



BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR
FINANCIAL SUPERVISION SECTOR

MEMORANDUM NO. M-2021-015


To : All BSP-Supervised Financial Institutions (BSFIs)

Subject : **Guidance Papers on Managing Terrorist Financing (TF) and Proliferation Financing (PF) Risks and Implementation of Targeted Financial Sanctions (TFS)**

The Monetary Board, in its Resolution No. 268 dated 04 March 2021, approved the issuance of the attached guidance papers, namely: *"Enhancing the Control Framework on Terrorist Financing"* and *"Strengthening Implementation of Targeted Financial Sanctions and Proliferation Financing Risk Management Framework"* attached as Annexes A and B, respectively. The guidance papers highlight the good practices, relevant typologies and red flag indicators related to terrorism, TF and PF, and implementation of TFS. They likewise identify areas for improvement to strengthen measures to detect, prevent, and mitigate risks arising from the aforecited activities.

BSFIs are expected to use these guidance papers in strengthening their Anti-Money Laundering/Combating the Financing of Terrorism risk management framework in a manner consistent with and proportionate to their risk profile.

For information and guidance.

 Digitally signed by
Chuchi G. Fonacier
Date: 2021.03.16
12:11:21 +08'00'

CHUCHI G. FONACIER
Deputy Governor

16 March 2021

Att: a/s

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE

 3/17/21
JOSE MICHAEL E. CAMACHO
Bank Officer-II, RMD

Administrative Services Department

Enhancing the Control Framework on Terrorist Financing

Guidance Paper
March 2021



CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE



JOSE MICHAEL E. CAMACHO

Bank Officer II, RMD
Administrative Services Department

Table of Contents

1 INTRODUCTION	1
2 EXECUTIVE SUMMARY	2
3 REGULATORY EXPECTATIONS AND KEY OBSERVATIONS	3
Regulatory Expectation #1: Institutional Risk Assessment (IRA) -	3
Regulatory Expectation #2: Customer Due Diligence (CDD) –	3
Regulatory Expectation #3: Transaction Monitoring -	5
Regulatory Expectation #4: Suspicious Transaction Reporting -	6
Regulatory Expectation #5: Training Program -	7
Regulatory Expectation #6: Compliance with Freeze Orders -	8
4 - DATA AND INFORMATION COLLECTION AND ANALYSIS	9
Red Flag Indicators.....	9
5 TERRORIST FINANCING TYPOLOGIES	12
6 CONCLUSION	15
APPENDIX I	16

**CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE**


3/17/21
JOSE MICHAEL E. CAMACHO
Bank Officer II, RMD
Administrative Services Department





1 INTRODUCTION

Acts of terrorism is criminalized in the Philippines under Republic Act (R.A.) No. 11479 or the Anti-Terrorism Act (ATA) of 2020. ATA criminalizes, among others, the threat, planning, training, and facilitating the commission of, as well as conspiracy, proposal and inciting to commit, terrorism. Moreover, R.A. No. 10168 or “The Terrorist Financing Prevention and Suppression Act of 2012” (TFPSA) defines and penalizes the crime of financing of terrorism, designates terrorist financing (TF) as a predicate offense to money laundering (ML), and authorizes the Anti Money Laundering Council (AMLC) to issue an ex parte order of freeze without delay on funds and properties related to acts of terrorism or TF.

Thematic review is an integral part of the menu of supervisory tools being used by the Bangko Sentral ng Pilipinas (BSP). Similarly known as horizontal or comparative assessment, thematic review pertains to focused evaluation of a particular process or risk area that poses safety or soundness concern to the operations of BSP-supervised financial institution (BSFI), in particular, or the financial system, as a whole. For anti-money laundering (AML) and combating the financing of terrorism (CFT) supervision, the conduct of thematic review is informed by the results of the National ML/TF Risk Assessment (NRA) exercise and surveillance activities aimed at identifying emerging threats in the financial sector. This enables the BSP to provide further guidance to BSFIs in proactively identifying emerging ML/TF risks and propose appropriate measures to mitigate them.

Scope of the Thematic Review on Terrorism and TF

The thematic review covering a select number of BSFIs aims to assess the existing preventive measures and internal control mechanisms of BSFIs, specifically customer due diligence (CDD) and ongoing monitoring of transactions, in identifying and reporting TF and other related activities. The scope includes evaluating the comprehensiveness of institutional risk assessment (IRA) on terrorism and TF and adequacy of procedures to ensure compliance with obligations under the TFPSA.

 <i>Institutional Risk Assessment</i>	<i>Ongoing monitoring of transactions</i> 
 <i>Customer due diligence</i>	<i>Obligations under TFPSA: Freezing, Suspicious Transaction Reporting, Training Program, Compliance with Freeze Orders</i> 

The selected BSFIs covered under the thematic review consist of banks, money service businesses (MSBs), electronic money issuers (EMIs) and virtual currency exchanges (VCEs) representing each sector.

2 EXECUTIVE SUMMARY

The number of recorded terrorism incidents in the country is on an upward trend in the last three decades starting from 1990 to 2017 totaling 5,867 incidents¹. The increasing number of these incidents carried out by terrorist organizations and other local threat groups indicate the presence of funds and material support for terrorist activities. Based on the Philippine National Police (PNP) records for the period 2014-2016, there were 1,039² incidents related to identified local threat groups, mostly from Regions XIII (Caraga), Region V (Bicol), Bangsamoro Autonomous Region in Muslim Mindanao (BARMM) and Region XI (Davao). Furthermore, from 2017 to 30 September 2020, about 2,660 incidents have been recorded by law enforcement agencies (LEAs), registering 156 percent increase from total incidents noted in the Second NRA. Over 50 percent of the incidents occurred in the Mindanao region while 16 percent transpired in the Bicol Region³.

This thematic review reveals that BSFIs recognize the risks posed by terrorism and TF on their operations. They have generally established ML/TF risk management and control framework proportionate to their risk profile, albeit with noted areas for improvement. Policies and procedures and their implementation vary across the industry. Some BSFIs have adopted sound practices, particularly on customer identification and sanctions screening processes, and training program that others can emulate. There are also aspects that warrant enhancements, such as risk assessment on terrorism and TF as well as measures to strengthen conduct of CDD and suspicious transaction (ST) identification and reporting. BSFIs faced challenges in proactively detecting financial transactions that may be linked or related to activities of terrorist/threat groups due to the complexity of financial flows involving various sectors and significant volume of low value transactions. Moreover, most perpetrators have established legitimate sources of funds, such as self-employment and work in different sectors.

BSP's expectation on Board and Senior Management

It is necessary that the Board of Directors (BOD) and Senior Management (SM) set appropriate and proactive tone from the top and institute culture of both risk awareness and compliance within the organization to ensure effective implementation of a sound CFT framework capable of detecting and mitigating risks arising from terrorism, TF, and other related activities.

This Paper provides essential reminders and practical guidance intended to enhance the BSFIs' understanding and appreciation of their obligations under the TFPSA. BSFIs should study and consider the guidance to improve their AML/CFT framework and processes relating to TF detection and prevention, in a proportionate manner with due regard to the complexity of their operations and profile of their customers.

¹ Data retrieved from <https://www.start.umd.edu/gtd> University of Maryland accessed on 16 December 2020

² 2nd NRA 2017, The Philippines Second National Risk Assessment on Money Laundering and Terrorist Financing





³ AMLC 2021 Terrorism and Terrorism Financing Risk Assessment

3 REGULATORY EXPECTATIONS AND KEY OBSERVATIONS

The thematic review highlighted both sound practices and scope for enhancements in managing risks arising from terrorism, TF, and other related activities.

