



BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR
FINANCIAL SUPERVISION SECTOR

MEMORANDUM NO. M-2021-017

To : All BSP-Supervised Financial Institutions (BSFIs)


Subject : 3rd Sectoral Risk Assessment for Banks and Other BSP-Supervised Financial Institutions

The Monetary Board, in its Resolution No. 269 dated 04 March 2021, approved the attached report on the 3rd money laundering (ML)/terrorist financing (TF)/proliferation financing (PF) sectoral risk assessment (SRA) for banks and other BSP-supervised financial institutions¹ (BSFIs), in line with the thrust of the Bangko Sentral to promote effective risk management systems to combat ML/TF/PF.

The assessment highlights (a) the ML/TF/PF threats and vulnerabilities of banks and other BSFIs, as well as consequences of criminal activities; and (b) the overall ML/TF/PF risks associated with the other priority areas such as trade-based ML/TF/PF, implementation of the targeted financial sanctions (TFS) regime, and assessment of financial inclusion products. The SRA aims to further enhance and update the stakeholders' understanding of the extent of proceeds of unlawful activities being coursed through BSFIs and their vulnerabilities to be used as channels/conduits for these proceeds. This will likewise inform risk-based supervisory and institutional strategies and priorities to address the identified ML/TF/PF risks.

BSFIs are expected to consider the findings and conclusions in the report in their respective institutional risk assessments and implement necessary measures to address the identified risk areas.

For information and guidance.

 Digitally signed
by Chuchi G.
Fonacier
Date: 2021.03.17
15:46:25 +08'00'

CHUCHI G. FONACIER
Deputy Governor

17 March 2021

Att: a/s

¹ Other BSFIs include non-bank financial institutions (NBFIs) namely, trust entities, non-stock savings and loan associations (NSSLAs), non-bank electronic money (e-money) issuers (EMIs), virtual currency exchanges (VCEs)/virtual assets service providers (VASPs), pawnshops and operators of payment systems. Risk assessment of MSBs was conducted separately by the AMLC, in coordination with the BSP



BANGKO SENTRAL NG PILIPINAS

MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING

SECTORAL RISK ASSESSMENT

MARCH 2021

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE


5/12/21

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

TABLE OF CONTENTS

| | |
|--|-----------|
| GLOSSARY OF TERMS | 4 |
| BACKGROUND | 7 |
| OBJECTIVES | 8 |
| SCOPE..... | 8 |
| ASSESSMENT METHODOLOGY AND DATA COLLECTION..... | 9 |
| EXECUTIVE SUMMARY | 10 |
| 1 OVERVIEW OF THE SECTOR..... | 13 |
| 2 SECTORAL THREAT ANALYSIS..... | 16 |
| PREDICATE OFFENSES | 16 |
| TERRORIST FINANCING | 23 |
| PROLIFERATION FINANCING..... | 23 |
| 3 VULNERABILITY..... | 24 |
| 3.1. BANKING SECTOR..... | 24 |
| ASSESSMENT OF CONTROLS | 24 |
| PRODUCTS AND SERVICES VULNERABILITY | 32 |
| 3.2. OTHER FINANCIAL INSTITUTIONS..... | 36 |
| 3.2.1. NON-BANK ELECTRONIC MONEY ISSUERS | 36 |
| ASSESSMENT OF CONTROLS | 37 |
| PRODUCTS AND SERVICES VULNERABILITY..... | 40 |
| 3.2.2. VIRTUAL CURRENCY EXCHANGES/VIRTUAL ASSETS SERVICE PROVIDERS..... | 41 |
| ASSESSMENT OF CONTROLS | 42 |
| PRODUCTS AND SERVICES VULNERABILITY..... | 46 |
| 3.2.3. TRUST ENTITIES AND LEGAL ARRANGEMENTS | 47 |
| ASSESSMENT OF CONTROLS | 48 |
| PRODUCTS AND SERVICES VULNERABILITY..... | 51 |
| 3.2.4. PAWNSHOPS | 52 |
| ASSESSMENT OF CONTROLS | 53 |
| 3.2.5. NON-STOCK SAVINGS AND LOANS ASSOCIATIONS | 56 |
| ASSESSMENT OF CONTROLS | 57 |
| PRODUCT VULNERABILITY | 60 |
| 3.2.6. OPERATORS OF PAYMENT SYSTEMS..... | 61 |
| 4 SPECIAL/FOCUS AREAS..... | 68 |
| 4.1. TRADE-BASED MONEY LAUNDERING..... | 68 |
| TRADE ENVIRONMENT..... | 69 |
| TRADE-BASED ML/TF/PF THREAT | 69 |
| VULNERABILITIES OF THE BANKING AND MSB SECTORS TO TRADE-BASED ML/TF/PF..... | 73 |

| | |
|---|-----------|
| 4.2. TARGETED FINANCIAL SANCTIONS ON TERRORISM, TERRORIST FINANCING AND PROLIFERATION FINANCING..... | 75 |
| THREAT ASSESSMENT | 75 |
| VULNERABILITY ASSESSMENT | 76 |
| 5 FINANCIAL INCLUSION | 78 |
| LANDSCAPE | 79 |
| FINANCIAL INCLUSION PRODUCTS..... | 80 |
| 6 TERRORIST FINANCING RISK | 85 |
| THREAT ASSESSMENT | 85 |
| VULNERABILITY ASSESSMENT..... | 88 |
| 7 IMPACT ASSESSMENT | 89 |

**CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE**

 3/19/21

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

GLOSSARY OF TERMS

| | |
|-------------|---|
| AAGR | Annual Average Growth Rate |
| ACH | Automated Clearing House |
| ACQ | AML/CFT Questionnaire |
| ACT | AML/CFT Template |
| ADB | Asian Development Bank |
| APCB | Association of Philippine Correspondent Banks |
| AML/CFT | Anti-Money Laundering and Countering the Financing of Terrorism |
| AML/CFT/CPF | Anti-Money Laundering and Countering the Financing of Terrorism and Proliferation Financing |
| AMLA | Anti-Money Laundering Act of 2001 (AMLA), as amended |
| AMLC | Anti-Money Laundering Council |
| AMLCs | Anti-Money Laundering Council Secretariat |
| API | AMLC Procedural Issuance |
| ARI | AMLC Regulatory Issuance |
| ARRS | AML Risk Rating System |
| ASG | Abu Sayyaf Group |
| ASN | Affiliate Switch Network |
| ATM | Automated Teller Machine |
| AUM | Assets Under Management |
| B2B | Business-to-Business |
| BDA | Basic Deposit Account |
| BIR | Bureau of Internal Revenue |
| BMPE | Black Market Peso Exchange |
| BOC | Bureau of Customs |
| BOD | Board of Directors |
| BSFI | BSP-Supervised Financial Institution |
| BSP | Bangko Sentral ng Pilipinas |
| CBR | Correspondent Banking Relationship |
| CDA | Cooperative Development Authority |
| CDD | Customer Due Diligence |
| CDO | Cease and Desist Order |
| COVID-19 | Corona Virus Disease 2019 |
| COR | Certificate of Registration |
| CPI | Corruption Perceptions Index |
| CPP-NPA | Communist Party of the Philippines – New People’s Army |
| CSO | Clearing Switch Operator |
| CTR | Covered Transaction Report |
| CP | Covered Person |
| D/C | Documentary Collection |
| D/R | Direct Remittance |
| DNFBP | Designated Non-Financial Businesses and Professions |
| DOS | Directors, Officers and Stockholders |
| DPRK | Democratic People’s Republic of Korea |
| DTI | Department of Trade and Industry |
| DUG | Dual Use of Goods |
| ECQ | Enhanced Community Quarantine |
| EDD | Enhanced Due Diligence |
| E-Banking | Electronic Banking |
| E-Commerce | Electronic Commerce |
| E-Money | Electronic Money |
| E-Wallet | Electronic Wallet |
| EMI | Electronic Money Issuer |
| eFPS | Electronic Filing and Payment System |
| EPFS | Electronic Payment and Financial Services |
| FATF | Financial Action Task Force |
| FX | Foreign Exchange |

**CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE**



JOSE MICHAEL E. CAMACHO

Bank Officer II, RMD

Administrative Services Department

Page | 4

| | |
|---------|---|
| FXD | Foreign Exchange Dealer |
| GBL | General Banking Law |
| GDP | Gross Domestic Product |
| GFI | Global Financial Integrity |
| GIS | General Information Sheet |
| IAD | Independent ATM Deployer |
| IBP | Integrated Bar of the Philippines |
| IC | Insurance Commission |
| IMA | Investment Management Account |
| INR | Interpretative Note |
| IP | Intellectual Property |
| IRA | Institutional Risk Assessment |
| I-SIP | Inclusion, Stability, Integrity and Protection Framework |
| KFR | Kidnapping for Ransom |
| KYC | Know-Your-Customer |
| KYE | Know-Your-Employee |
| L/C | Letter of Credit |
| LEAs | Law Enforcement Agencies |
| LEG | Legal Evaluation Group |
| LGU | Local Government Unit |
| LOC | Letter of Commitment |
| LTO | Land Transportation Office |
| MB | Monetary Board |
| MC | Money Changers |
| MER | Mutual Evaluation Report |
| MF | Microfinance |
| ML | Money Laundering |
| MOA | Memorandum of Agreement |
| MORB | Manual of Regulations for Banks |
| MORNBFI | Manual of Regulations for Non-Bank Financial Institutions |
| MORFXT | Manual of Regulations on Foreign Exchange Transactions |
| MRAS | ML/TF Risk Assessment System |
| MSB | Money Service Business |
| MTPP | Money Laundering and Terrorist Financing Prevention Program |
| MUP | Military and Other Uniformed Personnel |
| NACC | National AML/CFT Coordinating Committee |
| NACS | National AML/CFT Strategy |
| NALECC | National Law Enforcement Coordinating Committee |
| NBFI | Non-Bank Financial Institution |
| NBQB | Non-Bank with Quasi-Banking Function |
| NCR | National Capital Region |
| NGO | Non-Government Organization |
| NPA | Non-Performing Asset |
| NPL | Non-Performing Loan |
| NPP | Network Payment Processor |
| NPSA | National Payment Systems Act |
| NRA | National Risk Assessment |
| NRPS | National Retail Payment System |
| NSFI | National Strategy for Financial Inclusion |
| NSSLA | Non-Stock Savings and Loan Association |
| NOW | Negotiable Order of Withdrawal |
| O/A | Open Account |
| OFAC | Office of Foreign Assets Control |
| OFS | Other Fiduciary Services |
| OGB | Online Gaming Business |
| OPS | Operator of Payment System |
| OSEC | Online Sexual Exploitation of Children |
| OFI | Other Financial Institution |
| OTC | Over-the-Counter |
| OTP | One-Time-Password |

**CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE**

 3/19/21

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

| | |
|----------|---|
| PBS | Philippine Banking System |
| PCA | Prompt Corrective Action |
| PCOR | Provisional Certificate of Registration |
| PD | Presidential Decree |
| PEP | Politically Exposed Person |
| PF | Proliferation Financing |
| PhilPaSS | Philippine Payment and Settlement System |
| PhilPost | Philippine Postal Corporation |
| PNP | Philippine National Police |
| PSA | Philippine Statistics Authority |
| PhilSys | Philippine Identification System |
| POS | Point-of-Sale |
| PPPP | Public Private Partnership Program |
| PRC | Professional Regulation Commission |
| PSE | Philippine Stock Exchange |
| QR | Quick Response |
| RA | Republic Act |
| RBA | Risk-Based Approach |
| RCB | Rural/Cooperative Bank |
| RCL | Report on Crimes and Losses |
| RIRR | Revised Implementing Rules and Regulations |
| ROC | Report of Compliance |
| ROE | Report of Examination |
| RPAC | Rules of Procedure in Administrative Cases |
| RSA | Remittance Sub-Agent |
| RTC | Remittance and Transfer Company |
| RTGS | Real-Time Gross Settlement |
| SA | Supervisory Authorities |
| SAFr | Supervisory Assessment Framework |
| SAP | Social Amelioration Program |
| SDN | Specially Designated Nationals and Blocked Persons List |
| SEC | Securities and Exchange Commission |
| SFISC | Supervision of Financial Institutions Sub-Committee |
| SM | Senior Management |
| SOCTA | Serious and Organized Crimes Threat Assessment |
| SRA | Sectoral Risk Assessment |
| STR | Suspicious Transaction Report |
| SSS | Social Security System |
| SWIFT | Society for Worldwide Interbank Financial Telecommunication |
| TB | Thrift Bank |
| TBML | Trade-Based Money Laundering |
| TBPF | Trade-Based Proliferation Financing |
| TBTF | Trade-Based Terrorist Financing |
| TC | Trust Corporation |
| TE | Trust Entity |
| TF | Terrorist Financing |
| TFS | Targeted Financial Sanctions |
| TFPSA | Terrorist Financing Prevention and Suppression Act |
| TIP | Trafficking in Person |
| UBO | Ultimate Beneficial Owner |
| UITF | Unit Investment Trust Fund |
| UKB | Universal and Commercial Bank |
| UNSC | United Nations Security Council |
| UNSCR | United Nations Security Council Resolution |
| VA | Virtual Assets |
| VASP | Virtual Assets Service Provider |
| VC | Virtual Currency |
| VCE | Virtual Currency Exchange |
| WMD | Weapons of Mass Destruction |
| WB | World Bank |

**CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE**

 3/19/21

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

BACKGROUND

FATF Recommendation 1 (R.1) and its INR.1 require countries to identify, assess, and understand their ML, TF, and PF risks, take action and apply resources to ensure risks are mitigated effectively. Countries should therefore apply an RBA in implementing measures to prevent or mitigate ML/TF/PF that are commensurate with the risks identified. In particular, INR.1 provides that the ML/TF/PF risk identification and assessment should be on an ongoing basis in order to: (i) inform potential changes to the country's AML/CFT regime, including changes to laws, regulations, and other measures; (ii) assist in the allocation and prioritization of AML/CFT resources by competent authorities; and (iii) make information available for AML/CFT risk assessments conducted by financial institutions and DNFBPs.

Similarly, Section 3 of Rule 7 of RIRRs of the AMLA of 2001, as amended, provides that SAs shall conduct sectoral or sub-sectoral risk assessment to facilitate the preparation for the national risk assessment, or as it may deem necessary to determine, understand, mitigate, and manage the risks in their respective jurisdiction.

The BSP conducted its 1st SRA in 2014 (for the period 2011-2014) and 2nd SRA in 2017 (for the period 2015-2016), both in line with the NRA of the Philippines led by the AMLC. To update the results of the threat and vulnerability assessments in the 2nd NRA, the BSP conducted the 3rd SRA of banks and other BSFIs (*the sector*), which aims to understand and assess the emerging risks within the sector posed by current developments as well as changes in the ML/TF/PF landscape. The SRA is likewise in line with the NACS of the Philippines that aims, among others, for a strategic and collective response to the ML/TF/PF risks identified and provides for a whole-of-government approach in AML/CFT efforts.

OBJECTIVES

This SRA enables the BSP to identify and assess current ML/TF/PF “risk and context information” in the sector, the ML/TF/PF threats and vulnerabilities, as well as other significant ML/TF/PF developments involving the sector since the last NRA.

It also enables BSFIs to identify vulnerabilities and high-risk factors, analyze how these factors impact their businesses or the sector as a whole, and evaluate the associated ML/TF/PF risks. The SRA aims to enhance understanding of the possible prevalence of proceeds of unlawful activities being coursed through BSFIs and their vulnerabilities to be used as channels/conduits for these proceeds. This will likewise inform implementation of risk-based supervisory and institutional strategies and priorities to address the identified ML/TF/PF risks and typologies.

SCOPE

The BSP, in coordination with the AMLC and other relevant agencies or institutions, conducted the 3rd SRA of banks and other BSFIs. The scope of the SRA includes:

- a) Overall ML/TF risk assessment of the following BSFIs:
 - i. Banks;
 - ii. NBFIs included in the 2nd NRA of the Philippines, particularly trust entities and other legal arrangements, NSSLAs, non-bank EMLs and VCEs/ VASP; and
 - iii. Other FIs which are under BSP supervision and/or regulation, such as OPS¹, and pawnshops².
- b) Assessment of threat and vulnerability of priority areas such as *cash* and *cross-border* transactions as well as the *cross sectoral*³ linkages, TBML, TF, PF, implementation of the TFS regime, and financial inclusion products.

¹ As defined under R.A. No. 11127 or the NPSA, an operator refers to any person who provides clearing or settlement services in a payment system, or defines, prescribes, designs, controls or maintains the operational framework for the system.

² The risk assessment for pawnshops industry covers only its pawning activity. The remittance business of the pawnshops as corollary activity is covered in a separate risk assessment under the MSB industry.

³ Understanding and assessing the interconnection of different CPs within or across different sectors (such as banks, MSBs, DNFBPs, casinos, investment houses, insurance companies) and their interplay in the financial flows of proceeds of ML/TF/PF activities. Results were published through Memorandum M-2021-005 dated 13 January 2021 (<https://www.bsp.gov.ph/SitePages/Regulations/RegulationDisp.aspx?ItemId=4452>)

ASSESSMENT METHODOLOGY AND DATA COLLECTION

The methodology adopted for the SRA is largely shaped by the FATF guidance that risk is a function of three factors, namely *threat, vulnerability, and consequence*. Threat refers to the criminal elements that pose harm or can cause losses to the sector. Vulnerability refers to those attributes that can be exploited by the threat or may facilitate its activities. Consequence refers to the impact or harm that may be caused by the ML/TF/PF or underlying criminal activity. The Banking Sector Vulnerability Tool from the WB was also used in the vulnerability assessment.

This assessment involved using informed judgment considering the risk and context information of the Philippines, pertinent AML/CFT data, and discussions with relevant stakeholders. In this regard, the BSP used a combination of qualitative and quantitative data/information gathered from various sources, as follows:

- **Qualitative data.** These were drawn from content analyses and/or exercise of expert judgements of the BSP and key stakeholders. The ACQ was used to gather relevant AML/CFT information from BSFIs. Focus group discussions and presentations from select BSFIs likewise formed part of this assessment.
- **Quantitative data.** These include statistics for the period 2017 to 2019 (*with some requirements extending up to June 2020 as available and relevant to the assessment*). Primary data sources include existing prudential reports, ACT, CTRs and STRs statistics, typologies, investigation reports, and ML/TF cases provided by the AMLCS, as well as available strategic AML/CFT studies.

All UKBs as well as the top 20⁴ TBs and top 20⁴ RCBs participated in this SRA.⁵ These BSFIs represent 99 percent of the total assets of the entire Philippine banking system. Participation of other BSFIs, such as the NSSLAs, pawnshops, and non-bank EMLs, as well as the industry associations, relevant agencies, and SAs, was also solicited.

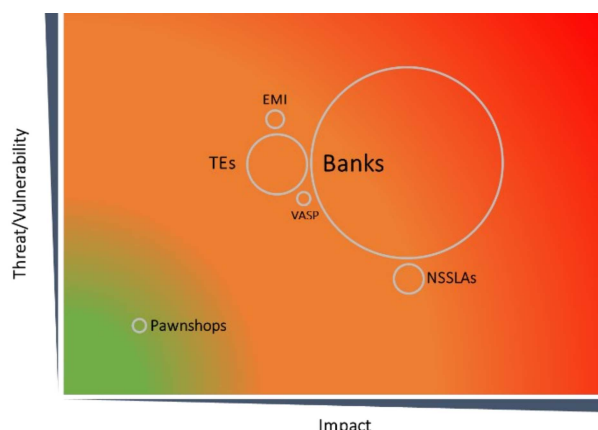
⁴ In terms of total assets as of 30 June 2020

⁵ Circular Letter No. CL-2020-032 dated 06 July 2020

EXECUTIVE SUMMARY

The Net Risk of Banks and other FIs supervised by the BSP is **Medium** except for pawning operations which posed **Low** risk.

The final assessment is based on the total risk ratings, scores, and evaluation of each component considered in this SRA: the criminal threat environment or nature and extent of the ML/TF/PF risks, the vulnerabilities of the sector, and the consequences or impact of the underlying criminal activities.



Responding participants/industries/agencies played a significant role in the assessment as they provided valuable insights on the ML/TF/PF threat environment of the sector, vulnerabilities to ML/TF/PF risks, impact of ML/TF/PF risks on the different stakeholders, and how to cushion the effect of these risks.

1. **Sectoral Threat Analysis.** The threat environment was assessed based on STR volume, level of criminal proceeds, and/or sectoral exposure to the most prevalent predicate crimes and ML indicators. For the covered period (from 2017-June 2020), a total of 1.775 million STRs were submitted by BSFIs, which account for 98.56 percent of the total 1.801 million STRs received by the AMLC. The STR submissions of BSFIs were primarily from the banking sector⁶ at 67.87 percent and 99.99 percent, in terms of volume and value (PhP6,155.2 trillion⁷), respectively. Based on analysis of relevant data and statistics, the level of threat posed by the following predicate crimes to the sector was assessed, as follows:

| | |
|---------------|---|
| High | Corruption, Drug Trafficking, Investment Fraud and Swindling, and Violation of e-Commerce Act and Cybercrimes |
| Medium | Smuggling, TIP, Environmental Crimes, KFR, Illegal Firearms/Gun-running, IP Rights Violations, Forgeries and Counterfeiting, and Tax Crimes |
| Low | Carnapping, Qualified Theft, and other predicate crimes ⁸ |

2. Net risk for TF is **high**. TF threat to the sector is **high** primarily driven by the presence of insurgent and terrorist groups in the country which appear to have a systematic and established method of raising funds for their operations.

⁶ Almost 100% of the STR proceeds/exposures were reported by the 46 UKBs from 2017 to 1st half of 2020.

⁷ Excluding two (2) STRs with inconsistent/outlier amounts

⁸ These include robbery and extortion, jueteng and masiao, violations of the Migrant Workers and Overseas Filipinos Act of 1995 and the Anti-Fencing Law, and Piracy on the High Seas.

3. *Banking Sector Vulnerability.* The overall vulnerability of the banking sector to ML/TF/PF risk remains **medium**. Banks have high inherent vulnerability to ML, TF, and PF due to their crucial role in the financial system facilitating financial transactions and flow of funds. The wide array of financial products and services, size of transactions, as well as the growing physical and digital network or delivery channels of banks are being exploited by criminals to obscure the illegal sources of their funds.

The quality of general AML/CFT/CPF controls is **medium**. Cognizant of these vulnerabilities, AML/CFT/CPF legal and regulatory frameworks and institutional mechanisms and controls were established and are continuously being refined and strengthened. Further, coordination mechanisms among relevant stakeholders are in place and utilized. Scope for enhancements in BSFIs are with respect to the conduct of IRA, suspicious transaction monitoring and reporting systems, and adequacy of resources.

