviews of wire transfer transactions/cross-border funds flow transactions undertaken to identify customers that pose higher sanctions risk.
- Individuals/entities identified to pose potential sanctions risks are included in banks' sanctions screening watch-list for transaction and wire transfer screenings.
- Banks obtain corroborative evidence for transactions that are not in line with a customer's profile or where the transactions exhibit sanctions-related red flags. For higher risk trade transactions, banks have engaged external intelligence providers to corroborate information provided in the trade documents.

4 Governance, risk awareness, accountability and communication

4.1 *Key findings:* Banks have put in place a governance process for the board of directors and senior management to be adequately apprised of sanctions risks relating to the bank's business. However, in some instances, the timeliness of such escalations needs to be improved. For example, MAS noted that while sanctions risks were identified as part of a bank's review, the bank's board of directors and senior management with ML/TF/PF risk oversight were not kept apprised while the review was ongoing. As a result, the bank's board of directors and senior management were unaware of the significant sanctions risks exposure. This also limited the ability of management to assess the adequacy of risk mitigating measures in place for such higher risk accounts.

4.2 Most banks already incorporate regulatory changes and PF typologies in staff training cycles. There is scope for more timely sharing of new/evolving typologies and red flag indicators, as they emerge, with front line and operations staff. This is important to raise their risk awareness and reinforce staff accountability for managing PF risks. MAS noted some instances where escalation by front office staff on sanctions-related risks were not timely due to staff oversight. These instances point to the need for PF sanctions risk awareness to be further strengthened. It is imperative that banks ensure that staff, including the front office (i.e. client-facing staff) and operations staff, are adequately trained and given timely and relevant updates on red flag indicators and typologies to heighten sanctions risk awareness. This is essential to strengthen banks' defences against PF risks so that management and the Compliance function make adequate interventions to mitigate the risks. Similarly, some banks do not have a structured channel for the audit and compliance testing/quality assurance functions to be apprised of PF-related sanctions issues. This information sharing is necessary to prompt timely and adequate auditing/testing of the relevant controls and enhancements put in place, to ensure effectiveness.

4.3 Banks already have in place, regular audit and compliance testing of key sanctions-related controls. MAS observed that some banks conduct sanctions-related controls testing on a yearly basis. In this regard, the frequency of compliance testing/quality assurance could be increased, in particular where new sanctions-related controls have been implemented, to enable timely identification of implementation issues/gaps for early intervention/enhancements. Such reviews could also cover the adequacy/timeliness of front office escalation, where relevant, as a form of feedback to the risk awareness/accountability assessment.

4.4 As the UNSCRs are updated, customers may not be aware of the extent and scope of sanctionable activities. In this regard, some banks have in place, a process to communicate the sanctions prohibitions to their higher risk customers and to obtain an undertaking from the customers, confirming that they would not engage in sanctionable activities. Notwithstanding such communications and/or undertakings obtained, banks have put in place ring-fencing controls to mitigate PF-related sanctions risks posed by customers.

Box Story: Educating customers on the risks of conducting sanctionable activities by operating companies

One long-established Singapore company in wholesale trading business, with Singaporean beneficial owners, had past trading businesses (non-sanctioned trade) with a sanctioned country. With the tightening of sanctions prohibition, the bank noted that this customer had set up a separate company, with the exact same beneficial owners. The separate company was originally involved in legitimate business. Both companies held separate bank accounts with the same bank. Several years after the setting up of the separate company, the bank detected that the transactions of the separate company were linked to counterparties that were known to deal with front/nominees on behalf of sanctioned entities. It became apparent that the separate company was set up specifically to ringfence the sanctions-related businesses from the original company. The customer, upon questioning by the bank, said that he was unaware of the implications of continuing such trades with the sanctioned country.

The bank noted that it was important to regularly engage and update customers about sanctions prohibitions to aid in effective management of sanctions risks.

Sound Practices

- Board of directors and senior management are apprised of PF-related issues and risks facing the bank in a timely manner.
- Banks have in place an appropriate incentive/accountability framework and timely training of PF red flags to ensure timely escalation of PF-related sanctions risks, including by front office staff.
- Banks have in place, an effective and structured channel to update the second and third lines of defence functions on PF-related risks to prompt timely and adequate testing of PF-related sanctions controls.
- Banks have clear and regular customer communications on sanctions prohibitions.

5 Conclusion

5.1 Overall, banks have in place policies, procedures and controls to detect and manage sanctions-related risks. Nonetheless, there are areas where banks should strengthen controls execution, which are discussed in sections 2 to 4 of this paper. In particular, there is room to further strengthen staff risk awareness, through timely sharing of red flag indicators and typologies.

5.2 Most banks have enhanced list-based sanctions compliance controls to address activity-based sanctions and use of front/shell companies to evade sanctions detection. These enhancements include among others:

(i) instituting a structured process for self-identification of gaps and controls enhancements;
(ii) sharpening existing CDD measures to identify higher sanctions risk customers;
(iii) conducting regular sanctions surveillance checks to assess banks’ risk exposure; and
(iv) enhancing ongoing monitoring checks to better detect and/or target transactions carrying PF risks.

5.3 These uplifts in controls enabled banks to be more vigilant to changes in customer risk profiles, which in turn prompted further due diligence where red flags were detected. It was through these enhanced controls that some banks were able to detect and mitigate potential sanctions evasion transactions.

5.4 Banks and FIs are expected to continue to strengthen and enhance controls to mitigate the risks and comply with regulatory obligations, as new typologies emerge. MAS will continue to share information and best practices to uplift industry practices.

Annex: Proliferation financing indicators

The following is a non-exhaustive list of indicators[6] of PF, which are relevant for customer and transaction monitoring:

i. The customer's transaction involves an individual or entity in a foreign country associated with proliferation and/or sanctions evasion concern;
ii. The customer or counterparty or its address is similar to one of the parties found on publicly available lists of persons who have been denied export licences, or has a history of export control contraventions;
iii. The customer's transactions involve possible shell companies (e.g. companies that do not appear to have real business activities in Singapore and display other shell company indicators);
iv. The customer is vague and resistant to providing additional information when asked;
v. The customer has a sudden change in business activities.
vi. The customer is known or believed to have previous dealings with individuals or entities in countries subject to UNSC sanctions; or
vii. Sudden/frequent changes in directorship/authorised signatories which are not well-explained or intended to conceal links with individuals associated with sanctioned countries/activities.

[6] More examples of these indicators can be found in the Guidance on Proliferation Financing in the MAS Guidelines and the FATF's 2018 "Guidance on Counter Proliferation Financing – The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction".