



BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR | FINANCIAL SUPERVISION SECTOR

MEMORANDUM NO. M-2022-038

To : **All BSP-Supervised Financial Institutions (BSFIs)**

Subject : **2022 Guidance Paper on Targeted Financial Sanctions (TFS) Implementation**

In its Resolution No. 1262 dated 25 August 2022, the Monetary Board approved the issuance of the attached guidance paper entitled "*Targeted Financial Sanctions Implementation*" (Annex A). The guidance paper highlights best practices, scope for improvement, and major challenges on TFS implementation as well as possible ways to address the same. It also identifies emerging typologies on the use of virtual assets for terrorist financing.

BSFIs are expected to use this guidance paper in strengthening their existing Anti-Money Laundering/Counter Terrorism and Proliferation Financing (AML/CTPF) controls to effectively implement TFS.

For information and guidance.

 Digitally signed by
Chuchi G. Fonacier
Date: 2022.09.05
17:55:35 +08'00'

CHUCHI G. FONACIER
Deputy Governor

05 September 2022

Att: a/s



BANGKO SENTRAL NG PILIPINAS

TARGETED FINANCIAL SANCTIONS IMPLEMENTATION

A THEMATIC REVIEW REPORT
SEPTEMBER 2022



TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	SCOPE OF THE THEMATIC REVIEW.....	2
III.	EXECUTIVE SUMMARY	2
IV.	REGULATORY EXPECTATIONS AND KEY OBSERVATIONS.....	3
V.	TYOLOGIES.....	9
VI.	CHALLENGES AND POSSIBLE SOLUTIONS.....	11
VII.	CONCLUSION AND WAY FORWARD.....	12

I. INTRODUCTION

Targeted financial sanctions (TFS) are among the key focus areas in the country's anti-money laundering/counter terrorism and proliferation financing (AML/CTPF) regime, in general, and by the Bangko Sentral ng Pilipinas (BSP)-supervised financial institutions (BSFIs), in particular. In its June 2022 statement, the Financial Action Task Force (FATF) highlighted that the Philippines should continue to work on implementing its action plan to address its strategic deficiencies, including by, among others, enhancing the effectiveness of the TFS framework for both terrorist financing (TF) and proliferation financing (PF).¹

It may be recalled that in 2020, the BSP conducted its first thematic review on TF and PF and implementation of TFS covering mostly universal and commercial banks. Based on the results, the BSP published guidance papers entitled "Strengthening Implementation of Targeted Financial Sanctions and Proliferation Financing Risk Management Framework" and "Enhancing the Control Framework on Terrorist Financing" through Memorandum No. M-2021-015 dated 16 March 2021.

This report presents the progress and developments on the sector's efforts and initiatives to understand their TFS obligations and implement TFS to prevent designated persons from accessing and/or using the financial system.

The Philippine Legal Framework

The main legal framework for TFS in the Philippines includes the following:

- Republic Act (R.A.) No. 9160 or the Anti-Money Laundering Act (AMLA), as amended;
- R.A. No. 10168 or The Terrorism Financing Prevention and Suppression Act of 2012 (TFPSA); and
- R.A. No. 11479 or The Anti-Terrorism Act of 2020 (ATA)

For uniform and effective implementation by BSFIs, the Anti-Money Laundering Council (AMLC) and the BSP issued TFS-related regulations and guidance papers. For example, TFS-related regulations have been issued to strengthen TFS implementation, such as the a) AMLC Regulatory Issuance (ARI) A, B, and C No. 01 dated 30 January 2021 amending certain provisions of the 2018 Implementing Rules and Regulations of the AMLA; b) ARI No. 02 dated 31 January 2021 amending certain provisions of ARI No. 04, Series of 2020²; c) 2021 Sanctions Guidelines on TFS dated 03 March 2021; and d) ARI No. 05 dated 28 July 2021 on guidelines for de-listing and unfreezing procedures. The BSP also issued frequently asked question (FAQ) on TFS through Memorandum M-2022-007 dated 02 Feb 2022 to enhance awareness and understanding by BSFIs of their TFS obligations.