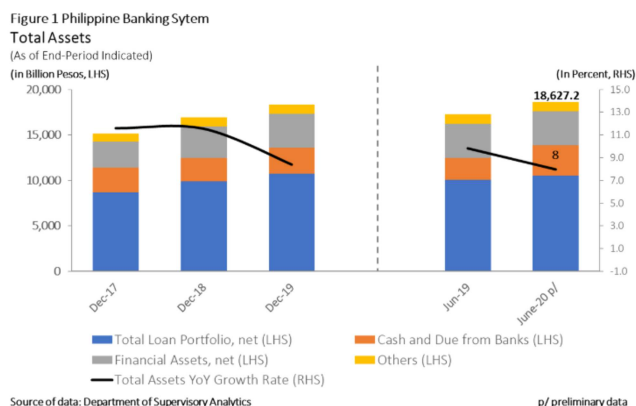
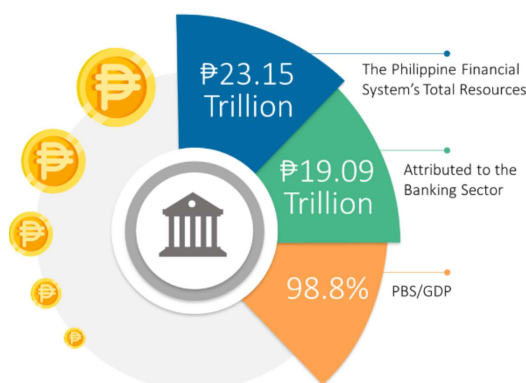
4. Results of the other priority areas are summarized below:

- a. *TBML.* The overall trade-based ML/TF/PF risk associated with the banking sector is **medium**. TBML threat is **high** in view of the prevalence of trade mis-invoicing in the Philippines, complexity and variety of trade-based ML/TF/PF schemes and techniques, intricacies in investigating and prosecuting ML activity of associated crimes such as smuggling, drug trafficking and financing of terrorism, coupled with the geographical landscape of the country that pose challenges in border management and controls. Mitigating controls to prevent TBML include AML/CFT and FX rules and regulations as well as specific measures on banks' trade finance facility.
- b. *TFS⁹.* Net risk for TFS on terrorism and TF, and PF, are assessed as **medium-high**. The threat posed by TF to the sector is **high**. With this, legal and institutional frameworks, and preventive measures are in place to mitigate TF and to implement TFS on TF. On the other hand, the threat posed by PF is **low** in view of nil and minimal trade transactions with DPRK and Iran, respectively. Vulnerability of BSFIs to PF-related sanctions and its evasion is heightened as the understanding of the sector on PF is still developing while PF-related measures are progressing.
- c. *Financial inclusion.* The risk assessment covers specific financial products and services aimed to advance the financial inclusion advocacy of the BSP. ML/TF/PF risks for microfinance loans, basic deposit accounts, micro-insurance, and pawning remains **low**. This is due to low transaction amounts involving these products as well as limited and well-defined product functionalities and target market. Meanwhile, e-money and remittance service of pawnshops were assessed as **"medium"** due to the increasing level of ML/TF threat and prevalent use of both products to send and receive low value remittances for a number of unlawful activities such as OSEC, extortion, and fraud.

⁹ 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 entities.

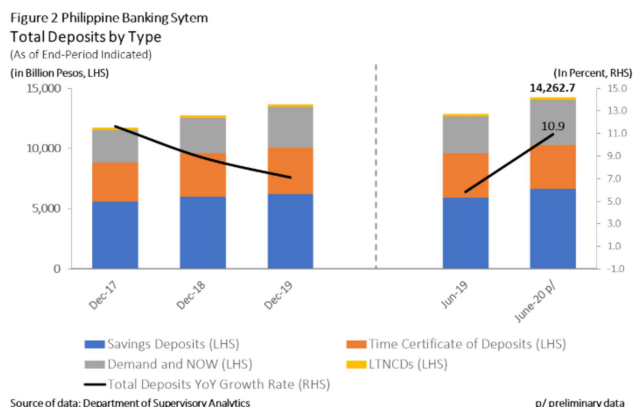
5. Considering the overall high threat posed by ML/TF/PF risks and the inherent vulnerabilities of the sector, the overall level of *consequences is high*. ML/TF/PF risks pose adverse effect across the financial ecosystem, specifically on the individual/customers, the financial institutions, the financial system, and the country. It may cause harm to national security and reputation due to the prevalence of high-risk predicate crimes. It may also undermine economic growth, result in significant loss of government revenue/funds, and increase in social cost, as well as cost of doing business and enforcement/implementation of law.
6. A collaborative approach among AML/CFT stakeholders in the government and private sector is vital in the country's AML/CFT initiatives to ensure that efforts are coordinated and synchronized to achieve well-defined goals. Key recommendations include, among others: (i) continue to strengthen coordination and information exchange mechanisms among AML/CFT stakeholders; (ii) enhance risk-based supervision and engagements with BSFIs; (iii) pursue vigorous outreach sessions to BSFIs to cascade the results of SRA and reinforce awareness on the emerging typologies; and (iv) for BSFIS, to further reinforce their respective AML/CFT framework to identify and mitigate ML/TF/PF risks, considering the findings in this report.

1 OVERVIEW OF THE SECTOR¹⁰



1.1. The Philippine Financial System's total resources as of 30 June 2020 amounted to PhP23.15 trillion,¹¹ of which, PhP19.09 trillion¹² or 82.5 percent is attributed to the banking sector. The PBS' assets represent 98.8 percent of the GDP. UKBs held the largest share of the banking system's total assets at 92.6 percent while TBs and RCBs comprised 6.0 percent and 1.4 percent, respectively¹³. The increase in total assets of the PBS slowed down in 2020 due to the impact of the COVID-19 pandemic. Year-on-year growth rate of the total assets of the PBS of 8.0 percent (*Figure 1*) was slower than the 9.8 percent growth rate in June 2019 and the 8.4 percent growth rate in December 2019.

1.2. Total deposits stood at PhP14.3 trillion as of June 2020 (*Figure 2*), posting a 21.56 percent growth¹⁴ from 2017. Deposits are mainly peso-denominated and sourced from resident individual depositors. Savings deposits had the biggest share of total deposits at 46.45 percent, followed by demand deposits and NOW accounts with 26.32 percent share, and time certificates of deposit with 25.7 percent share.



¹⁰ Mostly sourced from the Report on the Philippine Financial System – First Semester 2020

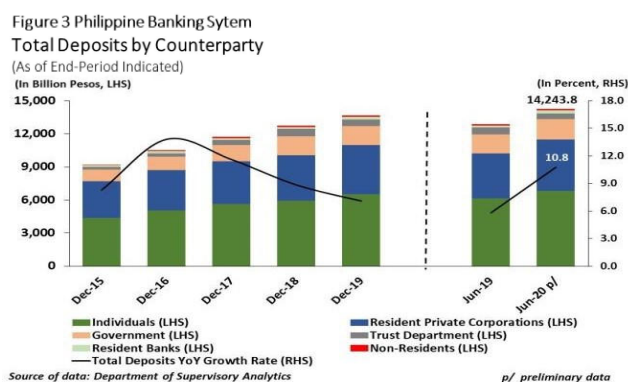
¹¹ <https://www.bsp.gov.ph/SitePages/Statistics/StatisticsMetadataDisp.aspx?ItemId=11>

¹² Gross of allowances etc.; Net amount is PhP18,627.2 trillion

¹³ Report on the Philippine Financial System – First Semester 2020

¹⁴ <https://www.bsp.gov.ph/SitePages/Statistics/BSFinancialStatements.aspx?TabId=1>

1.3. As to counterparty, deposits were mostly sourced from resident individuals and private corporations, with 47.8 percent and 32.7 percent shares, respectively (Figure 3). The FX risk of bank funding remained manageable as foreign currency denominated deposits only accounted for 15.5 percent of the banking system's deposit base as of end-June 2020.



1.4. The banking system landscape became more streamlined as a result of industry consolidation. Across banking groups, the banking system's network consisted of the following: 46 UKBs with 6,947 branches, 48 TBs with 2,606 branches and 447 RCBs with 2,818 branches as of 30 June 2020. While the UKBs held the bulk of the system's total resources, they represent the smallest number of head office count at 8.5 percent. The RCBs consistently hold a substantial share in the number of head offices at 82.6 percent while TBs held the remaining portion of 8.9 percent. Since 2017 to mid-2020, 1,119 additional physical banking offices were opened, 46 percent of which are banking offices of UKBs.

Banking offices are mostly located in highly urbanized and populated areas of the NCR, Calamba, Laguna, Batangas and Quezon Region (CALABARZON), and Central Luzon.

- 1.5. Banks continue to embrace financial technology and digital innovations in the delivery of financial services. BSFIs engage in EPFS to improve efficiency of financial transactions. Around 111 banks, consisting of 41 UKBs, 29 TBs, and 41 RCBs, are offering different modalities of e-banking platforms to the public. As of end-June 2020, the use of ATMs remained to be the lead electronic facility used by majority of BSFIs (143). Meanwhile, physical banking offices continue to expand notwithstanding the increasing use of digital banking¹⁵. Bank density ratio remained at 8 banks per city/municipality.
- 1.6. Physical banking offices overseas are located in the Middle East and Asia Pacific Regions. This is because of the prominence of Filipino communities in these regions particularly migrant workers. The foreign banking offices including remittance desk offices in Middle East, Asia Pacific, North America, and Europe are the significant enablers of remittance inflows to the country through the banks, as well as alternative delivery channels such as mobile banking, and remittance agents.
- 1.7. Php4.05 trillion or 17.5 percent of the total resources of the Philippine financial system is held by NBFIs such as Investment Houses, Financing Companies, NSSLAs, Pawnshops, Securities Dealer/Broker, Lending Investor, Venture Capital Corporations, Credit Card

¹⁵ Ibid

Companies, Government NBFIs, Credit Granting Entities, TCs, and MSBs. As of 30 June 2020, there were 1,250 NBFIs with 13,589 branches, and one (1) offshore banking unit.

- 1.8. Total assets of the trust industry contracted by 20.8 percent to PhP2.86 trillion as of 31 March 2020. Funds were mostly deployed into financial assets and deposits in banks. Nevertheless, investment in equity securities remained high, indicating greater preference of TEs for higher-yielding instruments. Meanwhile, the trust industry reported higher earnings due to the rise in fees and commissions of TEs.
- 1.9. The total assets of NSSLAs continued to increase year-on-year from PhP232 billion in March 2019 to PhP260.2 billion in March 2020 channeled to lending activities. Despite the industry's upbeat lending activities, credit quality has improved as the NPL and NPA ratios continued to decrease from 2018 to March 2020. The industry remained liquid, with stable funding and sufficient capitalization with the growth in members' capital contribution. Profitability was sustained driven by the steady growth of loans to members.
- 1.10. Meanwhile, pawnshops and MSBs have become major financial service access points to the underbanked and unbanked areas of the country. The emergence of digital platforms and solutions brings both opportunities and threats to the non-bank sector especially for pawnshops and MSBs, as using digital platforms has become a significant component of their business strategy. Pawnshops and MSBs posted network expansion with year-on-year growth of 9.0 percent and 20.2 percent, respectively.

**CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE**

 3/19/21

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

2 SECTORAL THREAT ANALYSIS

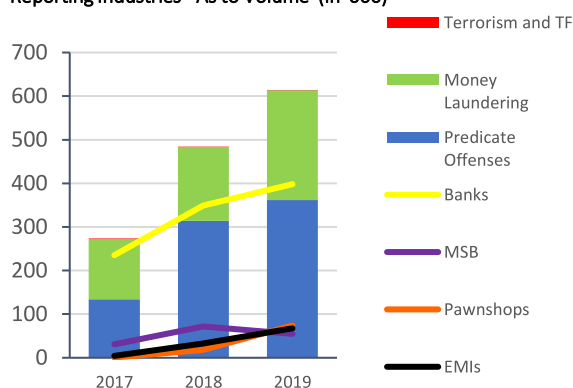
2.1. *Threat environment.* Based on SOCTA and other data/information gathered from relevant government agencies/LEAs, the estimated number of incidents of criminal activities in the country and the criminal proceeds generated for the period 2017 to 2018 (Figure 4)¹⁶ indicate that predicate crimes and possible related ML activities remain prevalent and pose continuing threat to the sector. (Details in succeeding sections of the report)

Figure 4. Incidents of Criminal Activities



2.2. From 2017 to June 2020, STRs submitted by BSFIs (1.775 million) account for 98.6 percent of the total STRs received by the AMLC (1.801 million). Figure 5 shows the generally increasing trend of STR submissions of BSFIs from 2017-2019. Bulk of these (around 70 percent) were from banks. These STRs mainly involved predicate offenses.

Figure 5. Types of Suspected STR Offenses by Reporting Industries - As to Volume (in '000)



PREDICATE OFFENSES

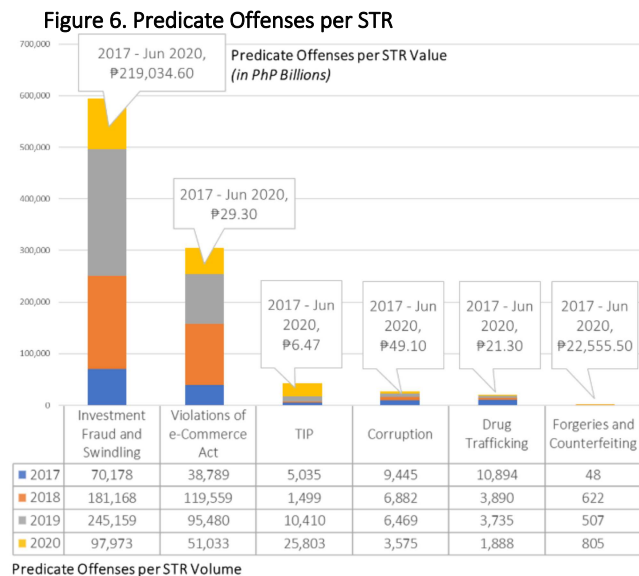
2.3. The level of threat posed by the following predicate crimes to the sector was assessed, as follows:

| | |
|--------|---|
| High | Corruption, Drug Trafficking, Investment Fraud and Swindling, and Violation of e-Commerce Act and Cybercrimes |
| Medium | Smuggling, TIP, Environmental Crimes, KFR, Illegal Firearms/Gun-running, IP Rights Violations, Forgeries and Counterfeiting, Tax Crimes |
| Low | Carnapping, Qualified Theft, and other predicate crimes ¹⁷ |

¹⁶ Sources include: for corruption (<https://cnnphilippines.com/news/2019/8/16/Government-corruption-loss-deputy-ombudsman-Cyril-Ramos>. Accessed on 22 October 2020); for smuggling, estimated amount per year (<http://www.fpi.ph/fpi.cms/Research>); for tax crimes, amount involved was for 2017-2019 (<https://www.bir.gov.ph/index.php/transparency/bir-annual-report.html>); environmental crimes, estimated amount per year (<https://www.adb.org/publications/addressing-illegal-wildlife-trade-philippines>); other crimes were taken from SOCTA covering periods from 2017-2018, and SEC website

¹⁷This includes robbery and extortion, jueteng and masiao, violations of the Migrant Workers and Overseas Filipinos Act of 1995 and the Anti-Fencing Law, and Piracy on the High Seas.

2.4. Predicate offenses posing high level of criminal threat to the sector are *investment fraud and swindling, violations of e-Commerce Act of 2000 and cybercrimes, corruption, and drug trafficking*. This is in view of the high number of incidents with various typologies and schemes, the significant amount of criminal proceeds they generate, and high impact to the sector. Meanwhile, *forgeries and counterfeiting and TIP, among others, pose medium threat* due to increasing exposure of the sector in terms of volume and value and emergence of new typologies through the use of information and communication technology. Other predicate crimes pose lesser threat. (Figure 6)



2.5. *Investment Fraud and Swindling*. This accounts for 33.49 percent and 71.06 percent of STRs, in terms of volume and value¹⁸, respectively. This can be attributed, in part, to the susceptibility of Filipinos to investment scams. For the covered period, SEC issued 34 CDOs against unauthorized sale of securities in the guise of investments¹⁹. The SEC also issued warnings to the public that VC issuances and cloud mining contracts require registration similar to securities. Of the total investment fraud-related STRs, 43.61 percent involved investment schemes estimated at PhP1.39 billion. These were subjects of 18 Freeze Orders and 584 negative media reports.

Swindling. STRs related to swindling were mostly ZSTRs²⁰ wherein either the subject is not an accountholder or is an accountholder but has no monetary transaction with the BSFI at the time the suspicious activity was determined. Usual swindling scheme involves claim of funds via the presentation of fraudulent documents.

Case 1: An organization solicited investments from the public in the guise of “donations” without the required license from the SEC. Alleged donations were deposited to around 50 accounts in nine (9) banks under the name of the organization and/or its senior officers. PhP149 million were frozen.

Case 2: A case of market manipulation. The scheme involves using dummy individuals to purchase shares of stock of a corporation during the initial public offering. Dummy bank accounts were opened, funded and controlled by the perpetrators to facilitate the stock transactions. Proceeds of the sale of stocks

¹⁸ Excluding outlier STR amount of USD100 trillion (PhP5,847 trillion) in Case 3 (Swindling).

¹⁹ <https://www.sec.gov.ph/sec-issuances/cease-and-desist-orders/>.

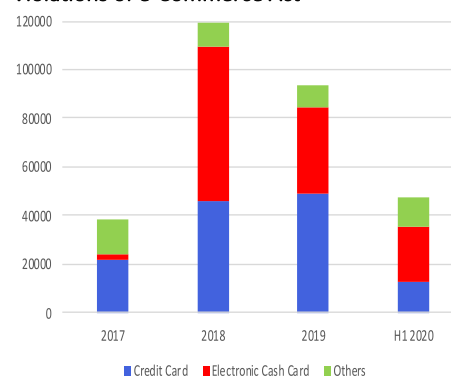
²⁰ STRs filed on the basis of suspicious trigger (ex. subject of news report, qualified theft, etc.) even if the subject has no monetary transaction with the CP at the time the suspicious activity was determined; AMLC Registration and Reporting Guidelines, Part 4: Annex B-34 – System Codes

were returned to the perpetrators through a series of fund transfers and check issuances. It involved approximately Php200 million in several BSFIs under numerous bank accounts.

Case 3: Swindling. Two reported attempts by a senior citizen-customer, assisted by a paralegal and real estate salesperson. The customer presented fraudulent identification documents to claim ownership of a USD100 trillion worth of gold bars. After verification, the Bank found a social media post of the customer who represented himself as an envoy and a member of a religious organization, charged with and “Gatekeeper” of Japanese plundered treasures.

- 2.6. **Violations of e-Commerce Act.** These comprised 17.17 percent of STRs, although funds involved appear minimal, at an average of Php1,800 per transaction. The shift of financial transactions to electronic or online platforms has resulted in the increase in related typologies amid the COVID-19 pandemic. The main products, services, and/or delivery channels used involved credit card and electronic cash cards (Figure 7). Majority of the cases under this category involved ATM skimming, unauthorized withdrawal transactions via ATM or unauthorized online purchases using electronic cash/gift/debit card.

Figure 7. No. of STRs involving Violations of e-Commerce Act



Case 4: The balances of certain bank accounts were increased through system manipulation/hacking, and the funds were subsequently transferred to certain beneficiaries in other BSFIs and withdrawn. Investigation results noted that recipients of the funds were previously involved in cybercrime incident.

Case 5: A dealer in securities illegally and fraudulently accessed the company’s account and transferred the shareholders’ stocks to a client worth around Php750 million. Various bank accounts of the perpetrator and his accomplices were noted to have deposit/withdrawal transactions which were not commensurate with their declared sources of income.

- 2.7. **Corruption.** Corruption remains a priority concern in the country. Based on the CPI 2019, corruption level has not improved²¹. Corruption related offenses reported in the STRs were however, minimal at 1.49 percent and 0.02 percent, in terms of volume and value. These involved frauds and illegal exactions, as well as graft and corrupt practices. Other reported incidents involved plunder, bribery and corruption of public officers, and malversation of public funds and property.

²¹ The Philippines ranked 111th, 99th and then 113th out of 180 countries in 2017, 2018 and 2019, respectively, with a score of 34 in 2017, 36 in 2018 and slid back to 34 in 2019 (<https://www.transparency.org/en/cpi/2019/results/table>). The CPI uses a scale from 0 to 100, where “0” means highly corrupt and “100” means very clean.

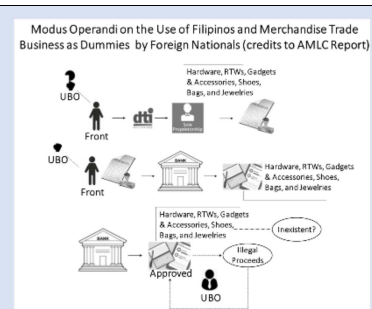
Case 6: *Certain government officials colluded with a corporate taxpayer for the settlement of the latter's income tax deficiency. The aggregate transactions of these government officials with several banks far exceeded their declared sources of income and have no underlying legal or economic justification. PhP75 million of subjects' deposits in banks were frozen.*

Case 7: *Certain government officials made multiple large cash deposits and withdrawals, where the amounts involved were inconsistent with their declared sources of income. The funds were moved from one account to another through fund transfers and check issuances. They also placed large investments in mutual funds, unit investment trust funds, time deposits, and life insurance using cash.*

- 2.8. **Drug Trafficking.** STR proceeds from drug trafficking has been increasing since 2018. Based on the 2019 SOCTA, the number of drug trafficking cases filed in court declined in 2018, although the amount of criminal proceeds involved increased by 20.8 percent. LEAs observed that the system of operations of drug groups remain unchanged, including their preference for bank wire transfers as a mode for paying illegal drugs. Legitimate businessmen expanded their assets through the illegal drug trade as drug distributors, financiers or as protectors to local criminal groups, while local drug lords laundered proceeds by using legitimate businesses²² as fronts. Nonetheless, minimal STRs were filed related to drug trafficking, most of which were triggered by negative news, receipt of freeze orders, or subjects of government investigations or AMLC inquiries. The transactions were coursed through deposits, international inward remittance, and inter-account transfers. Transactions usually involve large amounts ranging up to PhP861.00 million per transaction.

Case 8: *In the joint operation of LEAs, six magnetic lifters containing concealed shabu (methamphetamine hydrochloride) were found in warehouses in different locations. The owner of the warehouse turned in nine (9) checks representing lease payments. Funds in 44 bank accounts and 36 related bank accounts totaling PhP14.6 million were frozen.*

Case 9: *The use of dummies or shell companies by foreign nationals, mostly Chinese, was identified as a common modus operandi in laundering proceeds of illegal drug trade. Filipino nationals register retail businesses, mostly with no actual operations. After business registration, the Filipino owner opens bank accounts in the name of the newly-registered businesses. The bank accounts were used to receive and transact proceeds of illegal drug trade through a combination of cash and check deposits, inter-account transfers, check encashments and cash withdrawals. The foreign nationals who control said businesses serve as the UBO of said bank accounts²³.*



- 2.9. **STRs related to ML.** STRs related to ML based on suspicious nature of transactions and red flag indicators comprised 43.05 percent of total STRs filed by the sector, involving around PhP66.49 trillion. Majority of these STR were triggered by red flags identified by

²² 2019 SOCTA.

²³ AMLC Risk Information Sharing and Typologies; <http://www.amlc.gov.ph>

control units or the transaction monitoring system of the BSFIs. These transactions were usually coursed through deposit accounts and remittances, mostly filed using “ZSTR” code and/or attempted transactions. The suspicious circumstances noted included amounts not commensurate with the business or financial capacity of the client, lack of underlying legal or trade obligation, purpose or economic justification, or deviation from the client's profile/past transactions.

Case 10: *No underlying legal or trade obligation. These mainly involved attempted fraudulent international inward remittances amounting to EUR22.0 billion.*

Case 11: *Amount is not commensurate with the financial capacity of the client. Three STRs involved attempted account opening with supposed initial deposit of USD1 trillion and EUR200 billion, respectively.*

- 2.10. *ML Investigation/Cases.* For the covered period, there were a total of 49 bank inquiries conducted by the AMLC, 31 freeze orders issued, 22 petitions for civil forfeitures filed, and 10 ML complaints, among others. The criminal proceeds involved in these investigations were estimated at PhP3.0 billion of valuated assets and numerous motorized vehicles and real properties, PhP1.6 billion of which are currently subject of civil forfeiture proceedings. These orders/cases involved the top predicate offenses, such as violations of e-Commerce Act/cybercrimes, swindling/fraudulent practices, corruption, and drug trafficking and related offences.
- 2.11. *Industry Perspective.* UKBs and TBs consider violations of e-Commerce Act and cybercrimes as top threats, while drug trafficking and qualified theft pose highest threats for RCBs. Similarly, in the RCLs of banks, majority of the reported incidents pertain to falsification and swindling. Credit card and internet banking facilities were mostly used.
- 2.12. *Other Predicate Crimes Posing Medium and Low Threat to the sector are, as follows:*
- 2.12.1. **TIP²⁴.** TIP comprised 2.41 percent of the total STRs. Criminal proceeds from violations of the Anti-TIP Act of 2003 include an international inward remittance amounting to PhP5.69 billion reported by an MSB in 2017, comprising 99.35 percent of the funds generated from TIP. The MSB assessed that the transaction was possibly connected to cyberpornography. On the other hand, OSEC is an emerging risk with 21,395 STRs in 2020 comprising the majority of TIP STRs filed.