Regulatory Expectation #1: Institutional Risk Assessment (IRA) - BSFIs should conduct comprehensive risk assessment to identify, understand, and assess terrorism and TF risks arising from relevant factors, including those prescribed by the regulations.

Completion of IRA varies across different types of BSFIs, with universal and commercial banks (UKBs) at more advanced stage. EMIs and VCEs are completing their respective ML/TF risk assessments⁴.

 <p>Sound practices observed</p>	 <p>Areas for improvement</p>
<p>Some UKBs, particularly foreign bank branches, have <i>embedded periodic (i.e., every 2 years) ML/TF risk assessments as an integral part of their AML/CFT processes</i>. Such assessment considers terrorism and TF as predicate offenses and incorporates various factors, such as customer profile, geographic location, products, services, transactions and delivery channels. They also adopted methodologies suited to their own profile and operations.</p> 	<p>The assessment of risks on terrorism and TF is <i>not adequately covered in the IRA</i>, and relevant results of the national/sectoral risk assessments are not considered.</p>  <p><i>Qualitative assessment is not sufficiently supported by relevant quantitative data</i>, such as analysis of ST Reports (STRs) relating to terrorism and TF, and other associated unlawful activities, as well as known cases/typologies.</p>

Regulatory Expectation #2: Customer Due Diligence (CDD) – BSFIs should adopt adequate and appropriate CDD process and establish mechanisms to ensure effective implementation.

Most banks (especially those classified as complex) have adopted automated mechanism that facilitates seamless customer risk profiling. The process for non-bank financial institutions (NBFIs), such as MSBs, is crude and still developing, particularly in terms of assessing relevant criteria or factors. Proper assessment of customer risk profile will drive the level of due diligence to be applied during onboarding and throughout the life cycle of customer relationship.

⁴ The IRA shall be conducted, at least once every two (2) years, or as often as the Board or senior management may direct, depending on the level of risks identified in the previous risk assessment, or other relevant AML/CFT developments that may have an impact on the BSFI's operations.



Sound practices observed

CDD procedures are adequate. Controls are embedded in the digital onboarding system that facilitates customer identification, watchlist screening, and risk profiling that will inform decision on the customer relationship.



Sanctions lists used are broad. Databases, whether internally developed or through third party providers, include lists from relevant sanctioning bodies, such as the United Nations Security Council (UNSC) List and Office of Foreign Assets Control (OFAC)/Specially Designated Nationals (SDN) List. Internal database also includes persons cited in negative media reports on terrorism and TF, as well as those subject of previously filed STRs.

Clear policies for Non-Profit Organizations (NPOs) are established. Policies and procedures for NPOs, including conduct of enhanced due diligence (EDD) on those that pose higher risk to TF due to core characteristics⁵ are comprehensive.



Periodic or event-driven CDD reviews based on risk and materiality are conducted. On-going CDD in banks includes periodic or event-driven reviews that trigger updates to the customer profile. These include customer-specific or policy-driven trigger events.



Areas for improvement

Inadequate customer risk assessment. Inadequate process to understand the customer profile (e.g., business type, country of operation, source of funds, and source of wealth), the intended purpose, use and activity of the account or relationship (e.g., expected volume and amount of transactions, and supplemental information when the declared source of funds is remittance), as well as to verify other relevant information apparent during onboarding (such as declared counterparties and/or related parties, if any).



Non-inclusion of personalities subject of AMLC or law enforcement referrals in the database. This can be attributed to incomplete or limited information or absence of secondary identifiers. BSFIs should adopt guidelines for further verification and disambiguation of the relevant customer information.

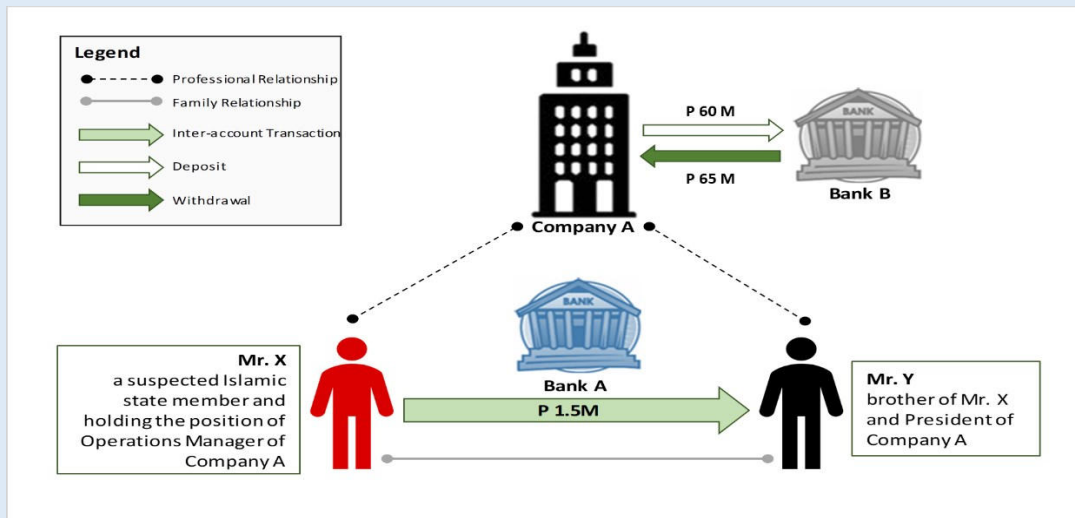


Screening system for complex MSBs is not fully automated. Manual screening process that is not commensurate with the risk profile of the BSFI.

Inadequate controls resulting in uneven implementation and documentation of conduct of EDD on high risk customers.

⁵ Such as interconnected networks, large workforce, legitimacy of identity and funds flow, and enjoys public trust/influence.

Case Study: Terrorist Financing Involving Banks



Bank A. A year after its establishment, Company A, a recruitment agency, opened an account with Bank A in 2016. In December 2016, Mr. X, a Kuwaiti national, made PhP1.5 million fund transfer, using his personal account to Mr. Y, his brother and the President of Company A, and also a client of Bank A. The funds were declared for travel expenses of Mr. Y but no documents were presented to justify the transaction. In March 2017, it was reported in the news that Company A facilitated the entry of Mr. X and the processing of his working visa as Operations Manager. Mr. X was eventually arrested in March 2017 in the National Capital Region (NCR), together with a certain Ms. T, a national of Syria and also a suspected member of Islamic State. Ms. T was also a client of Bank A. Their accounts were opened less than a year prior to their arrest and were closed in April 2017.

Bank B. Based on news report on the arrest of Mr. X and Ms. T, Bank B included their names in its internal watchlist database. Company A had several transactions from April 2017 to January 2018 which triggered alerts in Bank B's AML system. These transactions include check clearing for around PhP65 million, check deposit for around PhP60 million and check clearing for around PhP10 million. The account was closed in March 2018.

Regulatory Expectation #3: Transaction Monitoring - BSFIs should have robust AML/CFT monitoring system to proactively detect customer transactions and activities related TF.

Majority of STRs were triggered either by AMLC referrals or negative news information. BSFIs need to refine detection parameters and scenarios to capture relevant red flag indicators and transactions potentially linked to terrorism and TF activities.

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE

JOSE MICHAEL E. CAMACHO
Bank Officer II, RMD
Administrative Services Department

3 | Page



Sound practices observed

Automated monitoring systems complemented by manual mechanisms. Most banks and other complex BSFIs complement their automated monitoring system with manual mechanism, such as EDD on first time remittance transactions and sleeper accounts, to detect unusual transactions, including possible TF-related activities prior to processing.