¹ <https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2022.html#Philippines>

² Freeze Order for Potential Target Matches under the United Nations Security Council Consolidated Lists (Targeted Financial Sanctions)

II. SCOPE OF THE THEMATIC REVIEW

This follow through thematic review focused on two key areas. First, it assessed covered BSFIs' progress on TFS implementation, including their level of compliance post issuance of related regulations and guidance papers. Second, it sought to understand and compare existing policies, practices and challenges faced by BSFIs in implementing TFS, as well as possible ways to address the same.

Given the rule-based application of the TFS requirements, this review covered a broader number and type of BSFIs including less complex banks as well as non-bank financial institutions (NBFIs) such as money service businesses (MSBs), electronic money issuers (EMIs) and virtual asset service providers (VASPs).

III. EXECUTIVE SUMMARY

The results of this thematic review highlight the significant headway achieved by the BSFIs in terms of TFS implementation. Large and complex BSFIs have established policies and procedures to support implementation of the requirements of TFS and have installed sanction screening system with due regard to the complexity and nature of their operations. Meanwhile, simple BSFIs have adopted basic TFS-related policies particularly on onboarding screening with scope for improvements in terms of institutional TFS risk assessment, policies and dissemination, sanctions database maintenance, and scrubbing. The level of TFS and sanctions evasion risks, though, for these simple BSFIs are noted to be lower based on the profile of their customer base and results of review/risk assessment. Good practices and the areas for improvement on key TFS processes from risk identification/assessment to name match handling and freezing were detailed as practicable insights for BSFIs in further reinforcing their TFS framework. With the appropriate technical assistance, continuous engagements, monitoring and guidance, the identified scope for improvements can be feasibly addressed as observed in this thematic review.



Some typologies on the use of virtual assets in TF as an emerging risk trend were also noted in this review. Red flag indicators were developed to guide BSFIs in designing measures to detect, mitigate and manage risks arising from the use of virtual assets for TF. BSFIs are expected to consider this information in their risk mitigation strategies.

The notable progress in TFS understanding and implementation processes is the outcome of concerted efforts of all the stakeholders involved, mainly the BSFIs, industry associations and relevant government agencies. The various outreach sessions and continuing supervisory engagements, as well as the release of the 2021 guidance papers and the recent BSP and AMLC regulatory issuances, have provided specific guidance in implementing TFS for both complex and simple BSFIs. These activities should be sustained, along with the close cooperation and collaboration of all stakeholders, to address the identified challenges and continue this positive trajectory towards TFS understanding and implementation. With this, the BSFIs will be equipped with the necessary measures to prevent designated persons/entities from accessing and moving their funds through the financial system and to curb their illegal activities.

IV. REGULATORY EXPECTATIONS AND KEY OBSERVATIONS

Regulatory Expectation No. 1 (Institutional Risk Assessment or IRA): BSFIs shall conduct sanctions risk assessment, including for TFS on TF and PF which can be conducted as part of the overall IRA. TFS risk assessment pertains to the identification and evaluation of sanctions risk or risks of potential breach, non-compliance/non-implementation, or evasion of TFS obligations, and taking appropriate mitigating measures commensurate with the level of identified risks.

Large and complex BSFIs conduct annual or biennial IRA generally with adequate coverage of TF/PF and sanctions evasion risks. Simple BSFIs have either completed their IRA with needed enhancement on sanctions evasion risks or are still in the process of completing their IRA.



 <p>Good Practices</p>	 <p>Scope for Improvement</p>
<ul style="list-style-type: none"> (i) Including sanctions risk assessment to determine TFS vulnerability and assess risk direction apart from net risk; (ii) Considering the number of blacklisted and grey-listed customers based on suspicious transaction reports (STRs) filed in the last three (3) years; (iii) Conducting risk assessment on a per scenario basis with separate assessments for TF and PF; (iv) Formulating action plans for identified gaps and adoption of mitigating measures; (v) Managing TFS risks by engaging with the global law enforcement authorities where the BSFI has operations, maintaining a strong watchlist database, and implementing specific controls. 	<p>Consider to include:</p> <ul style="list-style-type: none"> (i) Geographical factors such as source and destination of transactions to identify exposure to sanctioned/cautioned countries and high-risk regions; (ii) Relevant studies/risk assessment reports such as the Second National Risk Assessment, the MSB Sector ML/TF Risk Assessment, and the 2021 Terrorism and TF Risk Assessment.