²⁴ TIP is punishable under R.A. No. 9208 or the Anti-Trafficking in Persons Act of 2003, R.A. No. 7610 or the Special Protection of Children Against Abuse, Exploitation and Discrimination Act, R.A. No. 9775 or the Anti-Child Pornography Act of 2009 and R.A. 9995 or the Anti-Photo and Video Voyeurism Act

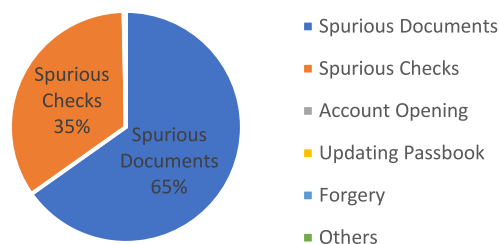
Case 12: OSEC Typology. A sender abroad (male offender) sends money through a bank or remittance company abroad to one or various beneficiaries in the Philippines, who are allegedly the facilitator/s of OSEC activities, in exchange for a broadcast of child exploitation material to the offender abroad.



2.12.2 Forgeries and Counterfeiting.

Forgeries and counterfeiting comprised 7.32 percent of STRs in terms of value, although incidents were minimal but on an increasing trend. Most of these offenses involved spurious checks or commercial documents (Figure 8) and were reported as ZSTRs.

Figure 8. Forgeries and Counterfeiting - As to STR Value



Case 13: In 2019, two corporations attempted to transact with banks by presenting fraudulent commercial documents involving USD780 million and EUR2 million.

Case 14: In 2020, the intended recipient of an attempted wire transfer from an international bank provided an "affidavit of fund origin" showing sole mandate and authority to administer a fund amounting to EUR2 trillion.

2.12.3. Tax Crimes. The BIR reported 618 tax evasion cases from 2017 to 2019 involving total amount of PhP75 billion, as follows:²⁵

Figure 9. Tax Crimes



The amount of estimated tax liabilities declined from 2017 to 2019, but the number of cases filed increased by 76 percent in 2018; and by 57 percent in 2019. Large taxpayers, who are mandated to use the eFPS and pay through banks, paid considerable taxes at PhP1.428 trillion in 2019 or 67 percent of total tax revenues. Meanwhile, the narratives of around 105 STRs include reference to possible tax crimes.

2.12.4. Smuggling. Third party observers like the Federation of Philippine Industries noted that smuggling accounts for more than PhP100 billion losses in government revenues every year.²⁶ The BOC reported a total of PhP14.2 billion estimated value of smuggled goods in 2017. In the same year, BOC filed 12 smuggling complaints.²⁷

²⁵ <https://www.bir.gov.ph/index.php/transparency/bir-annual-report.html>.

²⁶ <http://www.fpi.ph/fpi.cms/Research/uploads/Addressing%20Smuggling%20in%20the%20Philippines.pdf>.

²⁷ https://customs.gov.ph/wp-content/uploads/2018/09/2017_Annual_Report.pdf.

2.12.5. **Environmental Crimes.** According to the ADB, illegal wildlife trade in the country is a PhP50 billion industry.²⁸ So far, identified cases of illegal logging and illegal fishing have generated around PhP807 million in 2017 and 2018.²⁹


Case 15: Endangered species of animals were seized from the house of the accused. The animals, with an estimated value of PhP10 million, were smuggled from Indonesia and entered the country through Mindanao and bound to Manila. Financial investigation revealed that the accused maintained 17 bank accounts, with PhP1.6 million amount frozen.

Case 16: A number of respondents are facing charges for violation of P.D. No. 706 or the Revised Forestry Code for unlawful occupation or destruction of forest lands in a well-known beach destination in the country, as well as illegal gathering and collecting of timber and other products.

2.12.6. **KFR.** In 2017 and 2018, law enforcement authorities had detected around 111 cases of KFR incidents. Authorities have also observed that ransom payments in casino-related kidnappings were usually done through wire transfers, mobile-based payment solution integrated with social media app, and offshore banking.³⁰




2.12.7. **Illegal Firearms/Gunrunning.** Statistics on gun-running show increasing number of cases in 2017 and 2018. (Table 1):³¹

Table 1. Illegal Firearms/Gunrunning Statistics

| Gunrunning | 2017 | 2018 | Total |
|--|--------|--------|--------|
|  No. of operations | 185 | 451 | 636 |
|  Loose firearms recovered/confiscated/surrendered | 11,837 | 13,468 | 25,305 |
|  No. of cases filed in Court | 6,339 | 6,869 | 13,268 |

2.12.8. **IP Violations.** Combined efforts of LEAs yielded an estimated value of goods seized totaling PhP31.9 billion for the years 2017 to 2018. (Table 2):³²

Table 2. Intellectual Property Violation Statistics

| IP Violations | 2017 | 2018 | Total |
|---|----------|-----------|-----------|
|  No. of new cases | 194 | 166 | 360 |
|  Cases filed in court | No Data | 340 | 340 |
|  Estimated Value of Goods Seized | ₱ 8.4 Bn | ₱ 23.5 Bn | ₱ 31.9 Bn |

²⁸ <https://www.adb.org/publications/addressing-illegal-wildlife-trade-philippines>.

²⁹ PNP Annual Reports, www.pnp.gov.ph.

³⁰ 2019 SOCTA.

³¹ *Ibid.*

³² *Ibid.*

2.12.9. **Carnapping.** A total of 753 motor vehicles and 8,636 motorcycles were carnapped in 2017 and 2018. Banks are seen by LEAs as unwitting facilitators in carnapping activities³³ as well as in the Rent-Sangla scheme³⁴.

TERRORIST FINANCING

2.13. The extent and threat of TF activities to the sector is **high**. This was driven by the various violent incidents carried out by terrorist/threat organizations in the country, which appear to have a systematic and established method of raising funds for their operations. These include using illegal means to raise funds such as KFR and extortion, use of NPOs, family funding and other legitimate means to finance their activities. Cash transactions remain to be the mode for transfer of value for terrorist/threat organizations. Remittance transactions have also been used to transfer funds, especially from abroad. MSBs and banks are the most used channels in moving funds. Emerging threats include the use of virtual currency and/or cryptocurrency and social media or crowd sourcing.³⁵

2.14. Analysis of TF-related STRs for the covered period disclosed that possible terrorism and TF activities generated a total of PhP1.79 billion. In terms of proceeds, Bangsamoro Region accounted for 71.50 percent of the total STR value.

PROLIFERATION FINANCING

2.15. The threat environment in relation to PF of WMD in the Philippines is **low**. This is due to minimal transactions/connections with DPRK and Iran, and minimal import and export of DUGs. The Philippines' exposure to trade-based PF threat, based on trade transactions with DPRK and Iran, has been on a decreasing trend from 2017 up to August 2020. There is no trade of potentially strategic goods with DPRK for the period January 2018 to August 2020. Nevertheless, limited information on investigations related to PF incidents is one of the limitations in assessing PF threat to the sector.

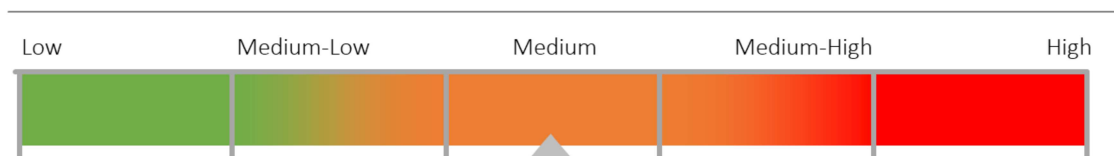
³³ *Ibid.*

³⁴ *Rent-Sangla/Benta Scheme* refers to the taking of motor vehicle (MV) through verbal agreement or by virtue of contract of rent or lease whereby the lessee failed to return the MV to the lessor after the expiration of the contract and disposed the same thru lease/sale intended for personal gain using falsified documents and without the knowledge and consent of the lessor/registered owner.

³⁵ AMLC's Terrorism and Terrorism Financing Risk Assessment 2021 (www.amlc.gov.ph)

3 VULNERABILITY

3.1. BANKING SECTOR



3.1.1. Overall vulnerability of the banking sector is *Medium*.

3.1.2. *The banking sector has high inherent vulnerability to ML/TF/PF risks.* Banks play a crucial role in the financial system facilitating financial transactions and flow of funds that underpin economic activity. The wide array of products and services, size of transactions, as well as the expansive and growing physical and digital network or delivery channels of banks provide criminals the opportunities and gateways to obscure the illegal sources of their funds. These render the products and services of banks the more preferred access points for ML, TF, and PF activities. Meanwhile, customer base and geographical locations pose medium level of vulnerability.

3.1.3. *The quality of general AML/CFT/CPF controls is medium.* Cognizant of these vulnerabilities, AML/CFT/CPF legal and regulatory frameworks as well as institutional mechanisms and controls were established and are continuously being adjusted and strengthened. The enhancements aim to further improve ML/TF/PF risk management framework to ensure that it remains commensurate with the prevailing risk context and aligned, to the extent possible, with international standards. Further, coordination mechanisms among relevant stakeholders are in place and utilized. The BSP, as the supervisor, adopts risk-based supervisory approach to assess adequacy of the BSFI's ML/TF/PF risk management framework and impose appropriate supervisory enforcement actions, as necessary. Scope for enhancements in BSFIs are with respect to the conduct of IRA, suspicious transaction monitoring and reporting systems, and adequacy of resources.

ASSESSMENT OF CONTROLS

3.1.4. *Quality of AML/CFT/CPF Legal and Regulatory Framework – High.* The AML/CFT legal framework in the Philippines is comprehensive, especially with the enactment of the following new laws, among others:

- R.A. No. 11521 (AMLA, as amended) (2021) – Recent amendments to the AMLA to strengthen the country's AML/CFT legal framework;

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE

3/19/21
JOSE MICHAEL E. CAMACHO
Bank Officer II, RMD
Administrative Services Department
Page | 24

- R. A. No. 11479 (The Anti- Terrorism Act of 2020) - An Act to prevent, prohibit and penalize terrorism;
- R. A. No. 11211 (The New Central Bank Act) (2019) - Amendments to the BSP Charter which include, among others, the expansion of BSP's supervisory/regulatory authority over MSB, credit granting business, and payment system operator; and
- R.A. No. 10927 (2017) - An Act Designating Casinos as CPs Under R.A. No. 9160, otherwise known as The AMLA, as amended.

The BSP issued new and enhanced AML/CFT regulations that are aligned, to the extent possible, with international standards and best practices. Likewise, enhanced guidelines on CBR were issued in 2020. Other BSP issuances include guidelines on the adoption of the NRPS framework, and rules and regulations on the payment system oversight framework and registration of OPS.

Targeted guidance and prudential reminders were also issued intended to enhance BSFIs' understanding of their AML/CFT obligations and enable them to refine their policies and procedures. These include reminders in dealing with MSBs and OGB customers, preventive measures relevant to illegal investment activities or schemes, guidance on managing ML risks related to OSEC, and reminders against financial crimes amidst COVID-19 pandemic, SMS-based attacks, and phishing attacks.

Various AMLC and international issuances such as UNSC resolutions, AMLC resolutions and regulatory issuances, and FATF publications were disseminated to the BSFIs for their information and guidance.

- 3.1.5. *Availability and Enforcement of Administrative Sanctions – High.* The BSP has a well-defined supervisory enforcement action framework. In the 2019 MER, BSP was cited to have proportionate and dissuasive remedial actions and sanctions. In addition, the API A, B and C, No.1 - RPAC dated 26 July 2019 further strengthens imposition of administrative sanctions by the AMLC. The RPAC is intended to apply to administrative cases for non-compliance with AMLA, as amended, and its implementing rules and regulations, of all CPs, including their officers, directors, and employees. It aims to employ a graduated scale of monetary sanctions based on the CP's asset size and gravity of the violation/non-compliance.

From 2017 to 2020, BSP imposed both monetary and non-monetary penalties against BSFIs for non-compliance with AML rules and regulations. Monetary penalties were imposed against several banks/NBFIs due to noted weaknesses in their risk management system and non-compliance with BSP's directives. Moreover, non-monetary enforcement actions such as written warnings, restrictive action on operations and remedial actions (e.g., action plan, LOC) were also issued.

Consistent with risk-based principle, the MOA between the AMLC and the BSP prioritizes those BSFIs posing higher risk based on their AML/CFT framework. The AMLC has enforced administrative actions on banks, which include filing of administrative charges, imposing monetary penalties, sending directives to explain, and issuing warning and reminder letters for non-compliance.

- 3.1.6. *Availability and Effectiveness of Entry Controls – High.* Market entry requirements are embedded in existing banking laws and regulations. These include the requirements for establishing banks such as the prescribed minimum capitalization and fit and proper standards for stockholders, incorporators, directors, and officers. The bank licensing process, which includes fit and proper assessment of stockholders, UBOs, directors and officers, is well defined. This involves, among others, the assessment of their integrity, competence, physical and mental fitness, and relevant education. Further, the BSP maintains a central information file³⁶ of watchlisted persons who are disqualified to hold a position in any BSFI, and those subject of material information (e.g., recipient of reprimand notices from the BSP). This ensures that only those qualified and fit to own, control, or manage a bank are allowed to do so to prevent illegal entities and/or their associates from owning, controlling, or holding a significant or controlling interest, or management function in BSFIs. The 2019 MER cited that the BSP implements robust market entry requirements for banks and TEs³⁷.



From 2018 to 2020, there were 34 denied applications for directors and officers of banks. Further, eight (8) prospective stockholders of banks were not approved. The denials were mainly due to failure to possess required qualifications or meet the prescribed requirements.

- 3.1.7. *Integrity of Banks' Staff – High.* Appropriate controls are being implemented to ensure integrity of the banking sector's staff. The BSP uses, among others, its internal watchlist file to screen prospective directors and officers of BSFIs. Banks are also required to adopt robust recruitment process, which includes screening of applicants, to ensure that employees are qualified and have no criminal records. Internal control measures such as rotation of duties, check and balance approach to assignment of duties and responsibilities, and the use

³⁶ Pursuant to Circular No. 1076, the BSP maintains two (2) files of watchlisted individuals: a) Disqualification File "A" (Permanent) and Disqualification File "B" (Temporary).

³⁷ 2019 MER Page 122

of key results areas, were also adopted to instill appropriate behavior and promote compliance culture.

Banks have developed their own policies and procedures in handling internal investigations and imposing sanctions against erring officers and staff. AML/CFT compliance is part of an employee's key results area, which serves as basis for performance evaluation/rating, bonuses, and promotion. Disciplinary actions imposed on banks' staff due to breaches of compliance policy include issuance of warning, reprimand, suspension and termination, and monetary penalties.

Based on RCLs, bank personnel were involved in minimal incidents at 5.60 percent. This is an indicator of the continuing improvement in staff recruitment and retention process of banks.

- 3.1.8. *Effectiveness of Sanction Screening and Suspicious Activity Monitoring and Reporting – Medium.* Banks have adopted the required monitoring system, which mainly involves the use of electronic AML system for complex banks, supplemented by manual monitoring system. The independence of banking units handling the alerts management system, which is either the compliance office or a designated unit within the bank, has been a key control enhancement to strengthen the ongoing monitoring process. As a result, CTRs and STRs filed by the banks remain significant (*Figures 10 and 11*).

Figure 10. CTRs and STRs Filed by BSFIs

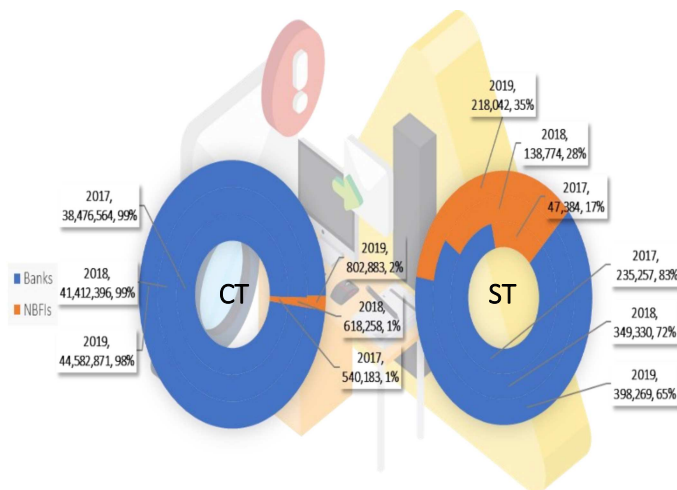
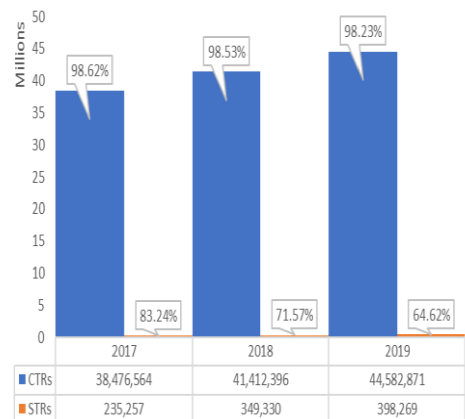


Figure 11. CTRs/ STRs of BSFIs to Total CTRs/STRs Received by the AMLC (Number and %)



- 3.1.9. Survey indicates that accounts and customers who were subject of STRs were either placed under enhanced monitoring, considered for inclusion in the watchlist databases and/or considered for termination of relationship.

Areas for improvement include implementation of risk-based updating of CDD information and customer risk profile, conduct of transactional due diligence as necessary, periodic review of the monitoring systems including the suitability of parameters to generate meaningful alerts and quality STRs, and having sufficient manpower complement in alerts management process.

- 3.1.10. *Banks have adopted sanction screening procedures for their customers and transactions to comply with the UNSCR on TF and PF.* This includes maintaining updated sanctions list database from relevant sources such as the AMLC, UNSCR, and the OFAC, and defining due diligence procedures and hierarchy of actions for target match clients. Sanctions screening policies include screening procedures and system for clients, including their beneficial owners, fund/wire transfer parties and trade transactions particulars such as vessels and types of goods. Banks should, nonetheless, continue to deepen their understanding and improve implementation of TFS.
- 3.1.11. *AML Knowledge of Banks' Staff – Medium.* Outreach sessions and trainings on AMLA, mechanisms to detect and report suspicious transactions, and emerging ML/TF/PF typologies are continuously being conducted even during the pandemic. Aside from trainings provided by the BSP, AML/CFT experts and system providers also offer AML learning sessions to the industry. Other forms of feedback mechanisms are implemented by the BSP and AMLC through BSP's regular examinations and thematic reviews, meetings with the industry associations, issuance of guidance papers and reminders, and responding to queries or clarifications of BSFIs.

Meanwhile, banks have internally-developed training programs for newly-hired personnel, ranging from basic AML/CFT training to more focused courses which are tailored-fit to the participants' functions. Refresher courses are likewise offered to banks' personnel through classroom discussion, online course, webinars, infographics, and e-mail blasts. The 2019 MER recognized that banks and their subsidiaries in the Philippines have a sound understanding of their ML/TF risks and AML/CFT obligations, particularly on the requirements for enhanced CDD and account monitoring relating to high-risk customers³⁸.

Scope for improvement is to enhance training modules to focus on specific or emerging ML/TF/PF typologies, deepen understanding of TFS requirements, and develop ways to proactively identify and detect unusual or possible suspicious transactions.

- 3.1.12. *Effectiveness of banks' Compliance Function – High.* This was anchored on the implementation of a group-wide MTPP, conduct of IRA, and independence of the Compliance Office with direct reporting line to the BOD or any board-level

³⁸ 2019 MER Page 103

or approved committee on AML/CFT. Most banks established a separate AML/CFT Board or Management level committee to discuss, among others, results of their IRA, emerging risks and typologies, TFS implementation, audit and compliance testing results, alerts monitoring and disposition, and trainings. The 2019 MER noted that UKBs have functioning internal controls and AML/CFT compliance structures and have established governance frameworks, with reporting lines from the compliance officer to the BOD, as well as reporting to risk and audit committees³⁹. Scope for improvement is the continuing need to ensure that the compliance function has adequate resources to enable it to discharge its evolving AML/CFT responsibilities.

- 3.1.13. *Banks' corporate governance on AML/CFT – High.* BSP issues regulations aimed to strengthen corporate governance in banks to sustain the resilience and stability of the financial system. The board has the ultimate responsibility to fully comply with the AML/CFT rules and regulations. The 2019 MER noted that banks and their subsidiaries in the Philippines have a sound understanding of their ML/TF risks and AML/CFT obligations, are implementing RBA to AML/CFT compliance and have functioning money laundering prevention programs⁴⁰. This was affirmed by the results of the onsite examinations which noted improving AML/CFT corporate governance in banks. Nonetheless, scope for improvements include proactively addressing emerging AML/CFT issues, ensuring adequate support in terms of skills and resources in the self-assessment functions, as well as deepening AML/CFT compliance and awareness culture in the BSFI.
- 3.1.14. *Availability and access of banks to beneficial ownership information – Medium.* The primary sources of beneficial ownership information are the SEC, PSE, CDA, and DTI. The SEC, in particular, maintains an online system, containing information on the companies' beneficial ownership, that allows the public to access reports for a fee. To further enhance the GIS information, SEC has issued Memorandum Circular No. 15 Series of 2019 to incorporate beneficial information in the GIS⁴¹. It is also formulating the framework for sharing of UBO information in coordination with other competent authorities. Meanwhile, beneficial ownership information is obtained by the AMLC thru bank records for intelligence and regulatory purposes. For BSP, CDD records of banks which are accessed during examinations include information on beneficial owners of customers. To further improve UBO identification and access to UBO information, the SEC together with other government agencies and with the assistance of the ADB, has an ongoing project on beneficial ownership information registry.

³⁹ Ibid

⁴⁰ Ibid

⁴¹ To reinforce the fight against dirty money, the SEC issued Guidelines in Preventing the Misuse of Corporations for Illicit Activities through Measures Designed to Promote Transparency of Beneficial Ownership ("BO Transparency Guidelines") through SEC Memorandum Circular No. 1 dated 27 January 2021.

- 3.1.15. *Availability of Reliable Identification Infrastructure – High.* A reliable identification infrastructure is available to banks. Clear, written, and graduated customer acceptance and identification policies and procedures are part of the AML/CFT policies of banks. Results of examinations for the past years showed continuing initiatives to enhance the customer onboarding process, such as implementation of system and manual controls to gather required information and validate the same from reliable sources, particularly from the government agencies that issued the identification documents. Banks also implement ID verification system. Some of these IDs have features to verify their authenticity such as the driver's license, PRC and Postal ID.

Meanwhile, the implementation of the national identification system, after the passage of the "Philippine Identification System Act"⁴², will further facilitate the conduct of efficient and reliable customer identification and will streamline customer onboarding process.

- 3.1.16. *Quality of risk-based supervision – High.* This mandate of the BSP is articulated in Sections 25 and 28 of R.A. No. 7653, as amended (The New Central Bank Act), Section 4 of the GBL of 2000, and Section 5.1, Rule 7 of the 2018 IRR of the AMLA.

The BSP implements RBA to AML/CFT supervision. This involves various supervisory activities to continuously understand the business model and risk profile of BSFIs and properly implement risk-based strategies. Offsite supervisory activities range from holding meetings with the BOD/SM, compliance office, and internal and external auditors, coordinating with the home regulator, as applicable, updating understanding of the BSFI's and sector's risk profile, and surveillance monitoring. Risk-based onsite examinations and thematic reviews are also integral parts of the supervisory activities. (See Figure 12)

Figure 12. Risk-Based AML/CFT Supervision



- 3.1.17. A dedicated unit within the BSP's Financial Supervision Sector is primarily responsible for assessing the BSFIs' compliance with the AML/CFT laws and regulations, the adequacy of their ML, TF, and PF risk management framework, and its effective implementation to prevent their use for ML/TF/PF activities.

⁴² R.A. No. 11055 signed on 6 August 2018. Section 9 of the Act requires every Philippine citizen and resident alien to personally register with the Philippine ID system.