Data analytics is being explored. As regards emerging trends and innovations, some complex banks have considered the creation of data analytics team responsible for AML/CFT initiatives, such as typology study, parameters tuning, and development of advanced analytical tools to support existing compliance functions.



Areas for improvement

Inadequate access to valuable information relating to terrorist/threat groups. Some BSFIs have not yet entered into the Public Private Partnership Program (PPPP) or Information Sharing Protocol (ISP) with the AMLC.

Limited red flag indicators. The distinct circumstances listed in the  implementing rules and regulations of the TFPSA⁶ are not fully considered in the transaction monitoring scenarios.

Inadequate measures to ensure gathering of vital information on remittance transactions. Some BSFIs do not supplement transaction monitoring with information on the purpose of the transactions and careful understanding of the relationship between the parties and the destination or source of funds.

Regulatory Expectation #4: Suspicious Transaction Reporting - BSFIs should have an effective ST reporting system to ensure complete, accurate and timely filing of STRs to the AMLC.



Sound practices observed

ST reporting chain is well-defined which considers independent and unbiased approval process.

Clear cut direction and hierarchy of actions to be taken were established in most banks. Actions



Areas for improvement

Inadequate procedures to ensure that STRs are meaningful. STR becomes more meaningful if it contains relevant information⁷, such as complete and accurate identifier information (e.g., name, birthdate, nationality, nature of business/

⁶ Section 3.a.15 of the Revised Implementing Rules and Regulations of the TFPSA

⁷ As required under the AMLC Registration and Reporting Guidelines

taken on customers subsequent to filing of STRs include, among others, tagging as high-risk for close monitoring of subsequent transactions, listing in the watchlist database, and/or subjecting to closure/termination policy, as warranted.

Adequate ST investigation and reporting process that results in submission of meaningful TF-related STRs. Most STRs (70 percent) were filed using suspicion codes PC13 (terrorism) and PC14 (TF). Other STRs provide narration of terrorism or TF as predicate offenses to ML using suspicious indicator (SI) codes, or other crimes linked to terrorism and TF, such as kidnap for ransom (KFR), drug trafficking, robbery and extortion, and illegal possession of firearms, ammunitions and explosives.

employment, address), appropriate transaction and SI codes to reflect the true nature of indicators and transactions, clear basis of filing or source or origin of suspicion, and adequate narrative that reflects the actual typology.

Insufficient investigation. Analysis is sometimes limited to the customer and his last transaction. Holistic review, including present and past transactions and identifying indicators of linkages to terrorism or TF related parties, is useful in understanding behavioral pattern and appreciation of the typology involved.

Regulatory Expectation #5: Training Program - BSFIs should have adequate and effective ongoing AML/CFT training program to increase awareness of employees concerning terrorism and TF risks, and their corresponding obligations relative thereto.



Sound practices observed

Annual and periodic AML/CFT training programs are in place. These serve as fundamental channel for disseminating policies and procedures to personnel. This is supplemented with regular issuance of general advisories to branches, units and remittance partners.

Case study: Company M is engaged in construction and real estate development. In March 2019, Mr. J, a Jordanian national, President of Company M, opened an account with the Bank with an initial deposit of Php11 thousand through the referral of Mr. J's wife, an existing account holder of the Bank. A day after the account was opened, a cross-border inward remittance of USD190 thousand was received from a certain Mr. L, in favor of Company M for its expansion. The Bank returned the funds to the originating institution because the client was not able to provide supporting documents citing confidentiality. Company M also had a check deposit of Php1.5 million in early August 2019. In August 2019, Mr. J was reported in a news article as the arrested Jordanian linked to Bin Laden.



Areas for improvement

Inadequate topics covered on terrorism/TF in learning modules. This includes citing the peculiarities of TF, relevant red flag indicators, typologies, and the fact that these may involve funds from legitimate sources.

Insufficient dissemination of relevant and practical information on terrorism and TF. The information that should also be shared with relevant units in the BSFI include personalities subject of negative news, high risk locations, customer/subject profile and demographics, as well as nature of transactions relative to confirmed terrorism and TF cases.

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE

3/17/21 7 | Page
JOSE MICHAEL E. CAMACHO
Bank Officer II, RMD
Administrative Services Department

Regulatory Expectation #6: Compliance with Freeze Orders - BSFIs should have measures to ensure strict compliance with obligations upon receipt of freeze order.



Sound practices observed



Specific guidelines and detailed procedures in handling account(s) that is/are subject(s) of freeze order are in place. These include, among others, timely freezing of funds and eventual blocking of accounts, and conducting further investigation to identify related and materially-linked accounts.



Areas for improvement

Inadequate controls to ensure timely reporting to the AMLC of all attempted dealings with regard to the frozen property or funds.

Case study: Inter-Sectoral Exposure involving a Bank and MSB

In October 2013, Ms. F opened an account with Bank Z with remittance as the declared source of fund. From February to July 2019, Ms. F had 11 incoming remittances (averaging around PhP60 thousand) from six different persons abroad from the Netherlands, Qatar, United Arab Emirates, and the United States of America. The funds were subsequently withdrawn in small amounts (around PhP7 thousand) through ATM for 95 times. In a news report in July 2019, Ms. F was identified as allegedly involved in a suspected TF case.

In December 2019, MSB A received a request from the AMLC for documents pertaining to Ms. F who was suspected to be a member of ISIS terrorist group and one of the two alleged sympathizers nabbed in a raid in the southern part of the Philippines per July 2019 news report. Ms. F resides in Metro Manila and her notable transaction was a domestic inward remittance for Php7 thousand from Ms. G, an online seller. Ms. G received funds from 2016 to 2018 from her relative, Mr. X. The transactions transpired in different locations specifically in the cities in southern Philippines, Southern Luzon, and NCR.

LEARNING POINT: *This case highlights the exposure of a bank and a NBFI to common subject customer (Ms. F). News scanning plays a significant role in the conduct of appropriate CDD procedures even prior to receipt of any AMLC referral.*

**CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE**

JOSE MICHAEL E. CAMACHO 8 | Page
Bank Officer II, RMD
Administrative Services Department

4 - DATA AND INFORMATION COLLECTION AND ANALYSIS

From September 2003 to March 2020, 2,450 STRs with aggregate value of PhP1.8 billion were filed⁸. Most of these STRs, both in terms of volume and value, were filed by BSFIs, specifically UKBs and MSBs. Some were also submitted by thrift and rural banks, EMLs, and non-stock savings and loan association. The significant number and amount of STRs filed by the banking sector is mainly driven by the sector's exposure to low volume-high value NPO transactions, as well as high volume-low value transactions of individuals. MSBs, on the other hand, are susceptible given the retail nature of transactions of their individual customers and their wide network of operations. On a more recent STR analysis by the AMLC, covering the period from 01 January 2018 to 31 December 2020, 61 percent were filed by MSBs and pawnshops while 29 percent were filed by banks. Monthly trend shows a surge in STRs from September to December 2020, after the enactment of the ATA⁹.