Box 1. IRA Methodology

Bank A has advanced TFS risk assessment. It developed risk criteria factors to determine specific vulnerabilities related to TFS, such as timing of scrubbing, number of name match and clients connected with STRs related to TF/PF, as well as timing of ST reporting and submission of return on freeze order.



Regulatory Expectation No. 2 (Policies and Dissemination): Based on the IRA results, BSFIs shall adopt proportionate and risk-based sanctions policies and procedures approved by the Board of Directors or equivalent body/authority to ensure that TFS implementation is in line with the BSFI's risk appetite and identified sanctions risk. Likewise, BSFIs shall conduct effective awareness and training programs on relevant sanctions risks and compliance with TFS obligations.

Large and complex BSFIs have generally acceptable TFS-related policies and dissemination. Meanwhile, simple BSFIs have basic TFS-related policies particularly onboarding screening but need improvements on other policy and training areas.

 <p>Good Practices</p>	 <p>Scope for Improvement</p>
<ul style="list-style-type: none"> (i) Timely updating of policies to align with latest TFS-related issuances; (ii) Mandatory and timely screening/checking the names of all prospective/existing customers, including authorized signatories and beneficial owners; (iii) Adequate reporting to the Board/ Management that includes TFS matters; (iv) Including TFS in training materials, covering TFS regulations, studies, common red flags and emerging typologies on TF/PF as well as full attendance by employees in these trainings; (v) Using email blast, group chat, vlog type media, and other modern channels for dissemination of new designations. 	<ul style="list-style-type: none"> (i) Institute process to ensure timely updating of policies and training materials to cover newly issued TFS-related regulations; (ii) Adopt customized training program commensurate with BSFI's risk profile and complexity for personnel performing TFS-related function.

Regulatory Expectation No. 3 (Systems): Risk-based measures should be adopted to support full implementation of TFS requirements. Section 911/911-Q of the Manual of Regulations for Banks/Manual of Regulations for Non-Bank Financial Institutions requires all covered persons to adopt an AML/CTPF monitoring system that is appropriate to their risk profile and business complexity. Universal and commercial banks and complex covered persons shall adopt an electronic AML system capable of monitoring risks associated with ML/TF/PF, which include functionality on, among others, watch list monitoring that checks transfer parties (originator, beneficiary, and narrative fields) and the existing customer database for any listed undesirable individual or corporation. BSFIs which are not required to have an electronic system of flagging and monitoring transactions shall ensure that they have the means to identify transactions or customers as required for monitoring and reporting.



Large and complex BSFIs have generally acceptable automated or semi-automated screening and monitoring systems. Meanwhile, simple BSFIs need to strengthen their manual screening systems.

 <p>Good Practices</p>	 <p>Scope for Improvement</p>
<ul style="list-style-type: none"> (i) Using screening system commensurate to BSFI's business model and risk profile such as automated screening and monitoring systems capable of real time onboarding scanning and comprehensive transaction screening for complex BSFIs, and acceptable manual screening and monitoring system for simple BSFIs; (ii) Adopting fuzzy logic in the screening system (<i>ranging from 72% to 93% with 85% as the most commonly adopted percentage</i>); Few BSFIs use risk-based fuzzy logic with lower 	<ul style="list-style-type: none"> (i) Resolve incompatibility of screening and monitoring system with legacy core system to complete automation projects; (ii) Improve screening system by considering the nature of operations and adopting fuzzy logic in screening systems for more reliable and efficient sanctions screening.

percentages for high-risk name matching [e.g., United Nation Security Council (UNSC), Anti- Terrorism Council (ATC), etc.] and higher percentage for low-risk name matching.	
--	--

Regulatory Expectation No. 4 (Sanctions Database Maintenance): BSFIs shall adopt risk-based measures that support full implementation of TFS requirements, including electronic and/or manual screening tools that are commensurate to the BSFI’s risk profile and complexity to ensure, among others, timely updating of sanctions lists, conduct of sanctions screening and implementation of TFS without delay. At a minimum, the sanctions database should include the UNSC Consolidated List and domestic designations, and their successor resolutions.³

Large BSFIs either with vendor subscription or internal sanctions database have generally acceptable sanctions database maintenance. Simple BSFIs are using internal sanctions database with some still needing enhancement on timely updating.