The unit develops AML/CFT supervisory strategies, rules and regulations, guidelines, and examination procedures, that are aligned with international AML/CFT standards and best practices adjusted according to the Philippines' risk and context. An AML/CFT examination manual is in place which contains specific procedures to be performed during AML examination across supervised institutions, with due consideration to the application of the principle of proportionality to ensure that procedures are relevant to the business and complexity of the BSFI examined.

To implement risk-based supervision, the BSP adopted the ARRS in 2012, which is a tool used to assess the robustness of the BSFI's AML/CFT framework. The ARRS was recently enhanced with the introduction of the MRAS which incorporates the determination of the inherent risk of the BSFIs and their net risk after considering the quality of risk management system. This is also aligned with the BSP's SAFR⁴³.

- 3.1.18. Banks have shown considerable progress in fulfilling their AML/CFT obligations and in complying with AML/CFT requirements since the adoption of ARRS in 2012. This was recognized in the MER which cited that the high volume of BSP's supervisory activity over the past five years has positively impacted the AML/CFT compliance of banks⁴⁴.
- 3.1.19. To supplement institutional onsite examination, horizontal or thematic reviews are also conducted to effectively utilize and manage resources in identifying the emerging sources of ML/TF/PF risks and vulnerabilities in a specific sector. Six (6) thematic reviews were conducted in 2019 and 2020 covering key areas such as risks posed by OGB customers, illegal investment scheme, CBRs, and risk related to OSEC, TF and TFS. These resulted in, among others, issuance of necessary guidance papers to inform BSFIs of how to identify and mitigate risks arising from these emerging issues.
- 3.1.20. *Close coordination with the AMLC and other LEAs.* The BSP closely coordinates with various governments agencies to inform risk-based AML/CFT supervision. The MOA dated 24 April 2019 between BSP and AMLC sets out the framework for cooperation and coordination with respect to information exchange, compliance, and enforcement between BSP and AMLC for the prevention, control, and detection of, and imposition of sanctions of the AMLA and TPFSA and other relevant laws and regulations. Also, there are periodic meetings through the NALECC Sub-Committee on AML/CFT as well as the

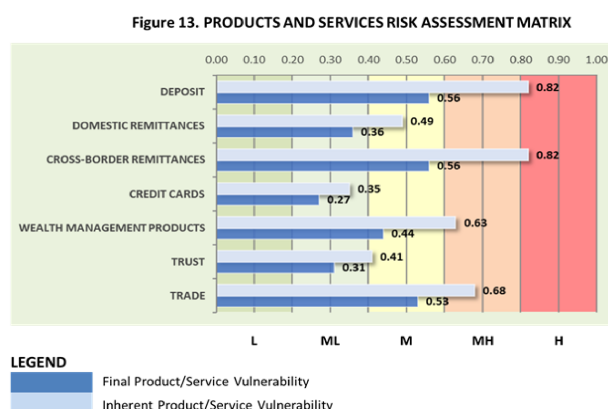
⁴³ SAFR is the BSP's risk assessment tool. It aims to facilitate robust, dynamic and forward-looking assessments of BSFIs. It explicitly links systemic importance and risk profile of a BSFI to the crafting of supervisory plans for each supervised institution such that: (i) supervisory attention continues to be proportionately focused on BSFIs that have greater impact and higher risk; and (ii) prompt and calibrated enforcement actions are deployed to reinforce prudent risk-taking behavior.

⁴⁴ APG AML/CFT Measures Philippines MER 2019, Par. 493, page 134

Sub-Committees under the NACS to achieve a whole-of-country approach to combat ML and TF.

PRODUCTS AND SERVICES VULNERABILITY

3.1.21. In terms of inherent vulnerability, deposit products and cross-border remittances have *high* vulnerability to ML/TF/PF risk, followed by trade transactions and wealth management (*medium high*). Domestic remittances and trust products are at *medium* risk level, while credit card products pose *medium low* risk. After considering the controls and features, net product vulnerabilities range from *medium low* to *medium*.



A. DEPOSITS - Medium

The inherent vulnerability of deposits is assessed as *high*. Almost all of the ML/TF/PF typologies involved deposit accounts, being the most common gateway to the financial system. Total deposit liabilities stood at PhP14.2 trillion⁴⁵ as of 30 June 2020, which funded 76.3 percent of total assets of the PBS⁴⁶. Most of the deposit account holders (99.2 percent) are residents and more than majority (around 80 percent) are classified as “normal” risk. Deposit products were largely used for cash transactions⁴⁷ (80.8 percent of the total covered transactions or PhP138.1 trillion) and to facilitate domestic and cross-border wire transfers. There are various alternative channels for account opening, such as technology-aided platforms, outsourcing arrangements, and third-party reliance. Technological innovations enable depositors to complete transactions using e-banking facility, withdraw through ATMs, and facilitate instant fund/wire transfers. Non-face to face use of the product is available supported by control measures.

Considering that existing and appropriate AML/CFT controls are in place, inherent ML/TF risk on deposit products is mitigated and thus, the residual risk on deposits is *medium*.

⁴⁵ Report on the Philippine Financial System – First Semester 2020

⁴⁶ <https://www.bsp.gov.ph/SitePages/Statistics/BSFinancialStatements.aspx?TabId=1>

⁴⁷ Top 5 transactions related to cash are CDEPC, CWDLO, DTDYC, CENC and KCCPC

B. DOMESTIC REMITTANCES – Medium low

Domestic remittance product and service has *medium* inherent risk. As of 31 December 2019, domestic remittances aggregated to PhP15.44 trillion⁴⁸, representing 62.91 percent of the total remittance transactions. Customers availing this service are mostly salaried individuals and/or domestic migrants, and most transactions originate from the NCR and CALABARZON region⁴⁹. There is a notable shift from “use of cash” to “electronic/mobile channels” since the launch of the NRPS in 2017 (i.e., Instapay and PesoNet) which contributed to the growth of domestic remittances. Non-face to face channel is prominent in delivering domestic remittance service through e-banking services/platforms, online fund transfers and bills payment.

Domestic remittance has been an attractive channel to money launderers in order to move money linked to illegal activities (e.g., TF and drug trafficking). Likewise, the growth of digital remittance services and technology has led to the emergence of new ML typologies through unauthorized fund transfers making it easier for criminals to circumvent identity verification processes⁵⁰.

In this regard, banks with domestic remittance services have general and specific AML/CFT controls, particularly for customer acceptance and identification, and ongoing monitoring of transactions. Likewise, banks generally have electronic systems to record and monitor domestic remittance transactions, thus, records are easily traceable. Nonetheless, there is a continuing need to refine and adjust measures, particularly on customer identification and monitoring given new typologies. Thus, residual risk is *medium-low*.

C. CROSS-BORDER TRANSACTIONS – Medium

Cross-border transactions are inherently *high* risk. These represent bank’s international wire transfers/remittances and trade finance products and services that are usually coursed through correspondent banking as well as private banking and wealth management. Cross-border transactions encompass remittances for both personal and business purposes as well as payments and receipts for trade transactions. In 2019, the Philippines ranked fourth worldwide among the top remittance receiving countries⁵¹. Total estimated international trade transactions of PhP18.45 trillion⁵² facilitated by

⁴⁸ Based on AML/CFT Survey conducted by the BSP covering UBs, KBs, TBs and RBs

⁴⁹ <https://www.prnewswire.com/news-releases/philippines-money-transfer-and-bill-payments-market-report-2018-over-the-past-six-years-the-bpo-industry-in-the-country-has-augmented-at-an-average-rate-of-25-30-300745723.html>

⁵⁰ *Ibid.*

⁵¹ <https://migrationdataportal.org/themes/remittances>

⁵² Data sources: AMLC, DTI, PSA, BSP, Respondent Banks to BSP survey via APCB.

banks from 2017 up to 1st half of 2020 account for 99.0 percent of the total assets of the banking system as of 30 June 2020⁵³. Transactions involved certain high-risk jurisdictions. The non-face to face feature is available for cross-border transactions but this was not widely used particularly in the case of trade transactions.

Transnational crimes usually use cross-border transactions to launder proceeds of the illegal activities. The risks are mitigated by specific controls for cross-border remittances, such as designating a specific unit handling these transactions, pre-credit review, and screening of counterparties, including vessels and ports for trade transactions. Thus, residual risk for cross-border remittances is *medium*.

D. WEALTH MANAGEMENT PRODUCTS – **Medium**

Inherent risk of this product is *medium high*. Total exposure is considered medium at PhP1.15 trillion⁵⁴ for 2019, which accounts for 6.27 percent of the total assets of the PBS as of 31 December 2019. Average transaction size is high at around PhP31.0 million as this is offered only to a select market segment of high net-worth individuals and corporate clients, who are generally known to the bank. Almost 98 percent of the wealth management/private banking clients are domestic individuals and juridical entities. Most banks assign specific relationship managers/account officers to personally cater to the needs of the customer.

Common ML typology for this product includes co-mingling of illicit funds as deposit/investment products in large aggregate cash transactions/investments and/or movement/transfer of large cash, check, or wire deposits into various cross-border transactions. Use of the product/service in fraud or tax evasion schemes exists but on a limited scale. It will be useful if CTR/STR data will contain identifier to relate the transaction to wealth management/private banking account or customer. This will provide more accurate information on the extent of use of wealth management/private banking for ML/TF/PF activities.

Final product vulnerability or residual risk is *medium* given the existing AML controls in place, such as establishment of the true and full identity of the customer and beneficial owners, and sources of wealth and funds, and the required senior management approval, other than the relationship manager/account officer. Strict monitoring of transactions is an ongoing process to ensure that transactions have underlying legal or trade obligation and source of funds is established.

⁵³ <https://www.bsp.gov.ph/SitePages/Statistics/BSFinancialStatements.aspx?TabId=1>

⁵⁴ Based on AML/CFT Survey conducted by the BSP covering UBs, KBs, TBs and RBs

E. CREDIT CARD – Medium low

Inherent risk for credit cards is *medium low*. Credit card limits approved/granted increased from PhP1.20 trillion in 2017 to PhP1.50 trillion as of 30 June 2020. This represents 15 percent of Total Loan Portfolio of the PBS.⁵⁵ Customers are mostly retail with normal to low risk profile. About a third of the transactions were done abroad. There are alternative servicing-channels such as through agents who solicit new clients.

A common ML scheme is when a cardholder prepays using illicit funds, creating a credit balance on the account. Subsequently the cardholder requests for a credit refund, which enables him to further obscure the origin of the funds and use it for other transactions. Nonetheless, all banks offering credit cards have systems and controls. Anonymity issue is largely eliminated since both principal and supplemental cardholders are subjected to relevant CDD and on-going monitoring. Thus, the residual risk is *medium-low*.

F. TRUST PRODUCT – Medium low

Inherent risk of trust product and services is *medium*. As of 30 June, 2020⁵⁶, total AUM reached PhP2.99 trillion, posting growth of 10.85 percent. IMA individual and corporate clients posted an average transaction size of PhP13.04 million and PhP164.00 million, respectively. For other fiduciary activities, average transaction size is PhP25.66 million and PhP86.04 million for individual and corporate clients, respectively. UITF products, although retail in nature, showed a high average transaction size of PhP1.53 million and PhP3.05 million, for individual and corporate clients, respectively. Most clients are individuals (95 percent) and 87 percent are assessed as normal risk. ML typologies on the abuse of trust products is limited.

After considering existing AML/CFT controls, residual risk is *medium-low*. CDD procedures are performed during on-boarding of clients and on-going monitoring of transactions to understand the normal and reasonable business activities. Informative reports are required to be made by the trustee to clients and other parties who have legitimate interest in the trust. Likewise, banks submit periodic prudential reports on their trust business to the BSP.

⁵⁵ CCBAR as of 30 June 2020 from Department of Supervisory Analytics

⁵⁶ <https://www.bsp.gov.ph/SitePages/Statistics/BSFinancialStatements.aspx?TabId=3>

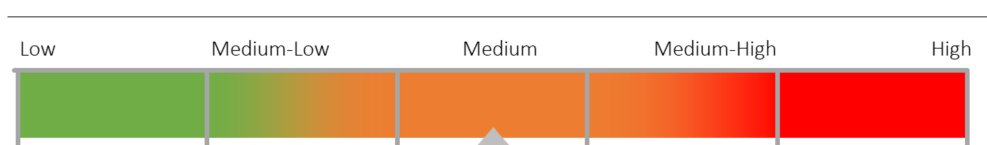
G. TRADE FINANCING – Medium

Risk associated with trade transactions is *medium-high*. Total estimated international trade transactions of PHP18.45 trillion⁵⁷ facilitated by banks from 2017 up to 1st half of 2020 accounted for 99 percent of the total assets of the PBS as of 30 June 2020. Majority of the customers (73 percent) are classified as normal risk. Avenue for cash transaction is limited but there is large exposure of trade commodities and services to both domestic and international markets. Transactions are inherently complex and document-intensive, which are usually processed manually.

The common trade-based ML/TF/PF methods or red flags include the submission of forged/spurious trade documents, request to credit trade proceeds to unrelated third party, consignment of imported goods to an unrelated individual, remittance and foreign exchange of trade payments for import and export of goods taking place outside the Philippines, dealings with trade parties involved in crimes such as drug trafficking, and misrepresentation on the description or quality of goods. The exploitation of shell or front companies significantly increased the vulnerability of trade transactions. With this, banks establish relevant controls deemed necessary to counter ML/TF risks from trade transactions. Majority of banks employ either or both manual and electronic monitoring tools to detect TBML transactions resulting in a residual risk of *medium*. However, further understanding and establishment of controls, covering all types of trade facilitation, other than trade financing, is needed to further reduce risks.

3.2. OTHER FINANCIAL INSTITUTIONS

3.2.1. NON-BANK ELECTRONIC MONEY ISSUERS



3.2.1.1. Non-bank EMI industry consists of NBFIs authorized under Section 402-N of the MORNBFIs to issue e-money⁵⁸. Non-bank EMIs operate e-wallets that enable users/accountholders to send and receive money values, as well as

⁵⁷ Data sources: AMLC, DTI, PSA, BSP, Respondent Banks to BSP survey via APCB.

⁵⁸ Electronic money (e-money) is defined under the same section as a monetary value as represented by a claim on its issuer, that is: (a) electronically stored in an instrument or device; (b) issued against receipt of funds of an amount not lesser in value than the monetary value issued; (c) accepted as a means of payment by persons or entities other than the issuer; and (d) withdrawable in cash or cash equivalent. E-money is not a deposit, thus it will not earn interest and will not be covered by deposit insurance.

make purchases and payments through accredited partner/agent outlets, using mobile phones and/or cash cards.

Since 2009, the number of non-banks with EMI license grew from seven (7) in 2016 to 24 as of 30 June 2020, but seven (7) are not yet fully operational. This contributed to the consistent rise in the volume and value of e-money transactions as the public becomes more attuned to the use of electronic gadgets for their payment needs⁵⁹. From 2016 to 2019, usage of e-money attributed to the non-bank EMIs posted an AAGR of 62 percent in contrast with the AAGR for banks at negative 4 percent.

3.2.1.2. *Overall vulnerability of the Non-Bank EMIs is medium.* The ML/TF/PF risk landscape of the EMI sector is constantly evolving. As innovative products/services⁶⁰ are introduced and financial transactions shift to digital channels, customers with varying risk profiles grow and network of delivery channels expand. These developments open new opportunities to various threat actors or criminals to exploit the vulnerabilities of the non-bank EMI sector. Thus, the overall inherent risk of non-bank EMIs is *medium*.

3.2.1.3. *The quality of general AML/CFT/CPF controls is medium.* AML/CFT legal and regulatory frameworks are in place, the scope of supervision and enforcement actions are adequate, and transaction limits are mandated. Continuing initiatives to strengthen EMIs' AML/CFT framework, processes and controls have been observed. Nonetheless, enhancements in the EMIs' AML/CFT/CPF controls and compliance culture are warranted including, but not limited to, aspects of customer and transaction monitoring and managing risks arising from outsourcing arrangements.

ASSESSMENT OF CONTROLS

3.2.1.4. *Comprehensiveness of AML Legal Framework – High.* Non-Bank EMIs are mandated to comply with the prevailing AML/CFT laws as well as the implementing rules and regulations issued by the BSP and the AMLC. They are subject to BSP supervision and regulation through Sections 402-N (Issuance and Operations of Electronic Money), 901-N (MSB Operations)⁶¹, and Part 9 of Q Regulations (AML Regulations) of the MORNBF⁶². These regulations govern the registration, operations and reporting obligations of

⁵⁹ Report on the Philippine Financial System 2nd Semester 2019 by Supervisory Policy and Research Department

⁶⁰ Use of QR Code for payments, transfers to/from deposit account for individual customers, linking an e-money account to a virtual card and/or an international payment account (created via access to payment operator's platform), among others

⁶¹ As amended by Circular No. 1039 dated 03 May 2019.

⁶² <https://www.bsp.gov.ph/Regulations/MORB/Sep2017MORNBF1.pdf> (for Volume 1) and <https://www.bsp.gov.ph/Regulations/MORB/Sep2017MORNBF2.pdf> (for Volume 2)

EMIs and provide the enforcement actions, sanctions and penalties for weaknesses in AML/CFT framework and breaches of AML/CFT regulations.

- 3.2.1.5. *Availability and Enforcement of Administrative Sanctions – High.* Sections 901-Q and 901-N of MORNBF provide for the sanctions on non-compliance with BSP regulations. Sanctions range from written reprimand to cancellation of registration. The BSP and the AMLC may also impose monetary penalties on EMIs for AML/CFT weaknesses and violations, pursuant to their respective mandates. Since 2017, two (2) EMIs were required to execute an acceptable LOC⁶³ to address deficiencies in AML/CFT controls relative to its profile. One has been released from its LOC as a result of improvements in the risk management framework.

In addition, EMIs have their own policies and procedures in handling internal investigations and imposing sanctions against erring personnel.

- 3.2.1.6. *Availability and Effectiveness of Entry Controls – High.* Requirements for licensing of non-bank EMIs are defined in the BSP regulations, such as fit and proper standards, minimum capitalization (Php100 million), and submission of notarized Deed of Undertaking stating, among others, the BOD's full responsibility to comply with AML/CFT requirements. The evaluation process involves understanding the business model, assessment of the adequacy of AML/CFT framework, and conduct of on-site verification.

From 2017 to 2020, 17 applications were returned due to failure to comply with existing requirements such as minimum capital, expected business model, and submission of documents. Meanwhile, two (2) out of around 90 officers were disqualified for negative information noted during the evaluation process.

- 3.2.1.7. *Integrity of Business/Institution Staff – High.* The requirements on fit and proper assessment as well as robust recruitment and screening process also apply to EMIs. This involved, among others, requiring the DOS to submit certification of no pending criminal and administrative cases, and conducting background investigation and criminal record checking. There is also continuous assessment on the fitness and propriety of DOS. From 2017-2019, 90 proposed directors/officers were found to have no derogatory record based on the results of screening against existing database.⁶⁴ No incidents of criminal activity involving DOS/employees of EMIs were noted or reported to BSP. The surveillance activity related to this

⁶³ The LOC is an enforcement action that involves the Supervisor requiring a BSFI's BOD to make a written commitment to undertake specific remedial actions within a reasonably short period of time to adequately address the root causes of the problem/s as determined by the BSFI

⁶⁴ Source, Technology Risk and Innovation Supervision Department, BSP

has also been improved with the issuance of Circular No. 1104 dated 27 November 2020 requiring MSBs, which include EMLs, to submit RCLs.

- 3.2.1.8. *Effectiveness of Suspicious Activity Monitoring and Reporting – Medium.* Given the huge volume and fast-moving transactions, EMLs have adopted electronic systems in recording customer information and transactions as well as in identifying and monitoring possible suspicious transactions. Customer screening against sanctions and watchlist databases is an integral part of the on-boarding and ongoing monitoring processes. As a result of their ongoing monitoring, STRs filed for the period covered grew from 4,316 cases in 2017 to 67,534 in 2019. This increased substantially to 72,453 for the first half of 2020 brought about by the growth in the use of digital payments amid the pandemic. This shows that the EMLs are progressively learning to identify various threats that are trying to exploit the industry.

Scope for enhancements in AML system and suspicious transaction monitoring include (i) reinforcing process to aggregate transactions on a customer level; (ii) adjusting system scenarios and parameters to detect relevant suspicious indicators; (iii) conducting periodic screening of customers; and (iv) reviewing/monitoring of outsourcing arrangements.

- 3.2.1.9. *Corporate Governance. – Medium.* EMLs have established appropriate governance structure to manage the risk arising from ML/TF activities. These include the establishment of Board and SM level committees, compliance office and audit. Various initiatives to improve governance are being undertaken such as revision of the AML/CFT policies and strengthening of monitoring systems. Nevertheless, scope for enhancements include conducting IRA, improving scope of reporting to the BOD/SM, and expanding audit coverage.
- 3.2.1.10. *Effectiveness of Compliance Function - Medium.* EMLs have dedicated compliance function that directly and regularly reports to the BOD and/or SM level committee(s) matters related to AML/CFT compliance and risk management, including compliance testing issues. Compliance officers are pro-active in addressing concerns through close coordination with BSP and active participation in industry discussions. Initiatives to further improve employee awareness, as well as the guidelines and scope of compliance testing are being done. Areas for improvement include having adequate staffing in the compliance office, proactive identification of STs, and improving RBA to compliance testing.
- 3.2.1.11. *AML Knowledge of Business Staff – Medium.* Board, senior management, and employees are required to attend the annual in-house trainings and refresher courses on AML/CFT. Policies are in place to guide personnel in performing their AML/CFT-related functions. New hires are trained and

made aware of their duties and responsibilities related to AML/CFT prior to job deployment. Nonetheless, continuous training of personnel is warranted to ensure effective implementation of key AML/CFT process, particularly in the areas of customer acceptance and identification and on-going monitoring of customers, emerging issues, and relevant typologies.

3.2.1.12. *Availability and Access to Beneficial Ownership Information – Medium.* The identity of the UBO is mainly obtained through the customer’s declaration and this is verified against the updated GIS filed with the SEC.

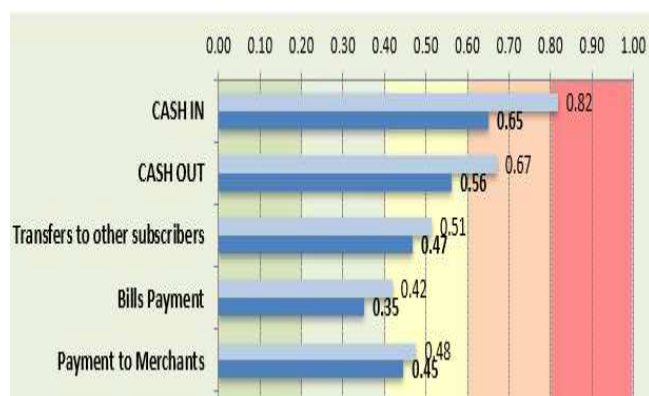
3.2.1.13. *Availability of a Reliable Identification Infrastructure – High.* EMLs’ customer identification process is primarily through the presentation of identification documents⁶⁵ issued by competent government agencies. Verification is made through online facility or via text to the provider of ID, as applicable. Meanwhile, the implementation of the national identification system will further facilitate the conduct of efficient and reliable customer identification and will streamline customer onboarding process. For corporate clients, documents such as proof of business or registration, and special licenses, as applicable, are required.

3.2.1.14. *Effectiveness of Supervision Procedures and Practices – High.* The risk-based supervision and assessment implemented on banks are similarly applied for EMLs wherein the degree and frequency of onsite examination and intensity of offsite supervision are based on the risk profile of the EMLs. Assessment includes determining the inherent risk and quality of risk management framework of the entity.