These STRs were largely triggered by AMLC referrals, while others were based on adverse news, branch referrals, as well as observations during conduct of BSP examinations. For banks, aside from AMLC referrals, STRs were triggered by the results of sanctions screening, AML/CFT monitoring system, and special reviews. Meanwhile, remittance partner referrals are common between MSBs and EMLs. MSBs are also filing STRs based on LEA referrals. (See Figures 1 and 2 below)

Figure 1

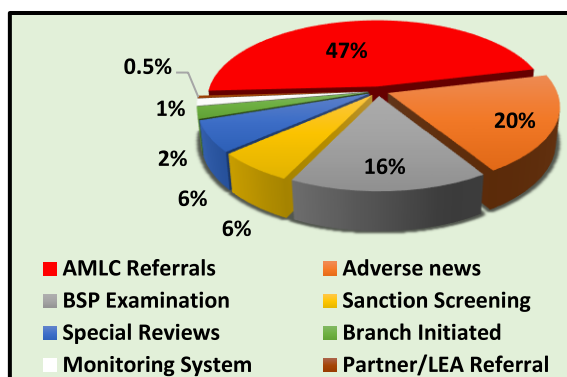
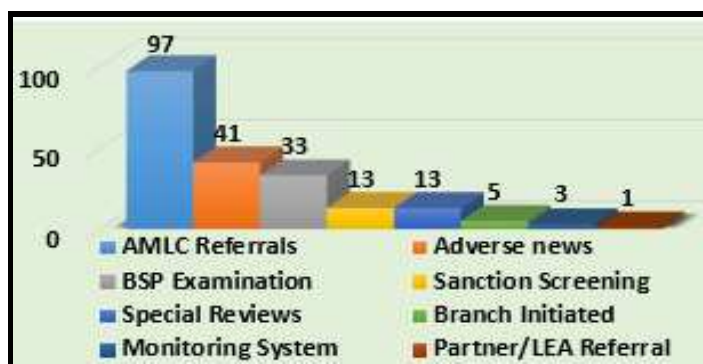


Figure 2



Red Flag Indicators

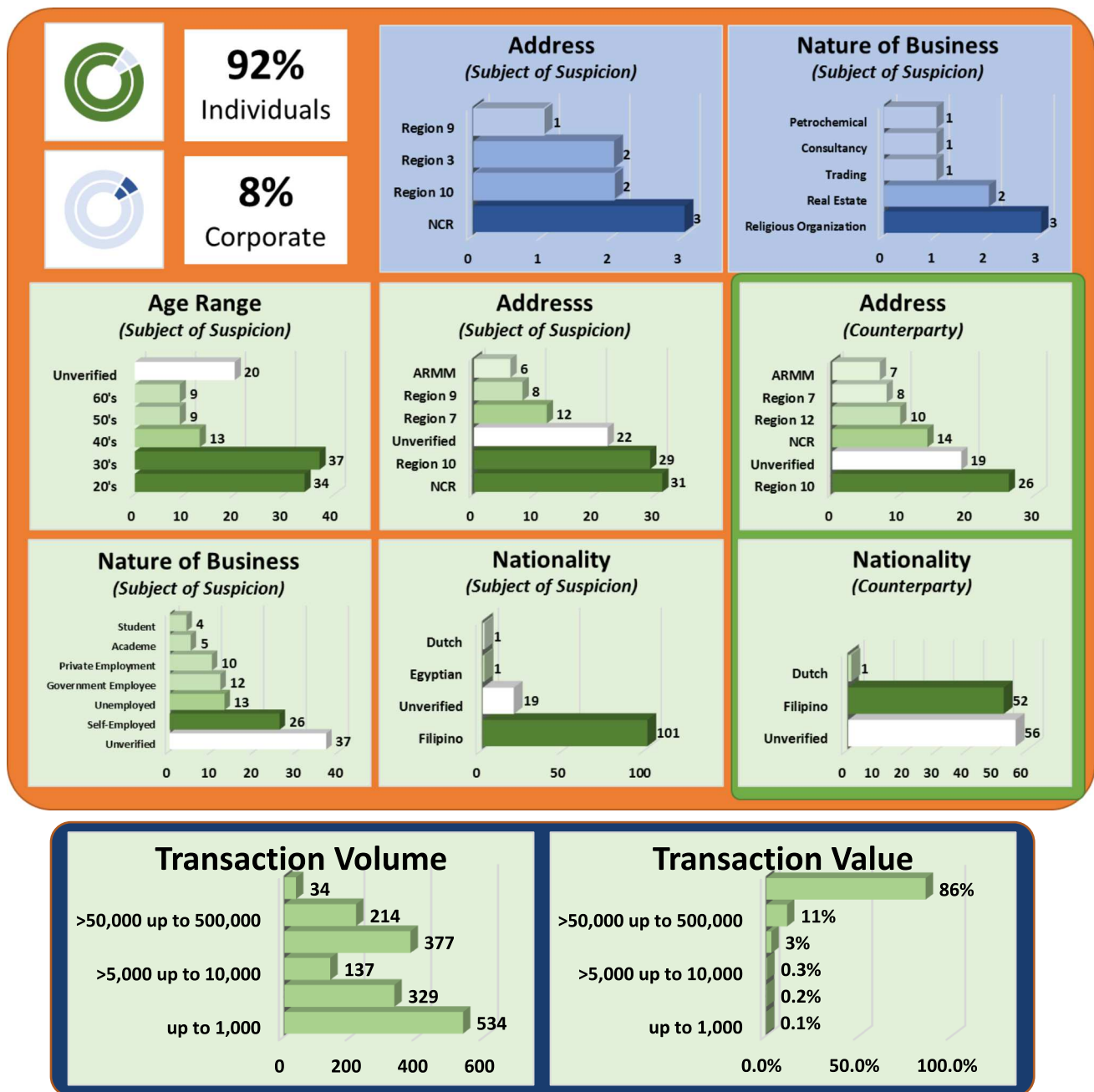
BSFIs should pay attention to the succeeding indicators presented in the dashboard and analysis of customer profile, geographic location, and products or services, when monitoring customer's transactions as these could indicate potential link to terrorism and TF activities. These were derived from the analysis of STRs filed by BSFIs subject of the thematic review and supplemented by analysis of relevant data from other sources such as various AMLC studies. These red flags are not exhaustive and the presence of one indicator does not necessarily mean that the transaction is certainly related to terrorism or TF. The use of combination of red flag indicators is recommended, especially in adopting detection parameters and scenarios in either electronic or manual monitoring system or data analytics.



⁸ Based on various data/ reports provided by the AMLC

⁹ AMLC 2021 Terrorism and Terrorism Financing Risk Assessment

The *financial system dashboard*¹⁰ below summarizes the results of analysis of STRs filed by BSFIs subject of the thematic review, particularly in terms of customer profile and geographic location. This can be used in designing relevant scenarios/parameters.



¹⁰ Dashboard based on terrorism and TF-related STRs. Unverified data in the chart pertains to missing information in the STR which can be attributed to the BSFIs' inability to gather relevant information, such as date of birth, nationality, address and nature of business, either during onboarding or updating/ongoing monitoring of customer/transactions.

Analysis of Customer Profile

- Majority of STRs involve accounts of individuals, mostly Filipinos, while other nationalities identified include Dutch, Egyptians, American, Australian, Indonesian, Jordanian, Kuwaiti, Qatari, and Turkish;
- Exposure to corporate customers, particularly NPOs, is apparent in banks;
- Majority of perpetrators are within the age range 21-40 years old; and
- Financial profile varies ranging from self-employed, private and government workers, while others were unemployed and few were students.

Analysis of Geographic Location

- Most subjects and counterparties in the STRs analyzed are from the NCR and in the Mindanao area; and
- Foreign addresses noted include Moscow Russia, Doha Qatar, and Jeddah, Saudi Arabia.