 Good Practices	 Scope for Improvement
<ul style="list-style-type: none"> (i) Subscribing to third party vendors (<i>with varying cost, depending on functionality and provider</i>) for screening systems that include development and maintenance of sanctions database with notification system (e.g., email) on new additions or updates and/or daily updating of global sanctions; (ii) Using manually developed internal sanctions database supported by adequate policies, dedicated personnel, and back up mechanism; (iii) Performing periodic quality assurance review or testing on the completeness of sanctions list and timeliness of updating; (iv) Information sharing by international tie up partners of names of persons of interest who are under investigation by law enforcement agencies in their countries of operation. 	<ul style="list-style-type: none"> (i) Adopt measures to ensure that sanctions list updates, including those issued during holidays or weekends, are timely checked/captured and designate responsible officers; (ii) Develop internal screening system appropriate to BSFI’s risk profile or explore available third-party vendors that can provide minimum TFS requirements and meet the BSFI’s cost consideration/budget.



Regulatory Expectation No. 5 (Name screening and scrubbing):⁴ The screening should be conducted (i) during the establishment of a relationship or opening of an account, or at the latest, prior to the first transaction; (ii) periodically over the course of the relationship, especially whenever new designations or updates are

³ Said lists cover (1) UNSC Consolidated List that includes UNSC Resolutions 1267/1989 (Al Qaeda), 1988 (Taliban) and 2253 (ISIL Daesh) for TFS on terrorism and terrorist financing; (2) UNSC Consolidated List that includes UNSC Resolution Numbers 1718 of 2006 (DPRK) and 2231 of 2015 (Iran) for TFS on PF; (3) Domestic designations (or those that are designated by the ATC pursuant to UNSC Resolution 1373, Section 25 of the ATA, Rule 15.b of the IRR of the TFPISA) and those proscribed by the Court of Appeals under Section 26 of the ATA.

⁴ Name screening and scrubbing are terms that are usually interchanged but for this guidance paper, name screening shall mean the traditional scanning of customer name against sanctions lists while scrubbing (reverse of name screening) is the scanning of new additions or the entire updated sanctions lists against the client database.

issued. All new designations should be screened against existing customer base without delay; and (iii) whenever there are updates to the client’s information such as change of Ultimate Beneficial Ownership (UBO), authorized signatories, or change in the names of clients⁵.

Large and complex BSFIs have generally acceptable name screening and scrubbing policy and implementation. Meanwhile, simple BSFIs need to strengthen their name screening and scrubbing policy/implementation.

 Good Practices	 Scope for Improvement
<ul style="list-style-type: none"> (i) Performing name screening of authorized signatories (AS), key officers and UBO that is made possible with the creation of Customer Information File (CIF) or internally developed software; (ii) Adopting screening systems that cover real time onboarding screening (including UBO and AS), automated periodic scrubbing (daily and weekly), and trigger-initiated scrubbing (e.g., change in customer information or update of the sanctions list); (iii) Integrating walk-in customers in the client databases which are then subjected to scrubbing. 	<ul style="list-style-type: none"> (i) Resolve interface limitations of the screening and scrubbing system with the legacy core system; (ii) Document and ensure audit trail on the conduct of screening, and test the reliability of logs in electronic systems; (iii) Enhance manual screening systems by defining trigger events, and assigning adequate personnel to timely scrub customers against new designations; (iv) Explore ways to capture AS and UBO in periodic scrubbing.



Regulatory Expectation No. 6 (Transaction Screening):⁶ At a minimum, BSFIs should conduct sanctions screening on (i) the names/aliases/country of residence or operations of their customers, including the names/aliases of beneficial owners or any person purporting to act on behalf of the customer, and their authorized signatories; (ii) transactors/non-accountholders who transact with the BSFI; and (iii) counterparties/other credentials or information in wire transfers or trade transactions, among others. Moreover, BSFIs should, at a minimum, screen the names/aliases/country of residence/operations of the non-customer remitter, beneficiary and intermediaries, and other information contained in the payment message of a cross-border transaction, subject to applicable rules⁷.