PRODUCTS AND SERVICES VULNERABILITY

3.2.1.15. *Cash-in and Cash-out services have higher vulnerability to ML/TF/PF risk, while other transactions such as transfers to other subscribers, bills payment and payments to merchants pose medium risk. After considering controls, the net risks of these products were medium, except for bills payment which was low.*

Figure 14. Product and Services Vulnerability



⁶⁵ These include, among others, Passport, Unified Multi-Purpose ID (UMID), Professional Regulation Commission (PRC) ID, Driver’s License and NBI clearance

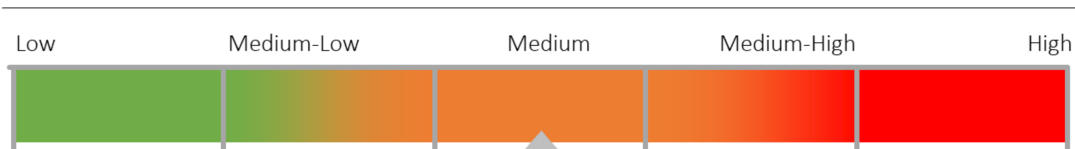
3.2.1.16. *Cash-in and Cash-out.* Cash-in and Cash-out transactions have inherently high and medium-high ML/TF/PF risk, respectively. With this, necessary controls and transaction limits are instituted, thus, the residual risk is **medium**. Cash-in and Cash-out transactions can be facilitated via cash centers, agents and fund transfer facility from and to an account maintained with a bank, another EMI or other financial technology companies. Cash-in is the entry point that can be utilized by criminals to channel illegal proceeds. Cash-out, on the other hand, is where cash withdrawal and cross-sector fund transfer transactions are facilitated. These can both facilitate cross-border fund transfers through the EMIs' global remittance partners. There is a notable growth of the channels utilized to facilitate top up (cash-in) and/or withdrawal (cash-out) of e-money, such as pawnshops, MSBs and other accredited/registered remittance agents, including convenience stores, gasoline stations, and grocery/sari-sari stores, among others. EMIs also accept various clients of different nationalities.

With these vulnerabilities, bespoke EMI regulations and EMI's risk management framework are designed to mitigate ML/TF risks, among others. These include (a) adopting monthly load limit of PhP 100,000, unless a higher amount was approved by the BSP; and (b) defining permissible transactions/functionalities depending on the level of KYC verification.

3.2.1.17. *Transfers to Other Subscribers, Payment to Merchants and Bills Payment.* Transfers to Other Subscribers pose medium net risk. This involves fund transfers to another e-money account, which can only be done by a fully-verified e-money account holder. Payment to merchants can be used via POS terminals, QR scanning devices or online portals. An emerging concern in this space is the use of this facility by basic/non-verified accountholders to perform cash-out. Necessary actions are being taken to curb this practice.

Lastly, bills payment, which posed low net risk, provides e-money accountholders a facility to settle utility bills, credit cards, taxes, insurance, or other dues payable to any accredited billers. Controls in place include setting daily maximum bills payment limits depending on the account type and requiring OTP for transactions beyond the set threshold.

3.2.2. VIRTUAL CURRENCY EXCHANGES/VIRTUAL ASSETS SERVICE PROVIDERS



- 3.2.2.1. VA refers to any type of digital unit that can be traded, or transferred, and can be used for payment or investment purposes. It is used as a medium of exchange or a form of digitally stored value created by agreement within the community of VA users. Meanwhile, VASP refers to an entity that offers services or engages in activities that provide facility for the transfer or exchange of VA, which involve the conduct of one or more of the following activities: 1) exchange between VA and fiat currencies; 2) exchange between one or more forms of VA; 3) transfer of VA; and 4) safekeeping and/or administration of VA or instruments enabling control over VA. In this report, the use of the term cryptocurrency, VC, and VA shall be used interchangeably. The same applies for VCE and VASP.
- 3.2.2.2. BSP-registered VCEs significantly increased from two (2) in 2017 to 15 as of 30 June 2020. Of these, only 8 are actively operating in the country. The value of VA transactions has been growing since 2017 while the volume remains on the average. This indicates an increasing value on each VCE transaction over time. Total volume and value of transactions of VCEs, stands at 4.272 million and PhP59 billion, respectively. The top three players comprised 99.4 percent of the total value of VA transactions as of 30 June 2020. The biggest VCE player, meanwhile, accounts for 97.7 percent of these transactions.
- 3.2.2.3. *Overall vulnerability for the VCE/VASP sector is medium.* The VCE/VASP sector is highly vulnerable to ML/TF/PF. VAs have unique features such as cross-border nature of transactions, capacity for fast settlement, facility for person-to-person exchange, and potential for increased anonymity and obfuscation of the source of the VA, transaction flows and counterparties through anonymizing tools and services. These are evident in the emerging use of VASPs for certain crimes such as those related to investment scams, swindling, OSEC, drug trafficking, and TF.
- 3.2.2.4. *The quality of general AML/CFT/CPF controls is assessed as medium.* The AML/CFT legal, regulatory and institutional frameworks are in place and generally consistent with international AML/CFT standards.

ASSESSMENT OF CONTROLS

- 3.2.2.5. *Comprehensiveness of AML /CFT/CPF Legal Framework – High.* The BSP has issued guidelines to enhance safeguards against emerging ML/TF risks from the use of VCs. Section 902-N of the MORNBFIs covers entities offering services or engaging in activities for the conversion or exchange of fiat currency to VC or vice versa. Under this, VCEs are required to register with the BSP as RTCs and the AMLC. They are also required to comply with minimum capital, internal controls, and reporting obligations, among

others. Transactional requirements⁶⁶ for large value pay-outs were also adopted as additional controls to manage ML/TF risks⁶⁷. Existing AML/CFT rules and regulations also apply to VASPs.

The regulatory framework for VASPs has been recently enhanced. Key amendments include the new requirements and standards issued by the FATF and other recognized risk management principles. The revised framework contains expanded definition of VASPs, CDD and transactional requirements. It emphasizes that all VA transfer transactions shall be considered as cross-border wire transfers and must comply with pertinent AML/CFT rules, including the travel rule requirement.

3.2.2.6. *Availability and Enforcement of Administrative Sanctions – High.* As with other BSFIs, VASPs are also subject to the Supervisory Enforcement Policy of the BSP. Section 902-N also prescribes additional monetary penalties, sanctions and other enforcement action/s to VASPs. These include sanctions for operating without prior registration from the BSP, violations of the AMLA, as amended, erroneous/delayed/non-submission of reports, and violations of any provisions of Section 902-N. Likewise, they are also covered by the AMLC's RPAC and ARI No. 5 (Enforcement Action Guidelines).

3.2.2.7. *Availability and Effectiveness of Entry Controls/ VCE Licensing Process – High.* VASPs are subjected to strict licensing process by the BSP. This includes assessing the fitness and propriety of the DOS, reviewing business model, and evaluating the VCEs plan to comply with the AMLA, among others. On-site verification procedures are conducted to verify the applicant's information technology applications/systems for AML/CFT compliance.

BSP has also adopted market monitoring and issued guidelines to other BSFIs on risk management practices for VCE clients which include requirement to deal only with BSP and AMLC-registered VCEs. There is continuous engagement and feedback mechanism with the industry. Surveillance activities, including market monitoring, is ongoing to identify unregistered BSFIs, including VASPs.

3.2.2.8. *Integrity of Business/Institution Staff – High.* As part of ensuring the integrity of the business and institution's staff, the BSP conducts assessment of the fitness and propriety of the VASP's DOS. This involves checking derogatory or negative information during registration process, and upon

⁶⁶ Large value pay-outs of more than P500,000 or its foreign currency equivalent, in any single transaction with customers of counterparties, shall only be made via check payment or direct credit to deposit accounts.

⁶⁷ <https://www.bsp.gov.ph/SitePages/MediaAndResearch/MediaDisp.aspx?ItemId=4211>

any changes in ownership and control structure of the VASPs. Meanwhile, VCEs also adopt their own KYE measures to ensure the integrity of prospective and existing employees. They conduct background and criminal record checking on prospective employees. Code of conduct, code of ethics and whistle blower policy were also adopted by VASPs to promote employee integrity.

- 3.2.2.9. *Effectiveness of Sanctions Screening and Suspicious Activity Monitoring and Reporting – Medium.* Overall effectiveness of suspicious activity monitoring and reporting varies across VCEs. The market leader has demonstrated an acceptable level of suspicious activity monitoring mechanism that is capable of detecting and reporting suspicious activities. On the other hand, other VCEs' monitoring systems are developing to effectively monitor and detect possible suspicious transactions. The STR submissions of VASPs were mostly filed by the top player. From a market share standpoint, this particular VASP comprised 99 percent and 93 percent of the total volume and value of transactions, respectively. VCEs conduct sanctions screening of customers and beneficial owners⁶⁸, and they also have policies in place to guide personnel in handling positive hits.

Scope for improvements include refining the parameters and scenarios, documenting the results of investigation, and increasing manpower complement, among others.

- 3.2.2.10. *AML Knowledge of Business/Institution Staff – Medium.* AML knowledge is reinforced through general trainings attended in various modalities (e.g., external seminars, echo sessions, classroom training). However, only 67 percent of the sector have completely attended the required AML/CFT trainings and refresher courses. Scope and reach of the regular refresher courses likewise need to be enhanced to align with the evolving risk and regulatory landscape of the sector.
- 3.2.2.11. *Effectiveness of Compliance Function – Medium.* In contrast with the other players, the VASP holding majority of the market share has its own Compliance Office and Internal Audit units. Scope for enhancements include assuring adequacy of manpower complement and self-assessment programs, and enhancing ML/TF risk management controls, particularly on CDD, transaction monitoring, and filing of CTRs/STRs.
- 3.2.2.12. *Corporate Governance on AML/CFT – Medium.* Degree of corporate governance effectiveness varies. One VASP player (with more than 90 percent market share) has instilled a culture of compliance among its

⁶⁸ These include the following: UNSC Consolidated List, OFAC-SDN List, AMLC Designated List, and EU Sanctions List, among others.

officers and employees, supports its self-assessment functions, and has provided timely and relevant AML/CFT issues to the BOD and SM. Compliance testing results are reflected in the employees' performance evaluation to ensure consistent compliance. The other VCEs need to further strengthen governance framework suitable to their risk profile.

3.2.2.13. *Availability and Access to Beneficial Ownership Information – Medium.* VASPs employ various means to identify and verify UBOs. These include e-KYC and technology-aided CDD and verification software, combined with manual measures, such as searching through company registration and/or international beneficial ownership registers and databases, and internet crawling. Nonetheless, the identification of beneficial ownership remains to be one of the challenges⁶⁹ of the VASPs considering the absence of a readily accessible central database system containing information on the beneficial owners (including their digital-specific IDs, addresses, and footprints).

3.2.2.14. *Availability of reliable identification infrastructure – High.* Depending on certain KYC threshold policy, VASPs generally rely on the IDs issued by official government authorities to conduct customer identification. These are further validated through online verification facilities to determine authenticity of some IDs. The enactment and implementation of the national ID, while still ongoing, is expected to facilitate and improve the conduct of identification and verification of customer identity.

Meanwhile, the FATF guidance on VAs/VASPs also recommend the gathering of non-traditional customer information such as IP address with associated time stamp, geo-location data, device identifiers, VA wallet addresses and transaction hashes. These should be explored to supplement and strengthen customer identification and transaction monitoring process.

3.2.2.15. *Quality of risk-based supervision – Medium.* RBA to AML/CFT supervision adopted for banks is also implemented for VCEs. The BSP established procedures for granting of COR and conducts ongoing supervision to assess compliance with requirements and commitments in their Deed of Undertaking⁷⁰.

Consistent with RBA, two (2) out of 15 VASPs were subjected to full scope onsite examinations in 2018 and 2019. These are the registered VCEs prior

⁶⁹ Based on the survey and interviews conducted, challenges that may hamper UBO identification/verification include : (1) presence of identity obscuring or anonymity enhancing technologies that impede ability to verify client's address/geographical location, authority in transacting, and if the transacting party is the actual registered client or the beneficial owner of the transaction and (2) counterparty implementation risk for dealings with other VASPs and jurisdictions with different AML/CFT requirements

⁷⁰ Deed of Undertaking include commitments of the VCE to comply with VCE registration, operating procedures, AML/CFT requirements, and reporting requirements among others.

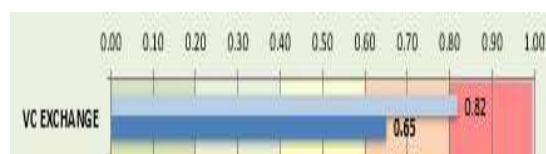
to 2018 and have combined 97.67 percent market share. The other VCEs were subjected to limited scope⁷¹ examinations as part of assessment for the issuance of COR.

One of the emerging supervisory concerns is the presence of peer-to-peer crypto marketplaces and dealings with unregistered/non-BSP registered entities. Hence, capacitating supervisors with surveillance technological solutions and continuing skills development are necessary to effectively monitor VASP activities and prescribe bespoke policies and guidance commensurate to the identified risks of the sector.

- 3.2.2.16. *Enforcement of Administrative Actions – High.* Although there were no records yet of monetary penalties imposed on VASPs given this is a fairly new segment, two VCEs were delisted between June to July 2020 due to non-compliance with the PCOR, and failure to commence operations within prescribed period. Directives to implement corrective actions were issued as well as warning to SM and BOD.

PRODUCT AND SERVICES VULNERABILITY

- 3.2.2.17. The services, conversion, or exchange to fiat currency to VC or vice versa, being offered by VCEs are inherently high risk to ML/TF.



- 3.2.2.18. The factors that increase the risk of VCEs include: (i) increasing volume and value of transactions which as of 30 June 2020 stood at USD 1.17 billion (approximately Php59.162 billion), which increased by 600 percent from 2018, (ii) high level of cash activities, (iii) existence of high-risk customers as well as clients from high-risk jurisdictions, (iv) increasing use of VAs in several ML/TF related crimes such as investment scams, swindling, OSEC, and TF, and (v) increasing number of STs involving VCs/VCEs with total of 103,291 STRs aggregating to Php1.910 billion⁷².
- 3.2.2.19. *Controls.* This risk is mitigated by the existence of controls. These include requirement for large transactions (i.e., Php500,000 and above) to be paid via check payment or direct credit to deposit accounts. Moreover, transactions related to cross-border from 2018 to 2019 are minimal with

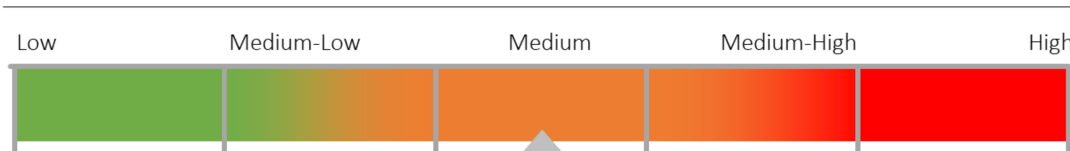
⁷¹ Includes AML components on CDD, onboarding procedures, CT/ST reporting, and AML Training.

⁷² 87 percent of STRs involved investment fraud such as participation in swindling, investments schemes, and other violations under The Securities Regulations Code of 2020 and deviations from the clients' profile and/or expected financial activity.

only 2 percent and 17 percent, respectively, of VA transactions. Average VA transaction is small ranging from PhP1,500 to PhP3,000 from 2017-2019.

3.2.2.20. Considering the foregoing, overall product vulnerability is *medium high*.

3.2.3. TRUST ENTITIES AND LEGAL ARRANGEMENTS



3.2.3.1. TEs are comprised of TCs and NBFIs with trust license supervised by the BSP. The main TE products assessed are business trust (e.g., UITF), agency/other legal arrangements, and OFS which involve private trust (e.g., court, testamentary, et. al).

3.2.3.2. As of 30 June 2020,⁷³ there are 36 BSFIs with trust authority including five (5) TEs with inactive status. Twenty-nine (29) operate as a separate business unit of banks, four (4) are TCs, and two (2) are NBFIs. As of 30 June 2020, stand-alone trust entities have total AUM of PhP1,073 billion or 5.76 percent of the banking sector assets.

3.2.3.3. For the purpose of this Section, the trust sector shall refer to stand alone trust entities only, excluding the trust operations of banks which were assessed in the product vulnerability assessment under the banking sector.

3.2.3.4. *Overall vulnerability of the trust sector is medium.* Inherent risk is *medium* in view of the features of the products and services that the TEs offer. Agency – IMA pose greater risk given its directional feature that allows the trustor to exercise investment decisions for the account. This makes the product attractive to high-risk clients in general. UITFs’ vulnerability increases due to the rapid growth of alternative delivery channels through individual and institutional agents, mobile banking applications and e-wallets. Albeit, typologies on the use of the trust sector or its products for ML is limited.

3.2.3.5. *The quality of general AML/CFT/CPF controls is medium.* Comprehensive legal framework and implementing regulations, such as guidelines on the identification of beneficial owner, robust risk-based supervision by the BSP, and continuous enhancements in the AML/CFT framework of TEs, are among the factors that mitigate identified threats to the sector.

⁷³ Last accessed on 03 December 2020: <https://www.bsp.gov.ph/Lists/Directories/Attachments/3/trust1.pdf>

ASSESSMENT OF CONTROLS

3.2.3.6. *Comprehensiveness of AML Legal and Regulatory Framework – High.* Similar with other BSFIs, TEs are required to comply with AML/CFT laws, rules and regulations. In addition, regulations specific to TEs are codified in the MORNBFI, which cover, among others, rules and policies governing trust licensing and operations of TEs.

3.2.3.7. *Availability and Enforcement of Administrative Sanctions – High.* Section 37 of R.A. 7653, as amended by R.A. 11211, provides for the sanctions to be imposed on TEs found to be engaging in unauthorized trust and fiduciary business, whether as a primary, secondary, or incidental business. Meanwhile, Section 91 of the GBL provides specific sanctions such as suspension, removal of directors or officers, withdrawal of authority to engage in trust, restriction of activities, and suspension of privileges to establish branches for willful violations of the provisions of the GBL. Section 002 of the T Regulations provides guidance on the deployment of enforcement actions, which include corrective actions, sanctions, and other supervisory actions. Further, the AMLC, pursuant to its mandate under the AMLA, as amended, can independently impose administrative sanctions on CPs, including TEs, pursuant to its RPAC.

For 2017 to 30 June 2020, three (3) TEs, which account for 95 percent of the total TEs' AUM, were assessed as having acceptable AML/CFT framework, relative to their size, complexity, and risk profile. Thus, enforcement actions deployed were mainly directives aimed to address pockets of identified areas of concerns.

3.2.3.8. *Availability and Effectiveness of Entry Controls- High.* Section 79 of the GBL and Section 103-T of the T Regulations govern the licensing process for TEs. This involves evaluating the qualifications, financial strength, legal structure and management, including the fitness and propriety of the TE's incorporators/subscribers. Any application to establish a TC may be denied on several grounds, such as failure to meet the prescribed qualifications or if there are issues or concerns on the purpose or proposed operations of the TC. Since 2017, only four (4) TCs were licensed.

3.2.3.9. *Integrity of Staff – High.* Under Section 80 of the GBL, TEs are required to administer the funds or property under its custody with the diligence of a prudent man. The cardinal principle for all trust and other fiduciary relationships is fidelity. In this regard, the BSP employs procedures similar with banks in assessing the fitness and propriety of DOS of TEs. Further, TEs are required under existing regulations to adhere and adopt measures to ensure the integrity of their personnel on a continuing basis. These include, among others, (i) complying with the Fit and Proper Rule under Section 118

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE

3/19/21

JOSE MICHAEL E. CAMACHO

Bank Officer II, RMD

Administrative Services Department

Page | 48

to 121-T, (ii) adopting check and balance control mechanisms in assigning duties and responsibilities to personnel under Section 129 - T, and (iii) performing periodic lifestyle check and providing training on ethics and governance under Section 125-T, among others. Moreover, the qualifications of all personnel involved in the sales of UITF were expanded to ensure their competence and integrity.

- 3.2.3.10. *Effectiveness of Suspicious Activity Monitoring and Reporting – Medium.* TEs have instituted their own ML/TF risk management and control framework, which includes board and SM oversight, ML/TF prevention compliance program, monitoring system, and internal controls and audit. Customer screening as well as electronic and manual monitoring and reporting systems are in place.

Scope for enhancements include (i) improving customer risk profiling methodology and conduct of appropriate CDD procedures, which affect the quality of ongoing monitoring; (ii) refining alerts parameters suitable to the profile of the TE and improving alerts investigation process; and (iii) continuously strengthening controls to achieve better implementation of AML/CFT policies and procedures.

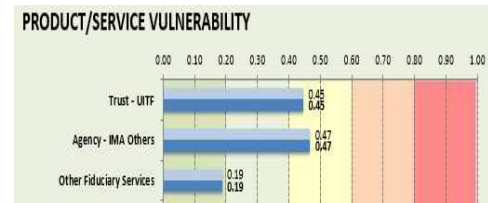
- 3.2.3.11. *AML Knowledge of Staff – Medium.* TEs adopt their respective AML training program tailored fit for personnel, management and AML officers. New employees are provided with relevant and updated AML/CFT-related trainings prior to deployment to their job functions. Refresher courses are offered annually to keep the staff abreast of new issuances and typologies. To foster culture of compliance and continuing AML education, TEs should ensure that their BOD and SM are likewise provided with sufficient AML trainings to enable them to effectively carry out their AML oversight functions. Also, TEs should monitor effectiveness of training programs conducted to detect skills gaps and address the same. This is to ensure that each personnel is aware of their AML responsibilities as well as the consequences of deliberately breaching AML/CFT obligations.

- 3.2.3.12. *Effectiveness of Compliance Function – Medium.* TEs have their respective Compliance Unit responsible for managing implementation of their AML/CFT framework, including the conduct of risk-based compliance testing. Manpower complement is generally adequate considering their risk profile. Scope for enhancements include improving risk-based compliance testing, particularly on review of conduct of EDD, and adequacy of alerts management. Nonetheless, commitments to improve and fully address issues raised by the BSP are well demonstrated.

- 3.2.3.13. *Corporate Governance- High.* BOD and SM oversight function of the major TEs is generally adequate in relation to their risk profile. BOD and SM are actively involved in AML/CFT matters which are adequately discussed during the BOD's regular meetings. Internal audit is independent and is supported by the BOD. Risk management practices of the major TEs are generally satisfactory. TEs should continually ensure that the BOD and SM are apprised of AML/CFT issues particularly those that have significant impact on their business operations to adequately provide guidance and direction.
- 3.2.3.14. *Availability and Access to Beneficial Ownership Information – Medium.* TEs are required to identify beneficial owners to ensure that beneficial owners' information are updated based on risk and materiality, and to include beneficial owners in their risk-based customer updating process. Beneficiaries of trust are obtained by TEs upon onboarding. Moreover, TEs also rely on GIS in the identification of UBOs for legal persons. Other sources utilized include publicly available information and third-party commercial database, among others.
- 3.2.3.15. *Availability of Reliable Identification Infrastructure – High.* Like other BSFIs, TEs also rely on the ID provided by official government authorities and registration documents provided by the relevant government agencies in the identification of their clients. Verification, on the other hand, is normally done via search facility in the online database of the issuers. Also, as an additional validation procedure, TEs send out confirmation letter after account opening and conduct visitation of client's residences, among others. The ongoing implementation of the national ID will further streamline the customer identification and verification process.
- 3.2.3.16. *Effectiveness of Supervision Procedures and Practices – High.* The supervisory framework, scope, risk prioritization, and risk rating system used for banks are also applied to TEs, with due regard to their operations and risk profile. BSP also engages in proactive dialogue with BOD, SM and other stakeholders of TEs thru trainings and meetings to discuss issues and concerns of the stakeholders.

PRODUCTS AND SERVICES VULNERABILITY

3.2.3.17. Among the trust products assessed, agency accounts, particularly IMA, pose the highest vulnerability at medium level. This was closely followed by UITFs, also at medium level. Other fiduciary services pose low level of ML/TF/PF risks. After considering AML/CFT controls in place, product vulnerabilities remain the same given the warranted improvements on the quality of compliance and certain specific controls, particularly on ST monitoring.