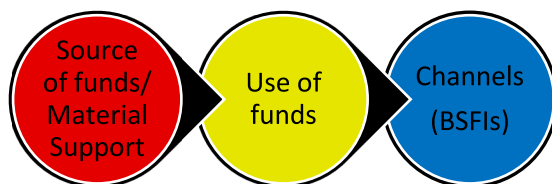
Analysis of Product/Service/Transaction Volume and Value

- Products/services availed or used in STRs relating to terrorism and/or TF vary among BSFIs. In banks, transactions are still concentrated in current and savings account transactions, mostly deposits and withdrawals. In MSBs, transactions involved both inward and outward transfers while in VCEs, domestic outward remittance and cash-in transactions were noted. For EMIs, transactions involved cash card loading and inter-wallet transfers;
- Use of ZSTR code¹¹ is prevalent in STRs filed by banks, MSBs and VCEs; and
- Transactions of corporate customers are low in volume but high in value, accounting for 86 percent (or PhP236 million) of total STR value. Conversely, transactions of individuals are voluminous but small in amount, such that more than 50 percent of total STRs (or 863 of 1,625 transactions) involve around PhP5 thousand only.

¹¹ The transaction code “ZSTR” shall be used if the subject is not an accountholder of the reporting institution or is an accountholder but has no monetary transaction with the covered person at the time the suspicious activity is determined.

5 TERRORIST FINANCING TYPOLOGIES

The Source-Use-Channel Model below encapsulates the flow of funds and how these funds are sourced and being used by terrorists and terrorist organizations in achieving their objectives, channeled through banks and other BSFIs.



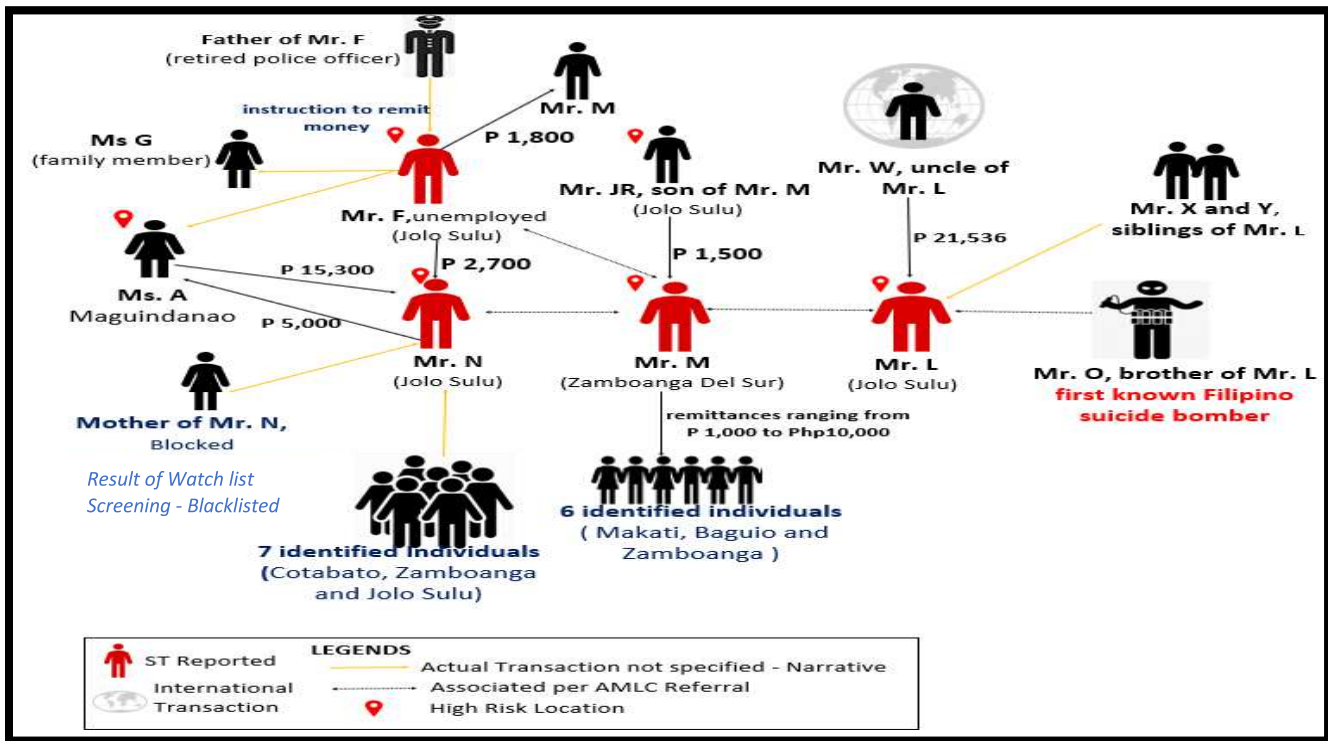
Terrorist/threat organizations predominantly use illegal means to raise funds, with KFR and extortion as the preferred means to obtain funding. Some also resort to legitimate means to raise funds, such as the use of NPOs, family funding, and legitimate business fronts. According to intelligence reports, it is suspected that these legitimate business fronts are likewise being used for drug trafficking. Use of funds are generally for operational purposes, such as purchase of ammunitions and vehicles. Threat groups also used part of the funds raised to support the communities of the locality where they operate. The groups provide the basic needs, livelihood support, and even educational opportunities to these communities. In turn, these communities provide safe-harbor for the terrorist organization/group.¹²

Cash transactions remain to be the usual mode for transfer of value as the physical movement of cash leaves no paper trail and is not hindered by AML/CFT safeguards present in the formal financial system. Remittance transactions through MSBs and banks have also been reported to be the delivery channel by which funds are transferred, especially from abroad. However, there were also noted unregistered MSBs that are utilized by terror groups to further avoid detection and to easily move funds in and out of the country. One of the emerging threats noted in TF is the evolution of virtual currency and/or cryptocurrency.¹³

¹² 2nd NRA 2017, The Philippines Second National Risk Assessment on Money Laundering and Terrorist Financing

¹³ AMLC 2021 Terrorism and Terrorism Financing Risk Assessment

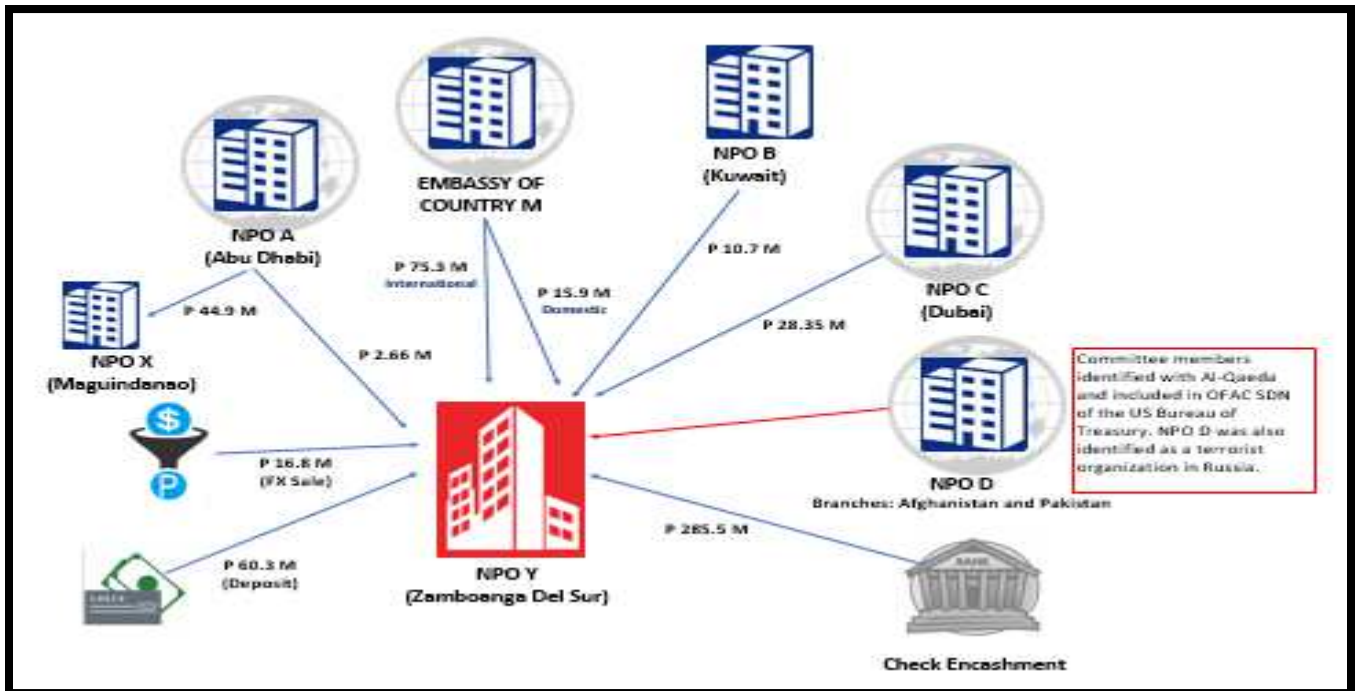
Typology 1. Web of remittance transactions of various personalities involved in TF facilitated through MSB