Most complex BSFIs perform transaction screening including for non-client counterparties and prior to fund transfer. Meanwhile, some simple BSFIs conduct transaction screening on fund transfers but does not include non-client counterparties partly due to system’s limitation or inadequate policy.

⁵ Memorandum M-2022-007 dated 02 Feb 2022 (FAQ on TFS)



⁶ Transaction screening is used to identify transactions involving targeted individuals or entities while name screening is designed to identify targeted individuals or entities during on-boarding or the lifecycle of the customer relationship with the financial institution, as differentiated by the Wolfsberg Group.

⁷ Memorandum M-2022-007 dated 02 Feb 2022 (FAQ on TFS)

 Good Practices	 Scope for Improvement
<ul style="list-style-type: none"> (i) Adopting automated transaction screening of both remitters and beneficiaries prior to wire transfers, subject to applicable rules for National Retail Payment System (NRPS) transactions; (ii) Screening transactions of occasional/non-accountholder clients (e.g., buyers of acquired assets or foreign currency); (iii) System blocking on transaction attempts by transactors with name match; (iv) On cross-border transfers, strictly requiring minimum payment information to aid in smooth screening by beneficiary institutions on ultimate senders; (v) For VASPs, subscribing to relevant vendors that facilitate sending and receiving of transaction information, which are subjected to sanction screening, to comply with the global travel rule requirement. 	<p>Adopt comprehensive implementing guidelines on transaction screening, and define mandatory parties to be included (e.g., both senders and beneficiaries of wire transfers including non-accountholders) and screening points (e.g., prior to fund transfer or movement of value), subject to applicable rules for NRPS transactions.</p>

Regulatory Expectation No. 7 (Name Match Handling and Freezing): BSFIs should have appropriate policies, procedures and processes to guide personnel in handling name matches, freezing actions in case of potential target match and target match, as well as filing of returns and STRs, as provided under existing regulations.

Improving practices in resolving name and potential target matches, with active coordination with the AMLC Secretariat.

 Good Practices	 Scope for Improvement
<ul style="list-style-type: none"> (i) Actively coordinating with the AMLC and using two levels of disambiguation; (ii) Embedding system capability to block transactions, maintain log of all transactions that were put on hold, and preserve emails and communications on the disposition of matches; (iii) Timely disposition of matches in coordination with the originating institution. 	<ul style="list-style-type: none"> (i) Adopt risk-based guidelines in handling name matches, potential target match and target match, and institutionalize process of coordination with the AMLC as part of the disposition procedures; (ii) File STRs on previous transactions of a potential target match or target match; (iii) Designate responsible officers in the disposition of name matches and ensuring audit trail.

Box 2. Potential Target Match Handling

BSFI A's policy provides that to be considered as "target match," most of the customer details should match such as names; aliases; date of birth; last known address; ID details; nationality; and nature of work/employment details. To trigger handling as "potential target match," the name and last known address, at least, should match. BSFI A encountered a case of "potential target match". Accordingly, the account was immediately frozen and an STR was filed. It also notified the AMLC regarding the potential target match. Upon further verification, it was confirmed that it was not a target match and the account was unfrozen accordingly. Availability of additional identifier such as photograph from the AMLC fast-tracked the disposition process.

V. TYPOLOGIES

This review also noted some typologies on the use of virtual assets in TF which may be used by BSFIs in understanding the schemes and TF activities using virtual assets. BSFIs are expected to develop sound risk management framework in mitigating TF risk exposures on the use of virtual assets. Based on these typologies, red flag indicators were developed to guide BSFIs in developing measures to prevent and detect TF activities using virtual assets.