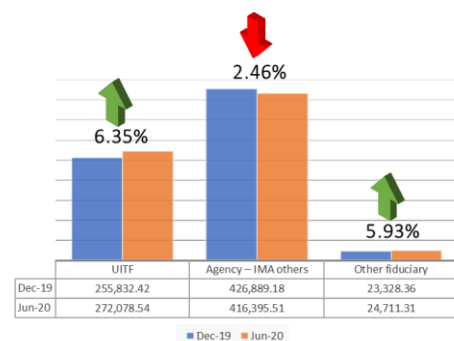


AGENCY IMA and UITF - Medium

3.2.3.18. IMA has high assets and transaction size. Minimum placement is at PhP100 thousand (previously at PhP1 million)⁷⁴. There are also high-risk clients such as NGOs and offshore companies. These clients account for at least PhP34.6 billion funds (3.22 percent of AUM). Further, the directional feature of IMA allows certain clients to instruct placement of funds which can be exploited by criminals for ML/TF activities.

3.2.3.19. Meanwhile, UITF recorded increasing volume and value for the covered period. Significant growth of PhP16.25 billion (6.35 percent) for the first half of 2020 was posted as shown in Figure 15. Further, there are some high-risk clients, which account for PhP16.50 billion or 1.54 percent of the total UITF portfolio. These include MSBs, NGOs, high net worth individuals, clients with adverse news, customers from high-risk jurisdictions, offshore companies, among others. The pooling of funds feature for settlement puts layers in the transaction to obscure the identity of ultimate customers. Moreover, there is a noted shift to new delivery channels (i.e., partnership with Non-Bank EMLs, and use of mobile application) which will widen coverage and market reach of UITF products.

Figure 15. UITF Growth



3.2.3.20. Meanwhile, the mitigating factors that reduced the vulnerabilities of these products to ML/TF/PF include: (i) generally acceptable AML/CFT/CPF controls; (ii) easy traceability of documents and transactions; (iii) settlement

⁷⁴ The minimum placement of PhP1 million was reduced to PhP100 thousand under Circular 1109 dated 04 February 2021.

of transactions coursed through depository bank; and (iv) low frequency of international transactions.

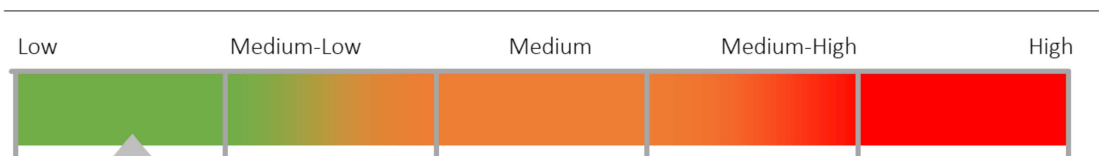
OFS – Low

3.2.3.21. OFS is assessed as *low*. Client profile is considered low given that arrangements/transactions are generally required by law or prescribed by the court⁷⁵ for purposes of preserving the funds/property for the benefit of both parties. OFS involves extensive documentary requirements which require personal interactions. Pertinent AML/CFT controls are in place.

OTHER ASPECTS OF LEGAL ARRANGEMENTS

3.2.3.22. The BSP, as a matter of policy, does not exercise supervision and oversight to non-BSP registered persons and individuals, including company service providers (CSPs) that perform isolated⁷⁶ trust activities. Based on the survey⁷⁷ of CSPs conducted by the BSP, they do not render services relating to legal arrangements. Meanwhile, the 2019 annual report of the BIR indicated that there are 4,028 registered trust taxpayers. This can be a starting point in taking stock of all legal arrangements in the country to inform policy and supervisory strategies and future risk assessments.

3.2.4. PAWNSHOPS



3.2.4.1. A pawnshop refers to a person or entity engaged in the business of lending money against a personal property delivered as a security for loans. It is synonymous and used interchangeably with pawnbroker or pawn brokerage. Filipinos consider pawnshops as an alternative means or even last resort to obtain credit by pawning their personal properties that are physically delivered to the control and possession of the pawnshop operator as loan collateral. It is a popular mode to tap immediate liquidity especially in cases of unforeseen need of the unbanked and underserved sector or those located in areas not served by the banks.

⁷⁵ Such as in cases of conflicting inheritance claims; judicial settlement of estate

⁷⁶ An isolated or single transaction conducted by trustee, CSPs or law firms is not considered a trust business within the contemplation of RA 8791. However, if there be a repetition or conduct thereof in a regular manner, they may be considered as engaging in business trust. A CSP, lawyer, or accountant that is designated as a trustee in an isolated trust transaction is classified as a DNFBP and is under the supervision of AMLC.

⁷⁷ 4 out of 9 CSPs responded to the survey

- 3.2.4.2. Over time, pawnshops became a major financial service access point to reach the financially unserved and underserved Filipino households and businesses. The pawnshop industry has evolved beyond traditional operations as a number of industry players engaged in corollary activities such as remittance (both domestic and international) and FX dealing/money changing. Other services offered by some pawnshops include bills payment and micro-insurance, among others.
- 3.2.4.3. The scope of this SRA covers pawning activity only. The MSB of pawnshops as corollary activity is covered under the MSB industry risk assessment.
- 3.2.4.4. *Overall vulnerability of the pawnshop sector is low.* Pawnshop operations are generally not attractive for ML activities, primarily due to low transactional amounts involved and the required face-to-face contact. General controls on AML/CFT/CPF are high.

ASSESSMENT OF CONTROLS

- 3.2.4.5. *Comprehensiveness of AML Legal Framework – High.* Pawnshop, as a BSFI, is a CP under Section 1, Rule 4 of the IRR of the AMLA, as amended. Sections 501-P and 922-Q of the MORNBFi provide the AML regulations and reporting requirements, respectively, for pawnshops. Moreover, BSP Circular No. 1039 dated 3 May 2019 was issued to amend pertinent provisions of the MORNBFi relative to the MSB corollary activity of pawnshops in accrediting their RSA, including certain conditions and supervisory expectations to be observed before they can accredit RSAs.
- 3.2.4.6. *Availability and Enforcement of Administrative Sanctions – High.* Sections 002-P and 701-P of the MORNBFi provide penalties and sanctions on violations of pawnshops to relevant rules and regulations. Any violation of the provisions of the regulations shall be subject to the administrative penalties under Section 37 of R.A. No. 7653, as amended, and implemented under Section 002-P, in relation to P.D. No. 114, otherwise known as the Pawnshop Regulation Act. Any administrative sanctions imposed by the BSP shall be without prejudice to the imposition of penalties under Section 18 of P.D. No. 114 and other applicable laws against the pawnshop, its proprietor, partners, directors, stockholders, president, officers and/or employees.

Administrative sanctions imposed by the BSP to erring pawnshops include cancellation/revocation of registration, issuance of directives and stern warning, requirement to execute an LOC, and imposition of monetary penalties. On the other hand, pawnshops also impose written warning/reprimand and suspension on their personnel for non-compliance with AML/CFT requirements/obligations.

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE

 3/19/21
JOSE MICHAEL E. CAMACHO

Bank Officer II, RMD
Administrative Services Department

3.2.4.7. *Availability and Effectiveness of Entry Controls – High.* Pursuant to Section 103-P of MORNBF, in considering the application to operate a pawnshop business, the BSP takes into account the fitness and propriety of the pawnshop operator and/or its incorporators, directors, partners, officers, financial capacity and ability to manage funds, operational capacity, reliability and efficiency of the system, and compliance with consumer protection and AML/CFT regulations, among others.

To further improve the licensing process for pawnshops, the BSP introduced series of enhancements, with the latest version published in BSP's 2020 Citizen's Charter and posted in the BSP website for public information in July 2020. A more thorough three-stage licensing process was introduced. The updates made in the Citizen's Charter ensure transparency, accountability and efficiency of the licensing process.

3.2.4.8. *Integrity of Entity's Staff – High.* Pawnshops have screening and recruitment process (i.e., conduct of background investigation prior to hiring) commensurate to their operations, to ensure that only qualified personnel are employed to assume sensitive functions. Others have adopted whistle blowing policy to encourage their employees to report irregular activities involving personnel without fear of reprisal.

3.2.4.9. *Effectiveness of Suspicious Activity Monitoring and Reporting – Medium.* Pawnshops' suspicious transactions reporting process is developing. Common weaknesses noted in monitoring system for flagging and reporting of suspicious transactions are mostly linked to pawnshops' MSB corollary activities. These affect the overall effectiveness of the suspicious activity monitoring and reporting.

3.2.4.10. *AML Knowledge of Entity's Staff – Medium.* Pursuant to Section 103-P of the MORNBF, as a pre-requisite for the issuance by the BSP of the Authority to Operate, the proprietor/partners/directors shall attend a seminar on AMLA, as amended, conducted by the BSP or the AMLC, or their accredited service providers⁷⁸. All pawnshops personnel are also required to undergo basic in-house AML training prior to performing their functions. Recent survey conducted by BSP showed that a total of 35,096 employees were able to attend AML trainings for the period covered. Although the COVID-19 pandemic disrupted the conduct of AML seminars for BSFIs in 2020, pawnshop applicants still comply with the required AMLA seminar by attending on-line seminars from training providers duly accredited by the AMLC. Meanwhile, although personnel have attended the required AML seminar, AML regulations and policies embodied in the pawnshops' MTPP

⁷⁸ Refers to an entity which has an adequate track record of successfully conducting training programs preferably on financial institution-oriented courses, including AML/CFT training.

are yet to be effectively implemented. Formal AML training program/ refresher courses, after the attendance to the required seminar, are yet to be established.

- 3.2.4.11. *Effectiveness of Compliance Function – Medium.* Large pawnshops, with nationwide operations and engaged in MSB as corollary activity, have compliance system in place with a full-time compliance officer. Adequate compliance staff, compliance program and regular compliance review and testing make their compliance function effective. Further, as pawning is the core business of the pawnshops, their understanding of the risks associated thereto is considerably high. The simple activity and transparency in the pawning operations make it less attractive to ML. Pawnshops also comply with AML rules and regulations relative to their pawning transactions. Scope for enhancements on implementation of appropriate CDD measures and risk profiling, on-going monitoring, and covered and suspicious transaction reporting mainly relate to their corollary business.
- 3.2.4.12. *Corporate Governance – Medium.* The organizational structure of pawnshops is relatively simple and clearly shows the relationship and reporting lines from staff level to the owners/board of directors. Larger and more complex pawnshops have board-level committees responsible for the conduct of IRA and ensuring appropriate mitigating controls are in place for the identified risks.
- 3.2.4.13. *Availability and Access to Beneficial Ownership Information – High.* Pawning clients are individual customers who are required to deliver the personal properties they own as loan collaterals. Hence, beneficial owner of the pawned item is identified.
- 3.2.4.14. *Availability of Reliable Identification Infrastructure – High.* The identity of customer is being established based on existing acceptable valid IDs (i.e., government issued IDs) subject to validation/verification of the information stated therein. This requirement will be further enhanced upon full implementation of the national ID, which aims to provide for a valid proof of identity for all Filipino citizens and resident aliens as a means of simplifying public and private transactions.
- 3.2.4.15. *Effectiveness of Supervision Procedures and Practices – High.* The BSP adopted a network-based examination, focusing on networks that are systematically connected rather than on an individual basis to ensure a more cohesive and effective supervision of the pawnshop industry. Supervisory strategy for pawnshops focuses on risk-based supervision for AML/CFT, among others.

3.2.4.16. ML/TF risks for pawning operations of pawnshops are assessed as low as their operations are generally not attractive for criminal activities. This is due primarily to low transactional amounts involved, wherein 66 percent were valued at PhP5,000 and below⁷⁹. Likewise, total size of the industry accounts only for 0.3 percent of the total loans and advances granted by the PBS⁸⁰ as of 31 December 2019. Owners of pawned items are identified and subjected to CDD requirements. Controls for on-boarding of clients as well as monitoring of their transactions are in place. Typical clients belong to the underbanked or unbanked sector (i.e., low to middle income class with no or limited access to other financial products and services). Pawning does not involve cross-border transactions. Moreover, there were only 17 STRs filed within the first half of 2020 involving pawnshop transactions from 2013 to 2019. Nevertheless, ML/TF risk may arise when stolen goods are pawned or clients fail to present proof of ownership or use illicit funds to repay the obligation or purchase at auctions.

3.2.5. NON-STOCK SAVINGS AND LOANS ASSOCIATIONS



3.2.5.1. NSSLA is an NBFI formed by individuals belonging to a certain well-defined group. It is regulated by the BSP and therefore considered as CP under the AMLA, as amended. NSSLA's business transactions are generally simple and the menu of financial products is limited to traditional investments and loans. Its customers are also members who are mostly employees of private company/conglomerate or department/branch/office of the government. NSSLAs are prohibited to solicit deposits or conduct business with the general public. The objective to sustain the profitable operations amid increasing resources has pushed some NSSLAs to widen the range of their existing products and services. Technological innovations are also being embraced by the NSSLA industry to expand its coverage as well as facilitate faster and more efficient delivery of its services.

3.2.5.2. The ML/TF/PF risks of NSSLA⁸¹ sector are assessed as *medium*. This sector provides limited financial products such as capital contributions, deposits

⁷⁹ Based on recent BSP survey on the composition of pledge loans in terms of value and volume of transactions

⁸⁰ <https://www.bsp.gov.ph/SitePages/Statistics/BSSelectedPerformanceIndicators.aspx>

⁸¹ R.A. No. 8367, Section 3 – NSSLA shall mean a non-stock, non-profit corporation engaged in the business of accumulating the savings of its members and using such accumulations for loans to members to service the needs of households by providing long term financing for home building and development and for personal finance

and loans to its members within a well-defined group⁸². Despite the simple and traditional products, the presence of significant number of members considered as PEPs resulted in medium inherent risk. Meanwhile, the comprehensive AML/CFT/CPF legal and regulatory framework coupled with effective risk-based supervision, balance the deficiencies in controls and compliance culture. Thus, quality of general controls is assessed as *medium*.

ASSESSMENT OF CONTROLS

3.2.5.3. *Comprehensive AML Legal Framework – High.* Under R.A. No. 8367, otherwise known as the Revised NSSL Act of 1997, the BSP was granted the power to enforce the laws, orders, instructions, rules and regulations approved by the MB applicable to NSSLAs. Accordingly, NSSLAs are considered CPs under the AMLA, as amended.

3.2.5.4. *Availability and Enforcement of Administrative Sanctions – Medium.* Sections 002-S (*Supervisory Enforcement Policy*), 003-S (*PCA Framework*), 324-S (*Sanctions on Loans/Credit Accommodations to Trustee and Officers*) and 703-S (*Enforcement Actions on BSP Regulations on Financial Consumer Protection*) of the MORNBFI provide penalties and sanctions on violations of NSSLAs to relevant rules and regulations. Pursuant to said supervisory enforcement policy, the three main categories of enforcement action, which include (a) corrective actions, (b) sanctions, and (c) other supervisory actions, may be imposed singly or in combination with others. Corrective actions are enforcement actions intended to require the BSFI to address the underlying cause of supervisory issues, concerns and problems which may include BSP Directives and/or LOC. Sanctions that may be imposed on a BSFI and/or its directors and officers, as provided under existing laws, BSP rules and regulations, are subject to the prior approval and/or confirmation by the MB. Sanctions to individuals are without prejudice to the filing of separate civil or criminal actions against them, when appropriate. Furthermore, subject to prior MB approval, the BSP, when warranted, may deploy other supervisory actions such as: (a) initiation into the PCA Framework; (b) issuance of a CDO against the BSFI as well as its directors and officers; (c) conservatorship; and (d) revocation or suspension of NSSL license; and (e) prohibition from doing business in the Philippines.

3.2.5.5. *Availability and Effectiveness of Entry Controls – High.* Pursuant to R.A. No. 8367, NSSL shall secure license from the MB before it can register with the SEC and transact any type of business. The MB can deny an application if it

⁸² Consist of, but not be limited to, any of the following: 1) employees, officers, and directors of one company, including member-retirees; 2) government employees belonging to the same department/branch/office, including member-retirees; and 3) immediate members of the families (up to second degree of consanguinity or affinity) of those falling under 1 and 2.

finds that the NSSLA is being organized for any purpose other than to engage in the business of a legitimate NSSLA or that its financial program is unsound. The MB may likewise revoke or suspend its license for such period as it determines necessary when the NSSLA willfully violates rules or regulations. Meanwhile, the enactment of R.A. No. 11211 (An Act Amending R.A. No. 7653, otherwise known as the “New Central Bank Act”) in February 2019 made the grounds for receivership of banks applicable to NSSLAs.

- 3.2.5.6. *Integrity of Entity’s Staff – Medium-High.* The election/appointment of trustees and principal officers of NSSLAs is subject to evaluation of the BSP, wherein fitness and propriety for the positions are assessed. The BSP also monitors the continuous compliance of trustees and officers with the qualification requirements. To date, there have been no recorded cases yet wherein personnel of NSSLAs have been directly involved in ML/TF activities.
- 3.2.5.7. *Effectiveness of Suspicious Activity Monitoring and Reporting – Low.* NSSLAs have inadequate policies and controls on monitoring and reporting of suspicious transactions. Automated system to analyze and flag unusual transactions has not yet been put in place even by the top three complex⁸³ MUP NSSLAs despite having significant risk exposure to possible ML activities. Current practice of NSSLAs in identifying suspicious transactions is based solely on news reports and pending legal cases. This is considered inadequate as it does not facilitate prompt and complete detection of possible suspicious transactions. Thus, latest examinations of NSSLAs disclosed several possible suspicious transactions that have neither been flagged nor reported to the AMLC.
- 3.2.5.8. *AML Knowledge of Entity’s Staff – Low.* Despite the trainings attended by NSSLA trustees, officers and personnel, the quality of AML/CFT compliance has not substantially improved as evidenced by recurring violations and failure to comply with BSP directives.
- 3.2.5.9. *Effectiveness of Compliance Function (Organization) – Low.* Robust compliance culture has not been fully institutionalized in NSSLAs. Adequate resources are not provided to the Compliance Office to ensure its effectiveness. Several NSSLAs do not even have their own full-time Compliance Officer. Moreover, some NSSLAs even failed to register with the AMLC for covered and suspicious transaction reporting.

⁸³ NSSLAs are considered complex when their resources exceed PhP5 billion and having at least any one of the following characteristics: (i) with extensive membership base; (ii) with serious issue/s on “well defined group” requirement; or (iii) with non-conventional business model; Electronic monitoring and reporting system for AML/CFT is required for BSFIs that are classified as complex.

- 3.2.5.10. *Corporate Governance – Low.* Membership based on well-defined group in NSSLAs has limited the number of qualified potential candidates for the positions of trustees and/or officers. In addition, board oversight over operations of NSSLAs is inadequate as most of the trustees are also working full-time either in government agencies or private corporations.
- 3.2.5.11. *Availability and Access to Beneficial Ownership Information – Low.* The following may hamper the effective access and verification of beneficial ownership information for NSSLAs: (i) the revised NSSL Act has allowed extended membership to close relatives (up to second degree of consanguinity or affinity) of the members; (ii) multiple memberships in different NSSLAs; and (iii) inadequate implementation of CDD particularly in verifying sources of funds.
- 3.2.5.12. *Availability of a Reliable Identification Infrastructure – High.* The unique structure of NSSLAs provides a reliable means of verifying the identity of its customer-member. Information about the employment and personal details of most members can be accessed by the NSSLAs directly from their mother companies. However, this may not hold true for extended or special membership such as the relatives of the members including those outside the well-defined group.
- 3.2.5.13. *Effectiveness of Supervision Procedures and Practices – High.* The BSP adopts a dynamic supervisory approach in the exercise of its mandate to regulate the operations of NSSLAs taking into account the accelerated growth rate and fast evolving environment affecting their risk profile. Specifically, the risk-based supervision has been adopted in drafting of examination program wherein priority is given to NSSLAs: (i) under PCA and LOC status; and (ii) categorized as complex and “deemed complex” with major supervisory issues.
- 3.2.5.14. *Availability and Enforcement of Administrative Sanctions (Implementation) – Medium.* With noted prevalence and persistence of AML supervisory issues in some NSSLAs, the use of appropriate and consistent enforcement actions, together with major policy reforms, serve as an important channel in improving the NSSLAs’ behavior as these promote greater discipline and responsiveness within the industry. The BSP’s deployment of timely enforcement action is crucial to avert development of issues into a serious weakness or problem that may threaten the soundness of NSSLAs. Between 2017 and 2018, some of the escalated supervisory sanctions include imposition of monetary penalties for willful refusal to permit examination, and revocation of licenses to operate as NSSLAs.

PRODUCT VULNERABILITY

| Factors | Vulnerability |
|-------------------------------------|---------------|
| Products and Services Offered | Low |
| Capital Contribution (Equity) | Low |
| Deposits | Medium |
| Loans | Low |
| Customer Profile | High |
| Geographic Location | Medium |
| Delivery Channels/Servicing Methods | Low |

3.2.5.15. Investing in NSSLAs has been attractive as members get higher rate of return compared to other financial institutions such as banks. Funds are also subject to lesser scrutiny and monitoring thereby making it susceptible to abuse and misuse. Over the years, the business model, operations, and financial structure of an NSSLA remain within the context of “savings” and “loan” wherein capital contributions and deposits of members are used primarily to finance its lending operations. Capital contributions, ranging from PhP1 thousand to PhP5 million for some of the top NSSLAs, allow members to share above market rate of returns depending on the performance of the NSSLA. Given the features and circumstances surrounding capital contribution, exposure to ML/TF risk is considered low. Nonetheless, ML risk for capital contributions account cannot be totally disregarded particularly in MUP NSSLAs where quite a number of members are tagged or classified as PEPs. Meanwhile, some NSSLAs accept traditional deposits (i.e., savings and time) as additional source of funds. Considering that the amount of deposits that members can place is generally not subject to ceiling and confidentiality of deposit accounts is protected under Section 6 of R.A. No. 8367 (NSSLA Law), as amended, ML/TF risk for deposit products is *medium*. On the other hand, NSSLA lending operations are centered on granting consumption loans that are anchored on the future compensation of the borrowing members in their mother companies. Among the main three products and services offered by NSSLAs, loans have the lowest vulnerability to ML/TF activities. Loans granted by NSSLAs are mainly for consumptions and other financial requirements of the borrowing members.

3.2.5.16. NSSLAs have been dominated by MUP, owning 86.8 percent of the industry’s total resources of PhP 260.2 billion as of end-2019. It is the main force behind the tremendous growth of the industry for the past several years. Incidentally, the MUP NSSLAs are also the most susceptible to ML/TF as they deal with a large number of members that are classified as PEP. Due to link of NSSLAs in the military as well as other branches of the government, it provides services to a significant number of PEPs particularly the acceptance of deposits and capital. In terms of geographical location, more than 80 percent of the NSSLAs’ head offices are located in the NCR. Nevertheless, memberships are spread all over the country including in four

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE

3/19/21

JOSE MICHAEL E. CAMACHO

Bank Officer II, RMD

Administrative Services Department

Page | 60

high-risk regions⁸⁴ known for having strong armed groups. NSSLAs have also members that are currently residing or stationed outside the country, 15 (less than 1 percent of the total 1.63 million members) of which are in several high-risk jurisdictions. Meanwhile, transactions of members are still mostly facilitated in a traditional manner (i.e., over the counter). NSSLAs usually have agreements with their mother companies for the automatic collections of loan payments, capital contributions and deposits from the monthly salaries and other benefits due to the members.