Remittances in small amounts and multiple layers involving several senders and receivers of funds mostly with familial relationships were facilitated through MSBs prior to receipt of AMLC referrals that triggered the filing of STRs. Declared purposes of transfers are allowances, household expenses, and payments. Subjects¹⁴ are residing in Mindanao, particularly in Jolo, Sulu, and Zamboanga Del Sur. Behavioral patterns of transactions in one-to-many and many-to-one correspondences, and linkage of the subjects to a retired police officer and to the first known Filipino bomber behind the twin blasts in Indanan, Sulu in June 2019 (based on news article) were noted.

¹⁴ These subjects are the four (4) individuals highlighted in red. They are both sending and receiving remittance to/from various counterparties and even among themselves.

Typology 2: Terrorist Financing – involvement of NPOs



Bank X's filing of STR relative to NPO Y was triggered by a discussion with the BSP examination team on the inclusion of NPO Y in the whitelisted accounts¹⁵. Upon review of the transactions/records, the client is a charitable institution receiving funds through remittances from various NPOs. Declared purposes are to build mosques and schools and to provide allowances for Islamic teachers. US Department of the Treasury designated and blocked the assets of NPO D, remitter of funds to NPO Y, due to its committee members' identification with Al-Qaeda and inclusion in the OFAC SDN List.

Refer to Appendix I for other typologies.

¹⁵ Refers to permanently suppressed alerts pertaining to a specific customer.

6 CONCLUSION



The number and extent of incidents in the country associated with terror/threat organizations, as well as their apparent systematic and established method of raising funds for their operations, warrant a strategic and targeted response from BSFIs.

To address the rising threat of terrorism and TF in the country, it is essential that BSFIs establish and maintain a robust ML/TF risk management framework that integrates detective, preventive, and corrective measures to disrupt the financial aspect of this criminal activity. This should be anchored not only on the risk assessment at both national and sectoral levels but also on the IRAs.

It is expected that the BOD and SM set a proactive and clear tone from the top and establish a culture of compliance in the organization to ensure effective implementation of a strong AML/CFT framework. BSFIs are also expected to conduct a review of processes and address any gaps identified, taking into consideration the results of this thematic review.

Various sectors should collaborate to strengthen processes to identify and report potential terrorism and TF activities. Strong collaboration of stakeholders is key to identifying customers and transactions possibly linked to terrorism and TF activity. In this respect, BSFIs are highly encouraged to participate in the PPPP of the AMLC to benefit from critical information exchanges. BSFIs may also be guided by issuances of relevant regulatory changes particularly on preventive measures against TF.

Lastly, continuing capacity building and information awareness play an important role in the country's fight against terrorism and TF.

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE

 3/17/21

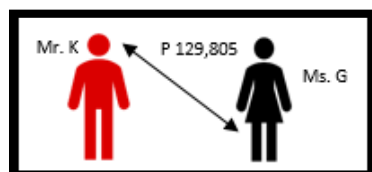
JOSE MICHAEL E. CAMACHO
Bank Officer II, RMD
Administrative Services Department



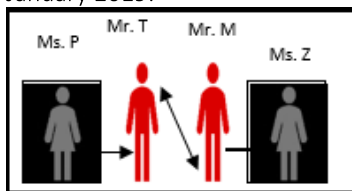
Other predicate crimes linked to terrorism and TF

Drug Trafficking

This is based on a **news article** published in March 2019 regarding the **arrest of narco-terrorists** in Manila namely, Mr. K, Mr. M, and Mr. T. The transactions of said suspects were facilitated by MSB X.



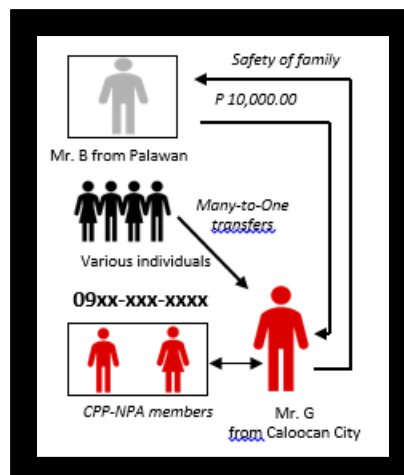
Ms. G (**unemployed, housewife**) **sent funds** to Mr. K **in tranches**. In September 2017, she sent five remittances that aggregated to Php89 thousand, which was followed by remittances worth Php27.7 thousand per month. The same amounts of funds were returned by Mr. K to Ms. G starting 2018 until the former's arrest in 2019. These **two were subjects of AMLC referral** provided to MSB X in January 2019.



In a separate occasion, the two other arrested suspects, Mr. T and Mr. M, were **transferring funds to each other**. Other remittances of Mr. M were mostly sent to Ms. Z in **Maguindanao** in 2018, which amounted to Php114 thousand for 3 transactions. On the other hand, a certain Ms. P (**also from Maguindanao**) was linked to Mr. T in numerous circumstances. In 2017, funds transferred by Ms. P amounted to Php92.7 thousand.

Robbery and Extortion

Mr. B (sender) received a **death threat** from Mr. G and was asked to **send money** in exchange for his **family's safety**. The **phone numbers** used by Mr. G were the same numbers being used by Mr. A, Mr. R, Ms. V, and Ms. F, who were confirmed by the PNP to be **members of ABC extremist group**.

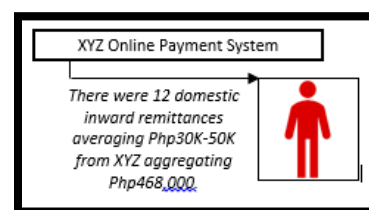


Another investigation disclosed that multiple inward remittances **coming from various individuals**, who were noted to be other **victims** of the same extortion activity of Mr. G, were made in favor of him. Mr. G introduced himself as a member of ABC extremist group.

Declared purposes of transactions were mainly for **business** or **donation** while stated sender-beneficiary relationships were **friends**.

Illegal/Unlawful Possession, Manufacture, Dealing in, Acquisition or Disposition of Firearms, Ammunition or Explosives

Based on **media reports** in 2014, Mr. C, a client of Bank Z, was **arrested** in Cebu together with the consultants of the XXX Group. They were charged with violation of R.A. No. 9516 and R.A. No. 10591 due to Mr. C's possession of: (i) a 0.5-caliber Colt pistol and three magazines with 17 rounds of ammunition; and (ii) a 9mm pistol with a magazine loaded with seven rounds of ammunition.