Typology 1: Funds from organized crime converted to crypto currency

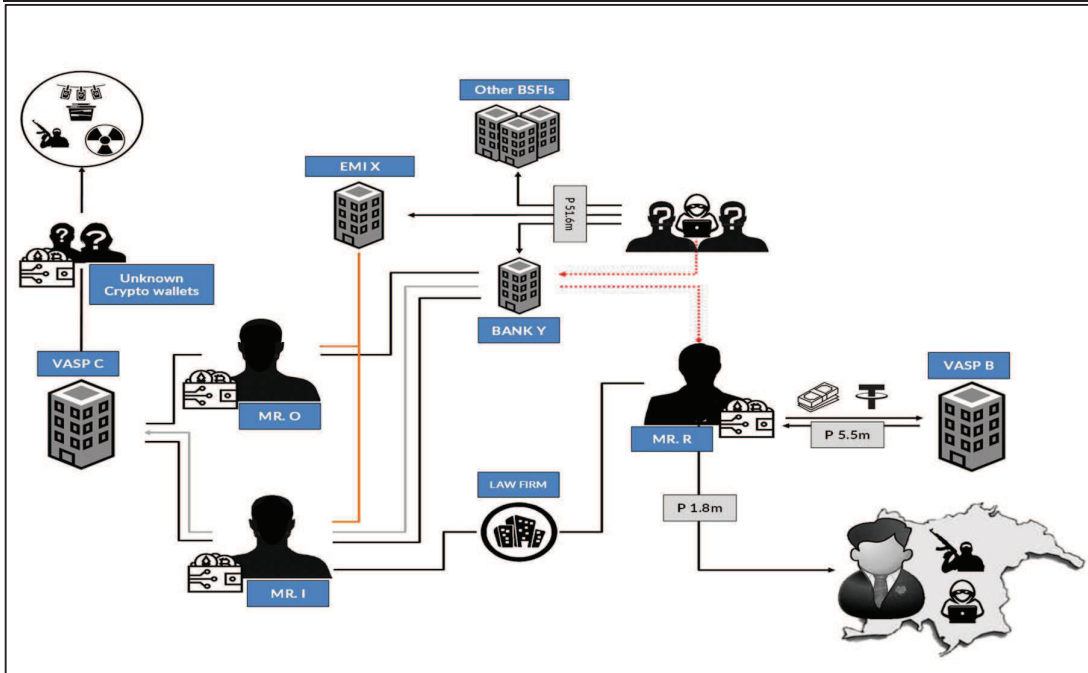
Profile: Mr. I and Mr. O posed as Nigerian students in the Philippines and enrolled in provincial colleges. Mr. R is a 29-year-old Filipino crypto trader with fund transfers from Nigerians suspectedly involved in a hacking incident. Mr. R and his counterpart Nigerians used a common law firm based on their transaction patterns in Bank Y.

Transactions: Mr. I was noted to have high volume cash in transactions in VASP C via his bank account in Bank Y ranging from P11,000 to P2,200,000. Similarly, Mr. O has high-volume cash in transactions in VASP C. Meanwhile, Mr. R had sale transactions of a crypto currency (a form of cash out) with VASP B totaling PHP5.5 million after Mr. I sent fund transfers to his accounts. Mr. R also sent two outward remittance transactions totaling P1.8 million to a foreign politically exposed person of Country S which was high risk for TF and hacking.

Funds Flow: Based on initial investigation, significant part of the proceeds of a hacking incident allegedly ended up in unidentified crypto wallets as planned, coordinated, and processed by Mr. I, O and other anonymous members of the group involved in the hacking.

Red Flags: 1) Based on investigations by EMI X, 56% of its more than 2,500 Nigerian accounts were found to have suspicious indicators and patterns (*e.g., voluminous transactions not commensurate to declared profile*) like that of Mr. I and Mr. O, and other Nigerians involved in cybercrimes and fraudulent activities; 2) Customers posing as Nigerian students but accumulating large amount of funds and active in crypto trading; 3) In a 2020 Interpol study (available in public domain*), Nigerian crime syndicates usually convert their crime proceeds to crypto assets and material portion eventually used in ML/TF/PF activities.