3.2.6. OPERATORS OF PAYMENT SYSTEMS

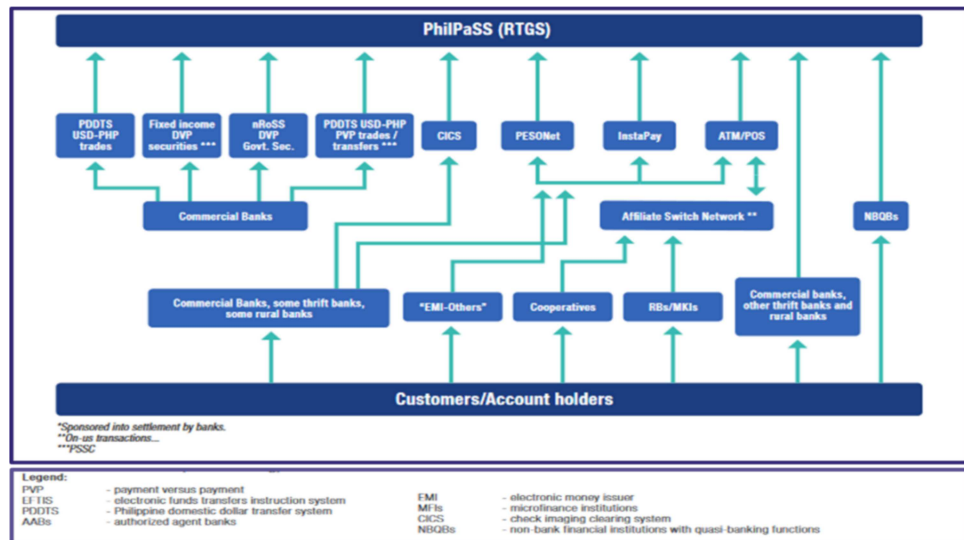
| Categories of OPS | ML/TF/PF Risk |
|--------------------------------|---------------|
| Operator of the RTGS System | Low |
| Cash-in System Provider | Low |
| CSO | Low |
| NPP | Low |
| Merchant Acquirer | Low |
| ASN | Low |
| Payment Gateway | Low |
| IAD | Medium |
| Platform Provider | Low |
| Bills Payment Service Provider | Low |

RISK ASSESSMENT PER OPS CATEGORY

3.2.6.1. *Operator of the RTGS System.* RTGS system is a large-value payment system that enables the transfer of funds between banks and other financial institutions. PhilPaSS is the RTGS system owned and operated by the BSP, with banks and selected NBFIs with quasi-banking functions as direct participants. It provides real-time settlement services in local currency for BSFIs. BSFIs send payment instructions via PhilPaSS and settlement is made through participants' demand deposit accounts maintained with the BSP. The PhilPaSS also supports settlement of transactions of other third-party systems such as ACHs, check image clearing system and exchange-of-value systems.

⁸⁴ Regions V (Bicol), XI (Davao), XIII (CARAGA), and the Autonomous Region of Muslim Mindanao

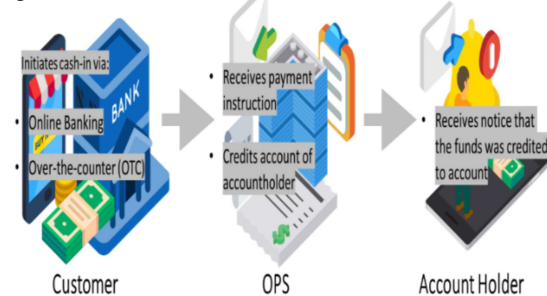
Figure 16. RTGS System



3.2.6.2. ML/TF/PF risk is low since participants of the system are mostly BSFIs that transact funds deposited with the BSP and subject to BSP rules and regulations including those on AML/CFT.

3.2.6.3. *Cash-in System Provider.* The cash-in system of OPS allows users to fund their wallet accounts by paying OPS in cash or its equivalent for the value to be stored in their wallets. Users may cash-in OTC through payment partners or via payment terminals/kiosks deployed in places such as building lobbies and malls. Users can also link their wallet accounts to other bank/EMI accounts or credit/debit cards. For OPS with closed-loop B2B wallets used for settlement of bills payment transactions to the OPS' network of merchants or billers, these B2B wallets are funded through bank deposits. OPS under this category include the cash-in systems of banks and non-bank EMIs.

Figure 17. Cash-In Service

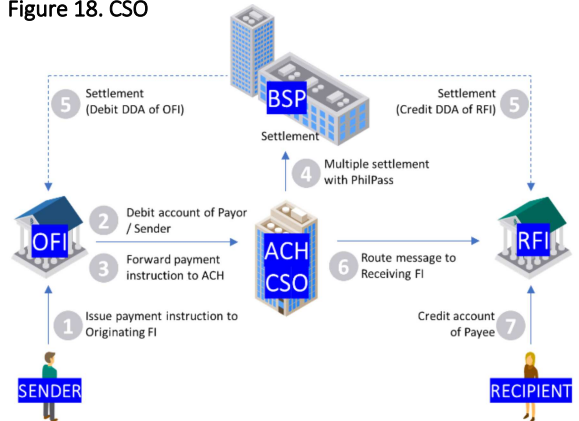


3.2.6.4. ML/TF/PF risk for this OPS category is low. Cash-in services through kiosks and OTC payments with payment partners and agents involve extensive use of cash. Transaction amounts vary depending on allowed services and transaction limits available to e-money accountholders, which are based on the level of CDD conducted on the accountholders. Existing regulation prescribes aggregate monthly load limit of PhP100,000 although EMIs may request for higher limits. Alternative modes are also available through mobile applications that allow linking of transactions to the user's bank/EMI

account, credit or debit card. Moreover, the funds in these wallets are not withdrawable in cash and can only be used for specific instances such as bills payment and usually function as mere ledger accounts in relation to the bills payment facility of the OPS.

3.2.6.5. **CSO.** The CSO is the system operator of the clearing system used by participants of an ACH. It provides clearing infrastructure for an ACH and i) performs netting of payment instructions received from participating institutions; ii) forwards net clearing positions to PhilPaSS based on agreed frequency under the ACH rules for direct settlement; and iii) generates clearing results, inward data files and reports, and makes the same available to the participants.

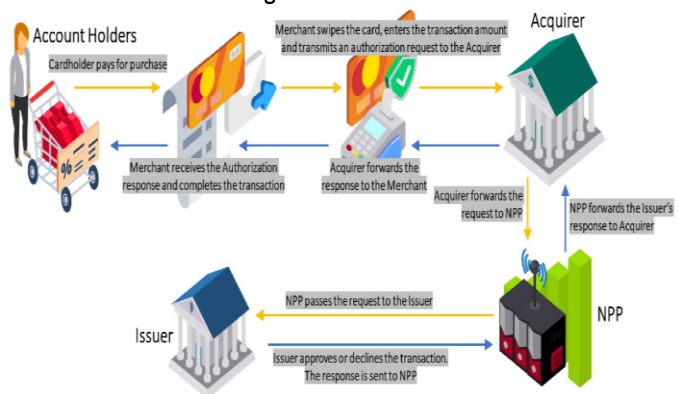
Figure 18. CSO



3.2.6.6. **ML/ TF/PF risk for CSO is low.** A CSO does not receive or hold funds but rather operates the system for clearing of payment instructions. The payment instructions processed by the CSO are from participating institutions of an ACH. Based on the criteria under the NRPS Framework, only banks and EMLs are eligible to become participants of ACHs whose fund transfer transactions are processed through the clearing infrastructure provided by the CSO.

3.2.6.7. **NPP.** The NPP processes, clears, and settles credit and debit card transactions. It provides a system or network infrastructure that facilitates the electronic exchange of information and funds among financial institutions, merchants, consumers and businesses. It administers the settlement between participants or member issuers and acquirers on an aggregate net settlement basis. This is done through a direct debit authority over the members' bank accounts. Where the transactions are made using cards issued in another country, the settlement accounts of the NPP in said country will be involved.

Figure 19. NPP

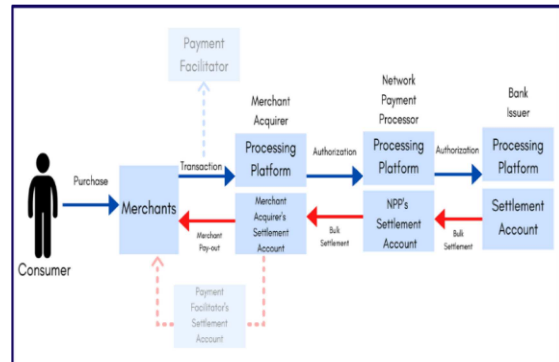


3.2.6.8. ML/TF/PF risk for NPP is low. NPP caters to its network members for the processing of credit card transactions. Funds in NPP transactions pertain only to settlement of the net payable positions of its members and are facilitated through automatic account debit and bank fund transfers.

3.2.6.9. *Merchant Acquirer.* Merchant

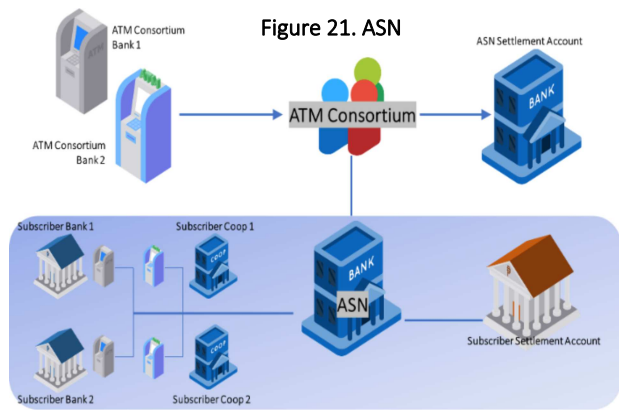
acquiring is the process through which merchants can accept electronic payments in exchange for goods and services from their customers. Merchant acquirers enable merchants to accept card payments acting as a link between merchants, the NPP and the issuers. It provides authorization, clearing, dispute management and information services to merchants. Some merchant acquirers also perform settlement services depending on the arrangement it has with its payment partners. In some arrangements, it is the merchant acquirer who settles directly with the merchants the amounts due to them from the issuing bank. For this purpose, the merchant acquirer maintains settlement accounts from which the funds due to the merchants are transferred to their accounts. Some arrangements involve a payment facilitator that acts as a mediator between the merchants and the merchant acquirer.

Figure 20. Merchant Acquirer



3.2.6.10. ML/TF/PF risk for this category is low. Clients of OPS providing acquiring and payment facilitator services are merchants of goods and services. These OPS handle funds that are settled in their favor by the NPP for settlement, in turn, of the amounts due to the merchants for authorized transactions processed by the NPP, through a settlement account. Depending on its business arrangements with the merchants, the acquirers and payment facilitators make final settlement with merchants either through bank transfer or check payment from the accounts they maintain in their settlement banks. As bank clients, they are subjected to CDD. Moreover, merchant acquirers generally employ accreditation process before onboarding merchants. There are also mechanisms in their agreement with the merchants that allow them to hold the settlement funds pending resolution of issues arising from consumer complaints, unusually high transactions or lack of proper bank documentation.

3.2.6.11. *ASN*. An ASN is an aggregator service provider that connects its ATM switch with an ATM consortium and extends that connection to its subscribers or members. The subscribers of the ASN, which consist of thrift, rural and cooperative banks and cooperatives, connect to the switch of the

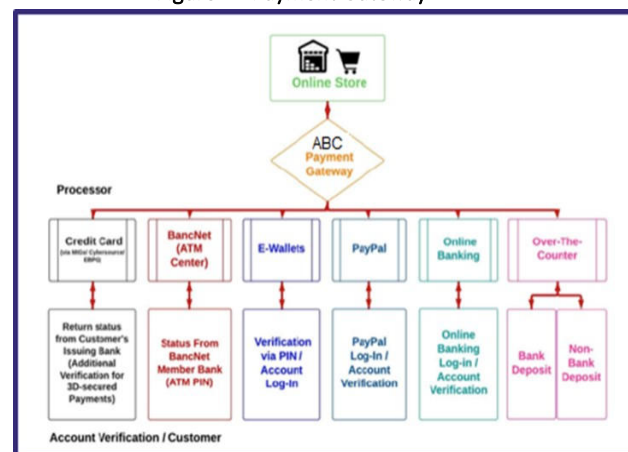


ASN with their own or outsourced switch. Settlement of funds by the ATM consortium to the ASN and by ASN to its subscribers is done through banks where the ASN and its subscribers maintain settlement accounts. ML/TF/PF risk for ASN is low. The services of an ASN to its subscriber members for switch connection involve only the settlement of the net payable positions of its members for issuing and/or acquirer transactions. Settlement is facilitated through bank fund transfers.

3.2.6.12. *Payment Gateway*.

A payment gateway, also known as *paygate*, is a vital component in processing electronic payments for merchants, connecting systems including POS terminals located in physical stores to accept payments such as cards or by mobile phones. Payment gateways allow

Figure 22 Payment Gateway



businesses/merchants to access the payment processor of their choice. A key function of a paygate is to facilitate the collection of customer's account information as well as other credentials and direct these data safely to the payment processor for the processing of payment transactions.

3.2.6.13. ML/TF/PF risk for paygate is low. Funds used for payment transactions originate from the customers' accounts (e.g., credit cards, debit cards, e-wallets and bank accounts) with financial institutions which have been subjected to CDD. Moreover, settlement process is done through the parties' respective bank accounts.

3.2.6.14. *IAD*. An IAD is a non-bank and/or non-financial entity that owns, manages, and places ATMs in retail premises such as convenience stores, airports, gasoline stations or in areas where ATMs deployed by banks are

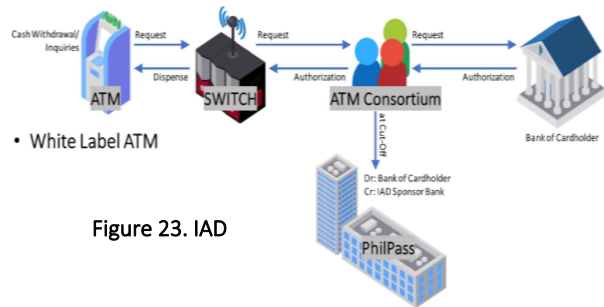


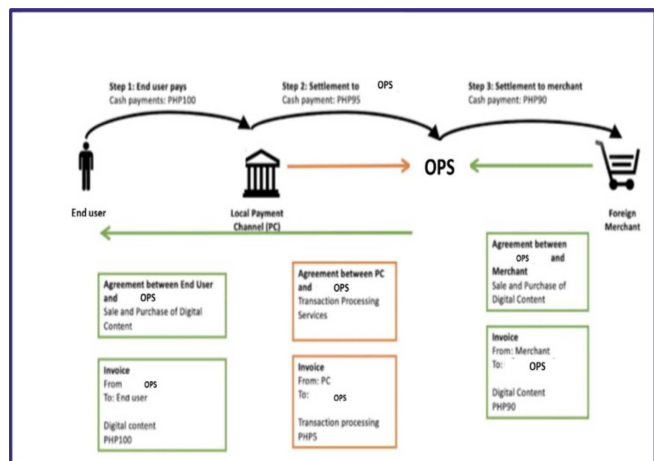
Figure 23. IAD

limited, including a system or network infrastructure that enables payments and other financial services. An IAD maintains a telecommunication link with an ATM consortium and enters into agreements with other international payment networks for the routing, authorization, and settlement of certain types of transactions such as cash withdrawal initiated by an ATM cardholder. Settlement of funds by the ATM consortium to IAD and IAD to cash provisioning bank is done through their accounts maintained with banks.

3.2.6.15. *ML/TF/PF risk for IAD is medium*. While cash provisioning services are typically performed by banks, an inherent vulnerability to this business model would be the possibility of the IAD entering into agreements for the supply of cash with non-bank entities that may be in possession of cash obtained from illegitimate activities. When this happens, illicit funds can now enter and become part of the formal financial system. However, safeguards can be employed to minimize ML risk such as requiring banks that engage IADs to conduct due diligence on these IADs prior to establishing relationships.

3.2.6.16. *Platform Provider*. A platform provider usually takes the form of a marketplace model in which merchants sell various consumer products on their platform. It creates value by connecting and facilitating exchanges usually between consumers/users and producers/merchants who do not have direct relationship. The platform

Figure 24. Platform Provider



provider may also handle the collection of payment and shipment of products of producers/merchants. The platform provider settles the payments directly to the merchants (e.g., digital publishers such as gaming

and streaming platforms) via its settlement accounts maintained with banks.

3.2.6.17. ML/TF/PF risk for platform provider is low. In the event that a platform provider also collects payments of products for a merchant/seller, it needs to enter into agreements with collection channels. Payments received by these collection channels are transferred to the platform provider through their bank accounts. The platform provider will then settle payments due to the merchants/sellers via their settlement accounts maintained with banks/EMIs.

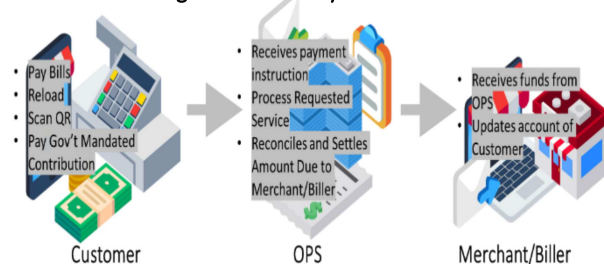
3.2.6.18. *Bills Payment*

Service Provider. A

bills payment service provider facilitates payment between a consumer/client and a direct biller/merchant specifically to accept a pre-determined payment

amount for and on behalf of the direct biller/ merchant from its consumer/client. A common example for this is a payment center where consumers/clients can pay their bills. Other bills payment service providers include i) authorized agent banks that act as collecting agent of government and non-government direct billers that accept payments on behalf of the said entity; ii) loan collection facilities that have written agreement with another entity (i.e., direct biller) particularly to collect loan payments on latter's behalf; and iii) top-up system providers that allow direct integration of its payment system/platform with a direct billers' website or existing system to accept bills payment.

Figure 25. Bills Payment



3.2.6.19. ML/TF/PF for this OPS category is low. Bills payment service providers accept payments on behalf of direct billers only from customers with valid accounts. The amount that needs to be paid by the customers is pre-determined by the direct billers. Payments received shall then be deposited to the direct billers' designated accounts with banks. In spite of the availability of electronic options, cash payments via OTC/payment machines are still very much prevalent.

4 SPECIAL/FOCUS AREAS

4.1. TRADE-BASED MONEY LAUNDERING

4.1.1. TBML is defined as “the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illegal origin or finance their activities.”⁸⁵ TBML is an emerging higher risk area for the Philippines. This was driven by several factors such as the growing trend of international trade, the inherently complex and complicated trade processes, and the geographical landscape and vast maritime borders and sea ports. These create an opportunity for criminal groups and TF networks to exploit the trade and related financial flows in the Philippines to facilitate a range of illicit financial flows, including laundering the proceeds of crime, enabling the movement of TF and PF or supporting sanctions evasion.

4.1.2. *The net trade-based ML/TF/PF risk associated with the banking sector is medium.* The threat posed by trade-based ML/TF/PF on banks is *high*. This



can be attributed to the prevalence of deliberate trade mis-invoicing in the Philippines⁸⁶, complexity and variety of trade-based ML/TF/PF schemes and techniques, intricacies in investigating and prosecuting ML activity of associated crimes such as smuggling, drug trafficking and financing of terrorism, coupled with the geographical landscape of the country that pose challenges in border management and controls. In this regard, mitigating measures are in place such as AML/CFT and FX rules and regulations, as well as general controls and risk management framework on banks’ trade finance facility.

4.1.3. *The net trade-based ML/TF/PF risk associated with the MSB sector is medium.* Based on available data, trade-based ML/TF/PF threat for



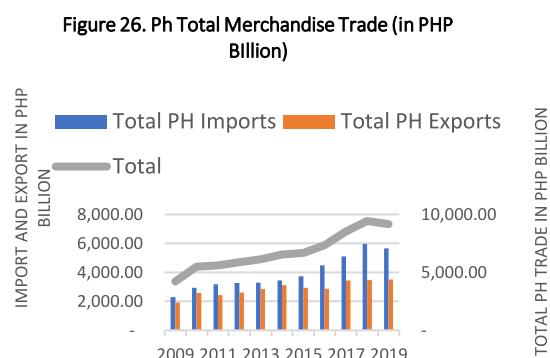
MSBs is *medium*. MSBs have minimal share on the recorded facilitation of trade payments. Nonetheless, there is a need to further enhance data collection on this aspect to inform future assessments. Subsisting issues of MSBs on ML/TF risk management framework make it highly vulnerable to ML/TF/PF.

⁸⁵ 2006 FAFT definition as re-affirmed in the Trade-Based Money Laundering Report: 2020 Update

⁸⁶ <https://secureservercdn.net/45.40.149.159/34n.8bd.myftpupload.com/wp-content/uploads/2020/03/GFI-Trade-IFF-Report-2020-Final.pdf?time=1603280556>

TRADE ENVIRONMENT

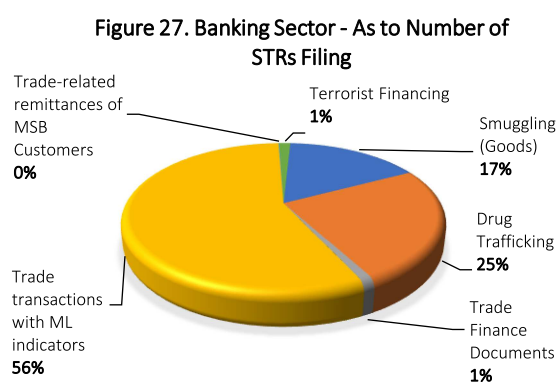
4.1.4. In the 2020 World Trade Statistical Review Report, the Philippines, which ranked 39th (from 52nd), is one of the countries which rose the most in world rankings for merchandise trade over the past ten years (2009 to 2019) (Figure 26)⁸⁷. Main imports originated from China (22.90 percent) and Japan (9.60 percent), while main export destinations included United States of America (16.30 percent) and Japan (15.10 percent)⁸⁸.



Total imports aggregating PhP17.98 trillion (60.24 percent) exceeded total exports aggregating PhP11.87 trillion (39.76 percent) from 2017 up to 1st half of 2020⁸⁹. The mode of payment⁹⁰ for trade transactions varies, depending on the existing relationship between the exporter (seller) and the importer (buyer) as well as the terms and conditions of the sale. Available data⁹¹ indicates that banks are the more preferred channels for trade payments, which facilitated an estimated amount of PhP18.45 trillion.

TRADE-BASED ML/TF/PF THREAT

4.1.5. *The trade-based ML/TF/PF threat to the banking sector is high.* STRs related to trade-based ML/TF/PF (Figure 27)⁹² primarily involved *trade transactions with ML indicators* (56.29 percent). These were transactions of customers with declared business of trading/freight brokerage/



⁸⁷ https://www.wto.org/english/res_e/statis_e/wts2020_e/wts2020_e.pdf; FX rate of USD1=PhP50.00 is used.

⁸⁸ https://www.wto.org/english/res_e/statis_e/daily_update_e/trade_profiles/PH_e.pdf

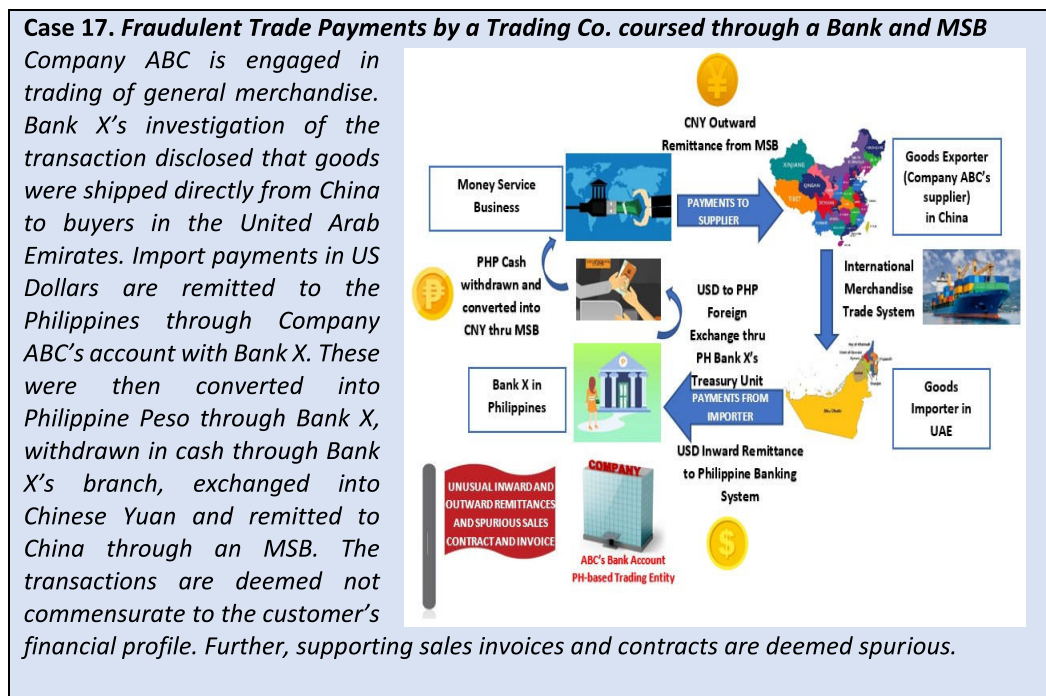
⁸⁹ DTI/PSA Trade statistics (2017 up to 1st half of 2020) <http://tradelinephilippines.dti.gov.ph/> and/or <https://psa.gov.ph/statistics/foreign-trade>; For presentation purposes, FX rate of USD1=PhP50.00 is used.