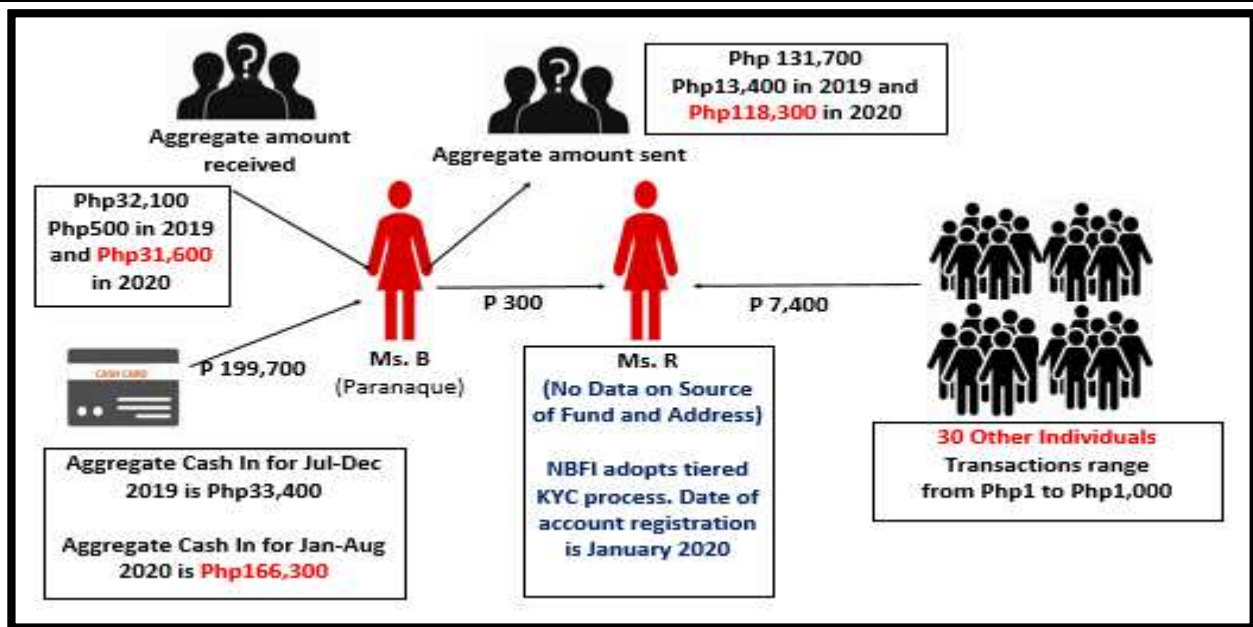
Mr. C opened an account with Bank Z in 2009 and he declared himself as **self-employed** in the CDD form. Based on other records, the client is the **owner** of a Cebu specialty products store, an **online business** that is not part of the Department of Trade and Industry database.

Apparently, there was **no justification** for the funds received by the client (Mr. C) from XYZ and there was **no information available** that can identify the **source** of said funds. Further, these transactions cannot be discounted as **proceeds from client's online business** given that its legitimacy cannot be validated. For a business that is supposed to operate online, it seems unusual that it has no online presence.

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE

3/17/21
JOSE MICHAEL E. CAMACHO 16 | Page
Bank Officer II, RMD
Administrative Services Department

Terrorist Financing – predicate crime to ML (round-off amounts)



NBFI A's STR filing relative to Ms. B and Ms. R was based on SI5 (*There is a deviation from the client's profile/past transactions*). Based on AMLC inquiry (received in August 2020), these customers were identified and believed to be involved in TF activity. Transactions review led to the conclusion that there is significant difference in the pattern of transactions of Ms. B as compared to her previous year's account history.

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE

JOSE MICHAEL E. CAMACHO
Bank Officer II, RMD
Administrative Services Department

17 | Page



Pasay City, Philippines

STRENGTHENING IMPLEMENTATION OF TARGETED FINANCIAL SANCTIONS AND PROLIFERATION FINANCING RISK MANAGEMENT FRAMEWORK

Thematic Review Report
March 2021

**CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE**


3/17/21
JOSE MICHAEL E. CAMACHO
Bank Officer II, RMD
Administrative Services Department

Table of Contents

<u>I.</u>	INTRODUCTION	3
<u>II.</u>	SCOPE OF THE THEMATIC REVIEW ON PROLIFERATION FINANCING AND TARGETED FINANCIAL SANCTIONS	5
<u>III.</u>	REGULATORY EXPECTATIONS AND KEY OBSERVATIONS.....	6
	Institutional Risk Assessment.....	6
	Policies and Controls	7
	Sanctions Screening.....	8
	Employee Awareness.....	8
<u>IV.</u>	OVERALL ASSESSMENT.....	9
<u>V.</u>	CONCLUSION	9

I. INTRODUCTION

Economic sanctions measures were instituted by the United Nations Security Council (UNSC) and some jurisdictions and supranational organizations¹. Security Council sanctions have taken a number of different forms, in pursuit of varied goals. The measures have ranged from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and financial or commodity restrictions². Being a member state of the United Nations (UN), the Philippines is committed to implement the sanctions imposed by the UNSC and other international sanctioning bodies and authorities.

To facilitate the implementation of targeted financial sanctions (TFS), the Financial Action Task Force³ (FATF) developed specific requirements to give effect to and implement relevant UNSC Resolutions (UNSCRs). Specifically, FATF Recommendations 6 and 7 relate to TFS on terrorism/terrorist financing (TF) and proliferation of weapons of mass destruction (WMD) and its financing, respectively.



WHAT?

Targeted Financial Sanctions means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities³

WHY?

coerce a regime/individuals within a regime into changing their behavior by increasing the cost on them to such an extent that they decide to cease the offending behavior;

constrain a target by denying them access to key resources needed to continue their offending behavior, including the financing of terrorism or nuclear proliferation;

signal disapproval, stigmatizing and potentially isolating a regime or individual, or as a way of sending broader political messages nationally or internationally; and/or

protect the value of assets that have been misappropriated from a country until these assets can be repatriated.⁴



HOW?

Targeted asset freezing
Prohibition against Dealing⁵

¹ Such as the United States' Office of Foreign Assets Control (OFAC), United Kingdom's Financial Conduct Authority (FCA), and the European Union (EU), among others.

² <https://www.un.org/securitycouncil/sanctions/information>

³ The UNSCR No. 2462 recognized the essential role of the FATF in setting global standards to combat ML, TF and proliferation financing.

⁴ Updated FATF Recommendations as of October 2020, page 128.

⁵ Anti-Money Laundering Council (AMLC) Regulatory Issuance (ARI) No. 004, Section 5.2.

⁵ ARI No. 004, Sections 6 and FATF Interpretative Note to Recommendations 6 and 7.