*<https://www.interpol.int/content/download/15525/file/Online%20African%20Organized%20Crime%20from%20Surface%20to%20Darkweb-17.08.2020.pdf>



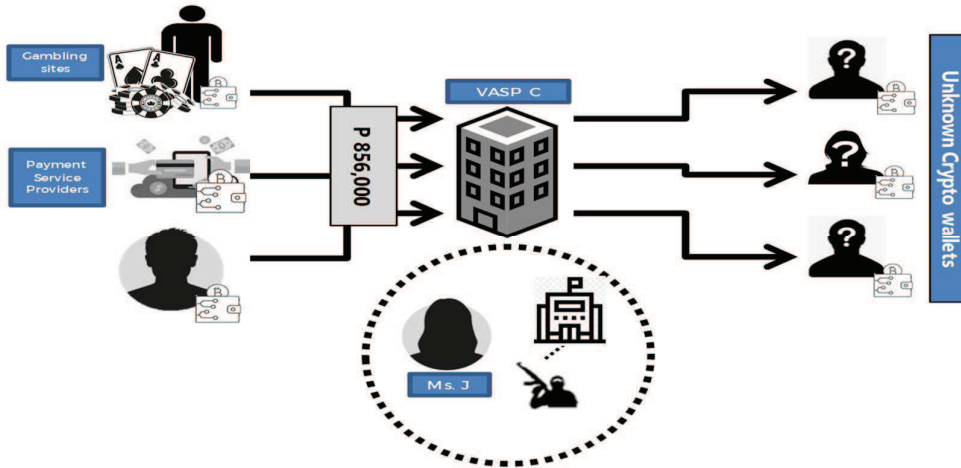
Typology 2: Affiliation to non-profit organization, illicit sources of funds and conversion to crypto currency

Profile: Ms. J is a project director of a non-profit organization which was suspected by law enforcement agencies to be involved in TF by supporting activities of a group in southernmost part of the country.

Transactions: Crypto account in VASP C of Ms. J was receiving cryptocurrencies (mostly bitcoin) from more than 300 external crypto wallets and other crypto accounts in VASP C accumulating to around P856,000.

Funds Flow: Funds were accumulated in Ms. J's account in VASP C and eventually transferred to crypto wallets with unknown addresses.

Red Flags: 1) Origin of some crypto currencies traced from gambling sites and payment service providers which were used as payment gateway of sites involved in gambling, illegal investment schemes, and online pornography, among others; 2) Affiliation to a non-profit organization but origin of funds was not aligned or even conflicting with the nature of the organization; 3) Accumulation of crypto currencies and transfers to crypto wallets with unknown addresses.



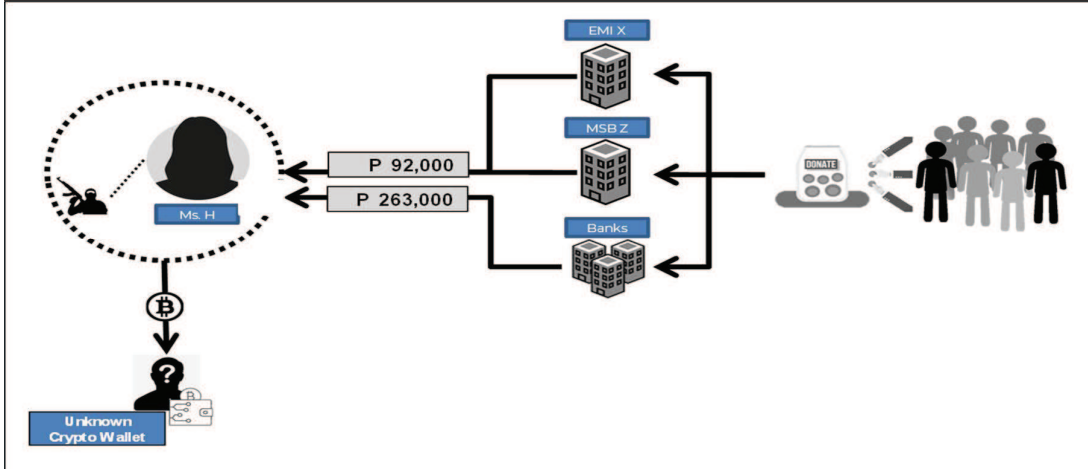
Typology 3: Funds from donation scam converted to crypto currency

Profile: Ms. H, a female college student in a location high risk for TF, was under investigation for alleged involvement in TF activities of a designated group.

Transactions: Donations from various senders coursed through EMI X and MSB Z (in small amounts not exceeding P2,000) for four months aggregated to around P92,000. Ms. H also received funds from various bank transfers that accumulated to around P263,000.









Funds Flow: It appeared that the accumulated funds were not used for the advertised purposes but were used to purchase cellphone load and were withdrawn by Ms. H. A part of the funds was used to purchase fraction of bitcoin which was eventually transferred to crypto wallet with unknown address.

Red Flags: 1) Posing as a member of a non-profit organization raising funds from donations for victims of calamities or for youth programs (donation scam as modus operandi); 2) Student profile but accumulates large amount of funds in a location known for terrorist activities; (3) Purchase and transfer of crypto currency to crypto wallet with unknown address.



VI. CHALLENGES AND POSSIBLE SOLUTIONS

TFS implementation presents difficulties to the sector which need to be recognized and addressed. This thematic review disclosed the following challenges in implementing TFS. We also present some possible solutions that the concerned stakeholders can undertake to improve TFS implementation.

 KEY RISK AREAS	 CHALLENGES	 TIPS/REMEDIES
 Institutional Risk Assessment	<ul style="list-style-type: none"> • Access or knowledge in applicable methodology in the gathering and analysis of data 	<ul style="list-style-type: none"> • Refer to guidance paper on the conduct of IRA, as well as available reference materials on IRA methodology for the sector • Participate in AML trainings that cover IRA • Engage industry associations, experts on IRA, and discuss/engage with supervisors
 Policies and Dissemination	<ul style="list-style-type: none"> • Lead time in catching up with evolving regulatory requirements • Access to studies and typologies 	<ul style="list-style-type: none"> • Designate personnel to ensure timely adoption of relevant regulatory issuances • Study relevant issuances/studies such as BSP's FAQ on TFS, and TF risk assessment reports • Participate in TFS related trainings conducted by the industry associations, BSP and AMLC, among others • Enroll in the AMLC's Public-Private Partnership on information sharing protocol
 Sanctions Database Maintenance	<ul style="list-style-type: none"> • Availability of vendor subscriptions that are cost-effective for small and simple BSFIs 	<ul style="list-style-type: none"> • Conduct extensive inquiry/market research on available and less costly vendor subscription that meets the minimum TFS requirements and commensurate to the risk profile of simple BSFIs
 Systems	<ul style="list-style-type: none"> • Access to studies that define reliable and optimum percentages for fuzzy matching 	<ul style="list-style-type: none"> • Adopt fuzzy logic in the screening system appropriate to the BSFI's risk profile (85% is the most common percentage used based on this review) while few BSFIs even use risk-based fuzzy logic setting lower percentages for high-risk matching
 Name Match Handling	<ul style="list-style-type: none"> • Availability of secondary identifiers of new designations needed for speedy disposition of name matches and/or timely uploading to screening systems 	<ul style="list-style-type: none"> • Coordinate with the AMLC on possible dissemination of other identifiers in addition to name for new domestic designations

VII. CONCLUSION AND WAY FORWARD

In the past three years, significant progress on TFS implementation was made possible due to the passage of additional enabling laws, release of related regulatory issuances and guidance papers, and focused interventions through industry engagements, outreach sessions and supervisory activities by the regulators. Likewise, the receptiveness and cooperation of the financial institutions and industry associations jumpstarted the successful implementation of the intended programs.

As we move forward, the challenge is to achieve sustainability as TFS risk is evolving and TFS implementation is a continuing obligation. BSFIs are therefore expected to establish and/or continuously improve their respective TFS framework to effectively implement TFS obligations. This includes calibration of existing AML processes to mitigate emerging risks such as the use of virtual assets in TF activities. Continuous collaborative and proactive engagement among industry players, regulators and other stakeholders should be pursued to continually address the challenges noted. Finally, the Board and Senior Management of BSFIs are expected to continuously provide high-level direction and adequate support and resources in their respective institutions to further strengthen safeguards and prevent the designated persons from accessing and moving funds in financial channels for TF and PF activities.