The Philippine Legal Framework

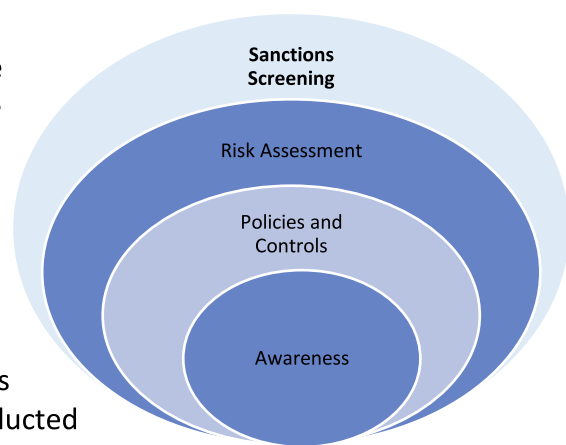
To fulfill the Philippines' international commitments and obligations consistent with national interest, the following laws were enacted to support TFS implementation:

- Republic Act (R.A.) No. 10168 or The Terrorism Financing Prevention and Suppression Act of 2012 (TFPSA) - It provides a legal framework for criminalizing TF as a stand-alone offense and grants AMLC the power to inquire and freeze assets related to TF or acts of terrorism without court order.
- R.A. No. 10697 or Strategic Trade Management Act (STMA) – It aims to take and enforce effective measures to establish domestic controls to prevent the proliferation of WMD and their means of delivery, including provision of related services, such as the financing thereof.
- R.A. No. 11479 or the Anti-Terrorism Act (ATA) of 2020 – It repeals the Human Security Act (HSA) of 2007 and enhances the designation mechanism through the Anti-Terrorism Council's automatic adoption of UNSC Consolidated List and consideration of request for designation by other jurisdiction or supranational jurisdiction. It likewise strengthened proscription mechanism via the Department of Justice's filing of application before the Court of Appeals upon the recommendation of the National Intelligence Coordinating Agency.
- R.A. No. 11521 dated 29 January 2021 – It amends, among others, the Anti-Money Laundering Act of 2001 (AMLA) to empower the AMLC to implement TFS in relation to proliferation financing (PF), including ex parte freeze without delay against funds and properties owned by entities and individuals designated by the UN under its Resolution Nos. 1718 (2006) and 2231 (2015) and their subsequent resolutions.

II. SCOPE OF THE THEMATIC REVIEW ON PF AND TFS

Thematic review is an integral part of the menu of supervisory tools being used by the Bangko Sentral ng Pilipinas (BSP). Similarly known as horizontal or comparative assessment, thematic review pertains to focused evaluation of a particular process or risk area that poses safety or soundness concern to the operations of a BSP-supervised financial institution (BSFI) in particular, or the financial system as a whole. For anti-money laundering (AML) and combating the financing of terrorism (CFT) supervision, the conduct of thematic review is informed by the results of the National ML/TF Risk Assessment (NRA) exercise and surveillance activities aimed at identifying emerging threats in the financial sector. This enables the BSP to provide further guidance to BSFIs in proactively identifying emerging money laundering (ML)/TF risks and propose appropriate measures to mitigate them.

This thematic review is conducted with the objective of understanding and assessing the adequacy of BSFIs' current measures in identifying risks related to PF and implementing TFS requirements without delay. This includes assessing the effectiveness of the institutions' sanctions screening system and relevant policies adopted as a result of BSFIs' risk assessment exercise. The scope likewise includes other controls instituted to implement TFS and trainings conducted relative thereto.



BSFIs covered in the thematic review on TFS and PF include banks, money service business, electronic money issuer, and virtual currency exchange representing each sector.

III. REGULATORY EXPECTATIONS AND KEY OBSERVATIONS

This Guidance Paper sets out the BSP's regulatory expectations in establishing an effective risk management system to counter PF and to timely implement TFS that can be applied by BSFIs, taking into account their respective risk profile. BSFIs should consider this guidance paper in improving their respective (ML)/TF/PF risk management frameworks and processes to ensure effective implementation of TFS requirements. This likewise recognizes the challenges in implementing TFS in view that it is rules-based and requires immediate freezing of accounts of designated persons and entities, as well as prohibitions against dealing with their properties or funds.

1

Regulatory Expectation: Institutional Risk Assessment (IRA)

BSFIs' process in the conduct of IRA should be commensurate with their risk profile and encompass relevant potential financial crime risks, such as PF, sanctions risks and sanctions evasion. Risk-based measures of BSFIs reinforce and complement full implementation of TFS by detecting and preventing non-implementation, potential breach, or sanctions evasion.



What can be better?

- Conduct of IRA is still ongoing for some BSFIs
- Sanctions and PF risks are not adequately scoped or considered in the IRA



Good practice

- IRA methodology considers assessment of products, customers, and geographic location of the BSFI and its customers which may be exposed to PF, sanctions risks and sanctions evasion
- Controls to prevent sanctions evasion were implemented to business units identified to have higher exposures to relevant risks

2

Regulatory Expectation: Policies and Controls

BSFIs should have adequate and clear policies commensurate to their risk profile to prevent sanctions risks and their evasion, and to fully implement TFS requirements. These include hierarchy of actions to disambiguate possible matches, and appropriate and effective controls to counter PF.



What can be better?

- Policies are limited to the conduct of sanctions screening and performance of enhanced due diligence (EDD) in case of positive hit
- Inadequate controls to counter PF
- Incomplete database for dual-use goods (DUGs) and other strategic goods subject of bans/controls



Good practice

- Adopts policies on sanctions from relevant jurisdictions/ supranational level, application of freezing of funds, and prohibition in dealing with designated persons
- Implements a structured process, including tiered-approval, wherein a possible target match undergoes review for disambiguation
- Implements controls to screen other information in a trade transactions against list of sanctioned vessels and DUGs, among other things
- Employs sanctions risk rating for customers or account relationships as part of the customer due diligence during onboarding or upon trigger event
- Adopts red flag indicators to identify possible PF

3

Regulatory Expectation: Sanctions Screening

BSFIs should utilize appropriate and effective sanctions screening system to identify PF, implement TFS, and mitigate evasion of sanctions



What can be better?

- Sanctions screening is performed only upon trigger events, such as breach of internal limits
- Transactional sanctions screening is not performed on non-account holders/walk-in customers
- System used is not adjusted to suit the profile or complexity of the BSFI

Good practice



- Requires creation of Customer Information File in the system for all customers, including occasional customers, to ensure customer screening
- Uses trigger-event scenarios, such as changes in customer information or update of the sanctions list, to conduct periodic scrubbing of customer database
- Utilizes comprehensive and updated sanctions database

4

Regulatory Expectation: Employee Awareness

Employees of BSFIs are cognizant of the policies and procedures relevant to timely implementation of TFS and countering PF



What can be better?

- Trainings are limited to conduct of sanctions screening and subsequent EDD in case of possible match
- Dissemination of new policies is limited to publication through e-mails or BSFI's intranet



Good practice

- Trainings include case analysis wherein participants can apply their learnings in the training
- Employees are adequately informed of their adjudication process and when to implement TFS requirements

IV. OVERALL ASSESSMENT

Most BSFIs have adopted policies and procedures to implement the requirements of TFS and have installed sanctions screening system with due regard to the complexity and nature of their respective operations. For sanctions screening, the UNSC list is included by default in the sanctions system. Nonetheless, BSFIs need to assess their sanctions risk, which includes evasion techniques that can cut across the other operations of the institution, improve sanctions screening to cover funds/transactions of non-accountholders/walk-in customers, and enhance transaction monitoring through adoption of red flag indicators to identify PF activities. These should be complemented by the adoption of a continuing training program for personnel to deepen their understanding of the TFS requirements.

V. CONCLUSION

Implementing TFS requirements and countering PF are among the supervisory priorities of the BSP. The thematic review revealed that BSFIs have adopted policies and procedures to counter PF and implement TFS, although there are still areas that warrant enhancements. These include conduct of appropriate IRA, as well as adoption and/or enhancements of policies on TFS and control measures on PF. An equally important factor in this respect is the implementation of capacity building and awareness program for frontline employees on policies, procedures, and typologies regarding PF and TFS. The Board of Directors and Senior Management of BSFIs are expected to set a clear and proactive tone from the top and establish culture of compliance in their respective organizations to ensure effective implementation of a strong AML/CFT framework. BSFIs are also expected to review existing processes and address any gaps identified, taking into consideration the results of the thematic review.

The BSP will continue to engage BSFIs towards strengthening industry practices and institutional frameworks to mitigate PF risks and sanctions evasion, as well as to effectively implement TFS requirements.