⁹⁰ Modes of payment for Imports and Exports are discussed under Chapter II (Foreign Merchandise Trade Transactions) of the MORFXT

⁹¹ Data sources: AMLC, DTI, PSA, BSP, Respondent Banks to BSP survey via APCB

⁹² Based on analysis of 30,821 sample STRs. Sampling is applied for analytical purposes as trade-based ML/TF/PF STRs can involve different transactions codes and/or predicate crimes. Most of the STRs are filed under ZSTR code with nil amount.

shipping but were unable to provide supporting trade documents, or with transactions and/or counterparties that are not commensurate and/or inconsistent with their declared business. STRs indicating the *use of fraudulent trade finance documents or sanctions/internal database hits* involved significant transaction values, with 317 instances amounting to PhP4.67 trillion (98.10 percent of the total value of trade-based related STRs). Meanwhile, STRs involving import payments for clients of banks' MSB customers, being coursed through the banks' outward remittance facilities, present high trade-based ML/TF/PF threat, as the foreign correspondent bank had identified certain beneficiaries of import payments as shell companies. These STRs were driven by both customer-level monitoring via negative news or sanction screening and bank-wide transaction monitoring.



4.1.6. *Drug trafficking and smuggling (goods) are the top predicate crimes exploiting trade transactions.* STR analysis revealed that the use of cash in TBML is prevalent, which were mostly represented as proceeds of sale of merchandise or payments related to importation of goods. TBML is often combined with the use of shell or front companies and BMPE⁹³. In 2017, AMLC⁹⁴ had identified three (3) case typologies where the laundering of drug proceeds utilized bank accounts of merchandise trade businesses, as front companies, in receiving remittances, exchanging foreign currencies, transferring funds, and settling

⁹³ Based on FATF definition, its central feature includes the use of a money trader and their associates, facilitating the transfer of drugs cash into pesos. These money traders use the drugs money to purchase legitimate commodities from businesses.

⁹⁴ Based on AMLC Risk Information Sharing and Typologies and AMLC 2017-2018 AMLC Annual Report

invoices related to the trade flows, with estimated criminal proceeds of PhP968.60 million. According to the AMLC report⁹⁵:

“The modus operandi involves Filipino nationals (“the front”), who register sole proprietorship retail businesses with the DTI on behalf of certain foreign nationals, who are the actual and UBOs of the said businesses. These businesses are under the complete control and operation of these foreign nationals. After registration with the DTI, the front goes to the bank (mostly commercial and universal banks) with the newly acquired DTI registration permit to open an account in the name of the newly-registered business. The said bank account will then be managed and controlled by the foreign nationals—the UBOs—for the purpose of receiving funds from illegal proceeds. Moreover, majority of the registered sole proprietary businesses, as identified in this modus operandi, are discovered to be “shell companies” or inexistent companies.”

Case 18: Use of a Trading Co. as Front in TBML Activity Related to Drug Trafficking

Company GHI, a registered trading entity, is a new customer of Bank Z. Company GHI issued checks with significant amounts to several individuals and entities with no established purpose. Also, Company GHI had several transactions with an individual linked to drug trafficking. Meanwhile, Company X, a foreign trading entity in Country Y, remits funds to Company GHI. It appears that Company X had transactions with two (2) trading companies which are also customers of Bank Z. These two (2) trading companies made several fund transfers to individuals and entities linked to a drug trafficking personality.



Case 19: Use of Cash to Place Illicit Proceeds from Outright Smuggling⁹⁶ in a Bank.



Customer A has an account with Bank Y since 2012. He declared that he is the owner/manager of Company DEF, an entity engaged in shipping business. He was known by the branch as engaging in rice importation and distribution. In October 2017, the customer had two (2) high value inter-branch cash deposits aggregating to PhP7.45 million. The customer was unable to provide supporting documents to establish the transactions' underlying legal or trade obligation. He explained that these were payments for rice shipments but the importation process did not go through the normal channel, including customs duties and tax payments.

⁹⁵ AMLC Risk Information Sharing and Typologies

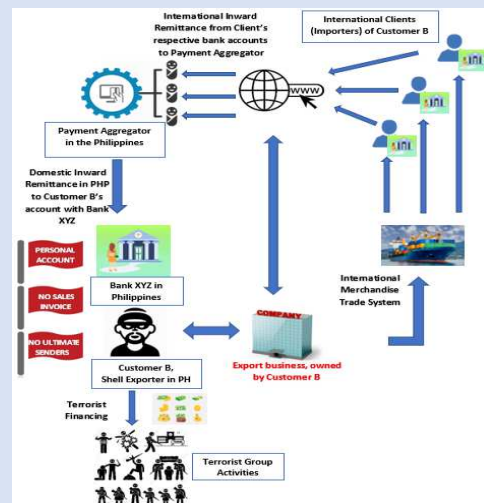
(<http://www.amlc.gov.ph/images/PDFs/2020%20AUG%20AMLC%20RISK%20INFORMATION%20SHARING%20AND%20TYPOLOGIES%20ON%20DRUG%20TRAFFICKING.pdf>)

⁹⁶ Based on the 2019 SOCTA Report, there are two (2) modus operandi: (1) outright smuggling, which constitutes activities that aim to illegally transport products by avoiding legal transportation and customs procedures; and (2) technical smuggling, which is defined as illegally importing items through falsified paperwork and/or erroneous declaration of item particulars, particularly on its “nature, kind, quality, quantity or weight”.

4.1.7. *STR analysis revealed that trade transactions facilitated by banks are also being exploited for TF. TBTF is a form of terrorist financing that involves disguising of funds or other assets, whether from legitimate or illegitimate sources, through the use of trade transactions.*⁹⁷ Sample STRs disclosed 421 reports (1.37 percent) on suspected members/financiers of terrorist groups, who are being investigated for funding terrorist activities, and are engaged in trading businesses.

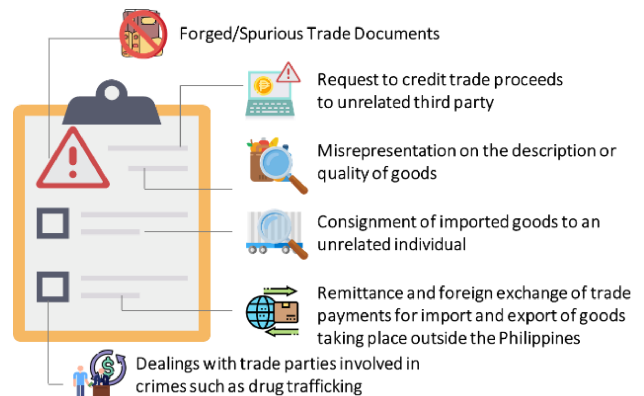
Case 20: Suspected Rebel Group Financier/Member Engaged in Dubious Trading Business to Fund Terrorist Activities, Coursed through Trade Payments

Customer B, an individual, opened an account with Bank XYZ in 2016. The declared source of funds is export business. As of 2018, there were more than 120 domestic inward remittances for around PhP9.20 million for the last 13 months. Bank XYZ verified these as proceeds from the sale of Customer B's exported shells to international clients, whose trade payments were coursed through a certain "Payment Aggregator". Customer B was unable to provide supporting documents, and failed to identify the ultimate source of the remittances. Investigation disclosed, among others, that customer was possibly involved in tax evasion and illegal trade of wildlife sources as well as secretly financing rebels in Mindanao.



4.1.8. *Red flag indicators.* There are various TBML typologies or techniques used by criminals and/or organizations. Figure 28 summarizes common trade-based ML/TF/PF methods or red flags identified by Philippine respondent banks and culled from STRs.

Figure 28. Red Flag Indicators



4.1.9. *The banking and MSB sectors' exposure to TBPF threat, as a result of Philippine's diplomatic and business relationships with DPRK and Iran*⁹⁸, is **low**. Total bilateral trade relations with DPRK and Iran were on a decreasing trend from 2017 up to 2020. In 2017, the Philippines suspended trade relations with DPRK to comply with a UNSC Resolution over its repeated

⁹⁷ FAFT definition under Trade-Based Money Laundering Report: 2020 Update

⁹⁸ Subject of UNSCR Sanctions on PF

missile tests.⁹⁹ There was no trade of potentially strategic goods with DPRK for the period January 2018 to August 2020. On the other hand, Iran has an aggregate USD2.38 million¹⁰⁰ import and export transactions which account for 0.0004 percent of the total merchandise trade of the Philippines. The past UN trade restrictions imposed on Iran led to a decline in Philippine trade transactions with Iran, particularly on banana shipments to that country¹⁰¹.

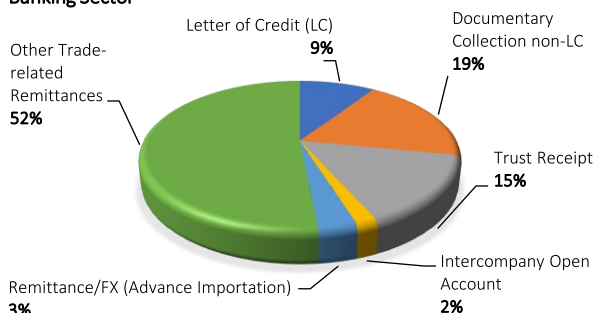
VULNERABILITIES OF THE BANKING AND MSB SECTORS TO TRADE-BASED ML/TF/PF

4.1.10. *The banking sector's vulnerability to trade-based ML/TF/PF risk is **medium**.*

Total estimated international trade transactions of PHP18.45 trillion being facilitated by banks for the covered period account for 99 percent of the total assets of the PBS as of 30 June 2020¹⁰². Trade financial solutions provided by banks facilitate the payment and shipment of physical goods around the world and/or provision of related guarantees and services. By their nature, trade activities, which involve cross-border transactions with various jurisdictions, are inherently complex and document-intensive. These are mostly manually processed and involve multiple parties that may likewise have complex ownership structures. Available information indicates that bulk of trade payments are mainly facilitated by UKBs in the Philippines.

- 4.1.11. As shown in Figure 29¹⁰³, 48 percent of these estimated trade payments are coursed through banks' trade finance products and services such as L/C, D/C and Trust Receipt. These are generally centralized in the Trade Operations Unit of banks, and allows for scrutiny of the proposed trade transactions. Servicing of the majority portion of trade payments (52 percent) through O/A, D/R, Advance Importation, or Self-funded/No-Dollar import arrangement varies depending on the banks' organizational structure, which can either be through branches, treasury, trade, or remittance units. In these cases, the service is more of facilitation of remittance/funds transfers wherein the evaluation and process of gathering of supporting documents vary. The depth of scrutiny is not as rigorous when the trade is facilitated through provision of credit or financing. Thus, these are more vulnerable to trade-based ML/TF/PF activities.

Figure 29. International Trade Products and Services - Banking Sector



⁹⁹ <https://www.reuters.com/article/us-philippines-northkorea-idUSKCN1BJ10K>

¹⁰⁰ Department of Economic Statistics, BSP. Transactions from 2017 up to February 2020.

¹⁰¹ <https://www.dof.gov.ph/philippines-iran-agree-to-expand-bilateral-relations/>

¹⁰² <https://www.bsp.gov.ph/Statistics/Financial%20Statements/Balance%20Sheet/3.aspx>

¹⁰³ Data sources: AMLC, BSP, Respondent Banks to BSP survey.

- 4.1.12. *ML/TF/PF risk controls.* The foregoing vulnerabilities to trade-based ML/TF/PF are mitigated by existing AML/CFT and FX rules and regulations governing banks in the Philippines. Generally, the ML/TF/PF risk management framework applied to banks' trade customers and transactions cover IRA, on-boarding due diligence, customer and transaction screening on sanctioned parties and/or high-risk jurisdictions, transaction monitoring, and red flag analysis and escalation process.
- 4.1.13. *Scope for enhancements.* There are pockets of areas warranting improvements given the challenges faced by the banks in detecting trade-based ML/TF/PF typologies or techniques. Detection mechanism of banks for trade-based ML/TF/PF-related suspicious transactions is still largely done manually. Screening of traded goods involved in the proliferation of WMD mostly rely on open-source searching tools or via in-house or third-party database. The lack of reliable references for price comparison between the "financial transactions" and "value of traded goods" primarily contributes to the increasing trade mis-invoicing risk in the Philippines as noted by the latest GFI Report¹⁰⁴. Likewise, there is a need to deepen technical knowledge given the complexity and decentralized processing of trade transactions. Finally, overall risk management system for TBML can be further enhanced to cover all products and services and/or banking units facilitating customers' trade transactions such as remittance and foreign exchange.
- 4.1.14. The trade-based *ML/TF/PF threat to the MSB sector is medium*. MSB sector has minimal share in the recorded facilitation of trade payments in the Philippines, estimated at PhP44.22 billion¹⁰⁵. Nonetheless, AMLC, in its report¹⁰⁶, had assessed that the illicit funding from smuggling were mostly coursed through MSBs from 2013 to 2017. Based on analysis of sampled 88 trade-related STs of the MSB sector, 96 percent pertains to unsupported inward remittance transactions of customers engaged in merchandise trade (import and export) business. The remaining 4 percent are connected to smuggling and drug trafficking based on negative news. MSB participation in trade-based ML/TF/PF activity is illustrated in Case 17.
- 4.1.15. Vulnerability of MSBs to trade-based ML/TF/PF risk is assessed as *high*. This is due to its involvement in AMLC investigations on TBML cases and subsisting

¹⁰⁴<https://secureservercdn.net/45.40.149.159/34n.8bd.myftpupload.com/wp-content/uploads/2020/03/GFI-Trade-IFF-Report-2020-Final.pdf?time=1603280556>

¹⁰⁵ AMLC – CTR and BSP-Department of Supervisory Analytics; Data collection on trade payments facilitated by MSBs can be further enhanced to inform future assessments

¹⁰⁶ Risk Assessment on the Philippine's Exposure to External Threats based on Submitted Suspicious Transaction Reports (STRs)(<http://www.amlc.gov.ph/images/PDFs/Study%20on%20External%20Threats%20Using%20STR%20Data%20from%202013%20-%202017.pdf>); Updated report as of 31 May 2019

issues on ML/TF risk management framework, particularly on customer identification, transaction monitoring and covered and suspicious transaction reporting systems. There is also room to enhance data collection on remittances relating to trade payments/transactions. Therefore, net risk of trade-based ML/TF/PF activities to the MSB sector is *medium*.

4.2. TARGETED FINANCIAL SANCTIONS ON TERRORISM, TERRORIST FINANCING AND PROLIFERATION FINANCING



4.2.1. *Net risk for TFS is assessed as Medium-High.*

4.2.2. *The threat posed by TF to the sector is high.* This is primarily driven by the high number of violent incidents associated with terror/threat organizations, who appear to have a systematic and established method of raising funds for their operations. The AMLC assessed threat of terrorism as high. Meanwhile, vulnerability of BSFIs to TF-related sanctions and its evasion is *medium* in view of the existing legal and institutional frameworks to implement TFS on TF. Further, control measures relating to key AML/CFT processes, such as CDD, sanctions screening system, and ongoing monitoring, are implemented to mitigate risk of them being used by designated persons, although there are areas for improvement.

4.2.3. *On the other hand, the threat posed by PF is low* in view of nil and minimal trade transactions with DPRK and Iran, respectively. Trade of strategic goods involve electronics and semi-conductors used by big technology firms while most of imported military goods are for the government. Vulnerability of BSFIs to PF-related sanctions and its evasion is *medium-high*. The understanding of the sector on PF is still developing while PF-related measures are progressing.

THREAT ASSESSMENT

4.2.4. *TFS on terrorism and TF.* Based on the AMLC's analysis of STRs, 61 percent of the transactions suspected to be associated with terrorism and TF from 2018 to 2020 were reported and coursed through MSBs and pawnshops while 29 percent were coursed through Banks. EMIs are also seen as potential channel for terrorism and TF funds, particularly in 2020 with the use of electronic cash cards. Accordingly, STR submissions by Banks and MSBs follow an increasing

trend, registering 194% and 489% average increase, respectively.¹⁰⁷ Thus, threat related risk of TFS on TF is assessed as *high*.

- 4.2.5. *TFS on PF*. PF threat to BSFIs is *low* due to minimal transactions/connections with DPRK and Iran, and minimal import and export of DUGs. TBPF threat has been on a decreasing trend from 2017 up to 31 August 2020. There were no trade of potentially strategic goods with DPRK from January 2018 to August 2020.
- 4.2.6. Trade dealings with Iran were minimal, representing negligible portion (less than 1 percent) of the total exports and imports of the country. These relate mostly to semi-conductors, metal furniture and other medical instruments. Exporters and importers of these goods are into solar manufacturing, woodcrafts and medical equipment distributors. Further, six-month data from AMLC on STR (Jan to June 2020) disclosed only 79 out of 388,717¹⁰⁸ total STRs, involving aggregate amount of Php25 million, are possibly related to PF.

Case 21: Bank A investigated a case related to PF. This refers to the account of ABC Corporation which was designated by the US OFAC in June 2019 for being owned or controlled by a sanctioned entity. Review of the account disclosed that transactions are of minimal amount only and the account has no activity since September 2017. The Bank subsequently closed the account in accordance with its policy.

VULNERABILITY ASSESSMENT

- 4.2.7. *Vulnerabilities of BSFIs on TFS on terrorism and TF*. Overall vulnerability of BSFIs to TF-related sanctions and its evasion is *medium*. There is appropriate legal framework to implement TFS. BSFIs have broadly recognized sanctions risk in their assessment of customers and products, and implemented sanctions risk management processes. Bespoke control measures in relevant processes, such as CDD, ongoing monitoring, and sanctions screening system, are implemented to mitigate risks. BSFIs maintain a database of UNSC Consolidated List and local designations, such as, among others, CPP/NPA also known as *Bagong Hukbong Bayan*, Islamic State in Iraq and Syria in South-East Asia, Dawlatul Islamiyah Waliyatul Masrik, Maute Group, Islamic State East Asia, Bangsamoro Islamic Freedom Fighters-Bungo, and other Daesh-affiliated groups in the Philippines. BSFIs also actively monitor news publication to update their watchlist database. In this regard, in coordination with the AMLC, BSFIs were able to freeze and report certain accounts based on target match. While BSFIs took immediate action to enhance their policies and procedures in relation to the Sanctions Guidelines, in-depth understanding of their TFS obligations should be developed and sustained given the complexity of TFS requirements. Likewise, there is scope for improvement in terms of

¹⁰⁷ AMLC 2021 Terrorism and Terrorism Financing Risk Assessment

¹⁰⁸ Source: AMLC

implementing transactional sanction screening particularly for non-accountholders or walk-in customers.

- 4.2.8. *Vulnerabilities of BSFIs on TFS on PF.* BSFIs vulnerability to TFS on PF is *medium-high*. The recent AMLA amendment authorizes the AMLC to implement TFS for PF, including issuance of freeze order. Meanwhile, risk mitigation measures for PF, commencing from risk assessment to transaction monitoring and identification of red flag indicators, are still developing. Few BSFIs have institutionalized concrete measures to mitigate PF risk. BSFIs have yet to consider assessing PF sanctions risk. Transaction monitoring and red flag indicators to identify PF activities are being developed/enhanced by most BSFIs. Enhancing training sessions to focus on TFS on PF is warranted to deepen understanding by BSFIs of their obligations to implement TFS.
- 4.2.9. In view thereof, the net risk arising from TFS in relation to terrorism, TF and PF is *medium-high*.

5 FINANCIAL INCLUSION PRODUCTS

- 5.1. This section covers the assessment of the ML/TF risks of the specific financial products and services aimed to advance financial inclusion advocacy of the BSP, as follows:

| Product | ML/TF Risk |
|---------------------------|------------|
| MF Loans | Low |
| BDA | Low |
| Microinsurance | Low |
| Pawning | Low |
| Remittance thru pawnshops | Medium |
| E-money | Medium |

- 5.2. The risk assessment for MF loans, BDA, micro-insurance and pawning remains **low**, similar to the assessment in the 2017 NRA. This is mainly due to the low transactional amounts involved in these products as well as the limited and well-defined product functionalities and target market, i.e., the unserved/underserved population. E-money and remittance service of pawnshops shifted to **medium** risk from the previous assessment of low and low-medium risks, respectively, in the 2017 NRA. This is attributed to the rising level of ML/TF threat¹⁰⁹ and emerging use of both products to send and receive low value remittances related to a number of unlawful activities¹¹⁰ such as transfers through mule accounts, fraud scams, OSEC and swindling.
- 5.3. Cognizant that advancing financial inclusion requires a whole-of-government approach, the BSP together with other government agencies launched the NSFI in 2015. The NSFI serves as a platform for public and private sector collaboration to harmonize initiatives and foster a more efficient process to achieve the shared vision of financial inclusion. This is supplemented by the Philippine Development Plan 2017-2022 which identifies financial inclusion as a component of the government's vision for the financial sector.
- 5.4. As a policy objective, financial inclusion is considered inter-dependent with financial stability and integrity, and consumer protection. The policy making approach is to balance these objectives through proportionate regulations that enhance financial access, protect consumers' rights, and ensure safety, soundness, and integrity of the financial system. In 2017, the BSP together with the Consultative Group to Assist the Poor completed a research exercise analyzing how linkages among I-SIP Framework have been managed in the case of several policies such as MF, micro-banking office, e-money, and pawnshops¹¹¹.

¹⁰⁹ The ratings for products of EMLs and pawnshops that are crucial to the low-income population should be taken under the broader context of OFIs assessment. The ratings in this section are specific to financial products designed for the underserved and unserved market segments, unlike the ratings in the section on OFIs which are based on the entire operations and customers of the entity

¹¹⁰ Refer to ML/TF risk assessment on pawning with remittance services and e-money

¹¹¹ Financial I-SIP: Observations and Lessons for the I-SIP Approach from the Philippines (April 2017)

LANDSCAPE

5.5. Access to financial services is essential for every household and business. Financial inclusion carries the potential of improving the well-being of the low-income population and the growth of micro, small and medium enterprises. Data on access to and usage of formal financial services in the Philippines suggest that the country's financial system has become more inclusive over the years. The number of bank branches increased by 4.1 percent covering 68.8 percent of all cities and municipalities in the country, while ATMs grew by 2.3 percent. Non-bank financial service

Table 3. Financial Access Points

| | 2018 | 2019 | Growth |
|---------------------------------------|--------|--------|----------|
| Banks | 12,316 | 12,820 | 4.1% ↑ |
| ATMs | 21,278 | 21,777 | 2.3% ↑ |
| NSSLAs | 196 | 200 | 2.0% ↑ |
| Credit Cooperatives | 3,881 | 2,711 | -30.1% ↓ |
| MF NGOs | 2,861 | 3,887 | 35.9% ↑ |
| Pawnshops | 12,107 | 13,801 | 14% ↑ |
| MSBs | 5,483 | 6,784 | 23.7% ↑ |
| Other Non-Bank Financial Institutions | 219 | 224 | 2.3% ↑ |
| E-Money Agents | 52,600 | 43,740 | -16.8% ↓ |

providers remain important access points especially in those areas without physical banking presence. Their presence translates to more than 70,000 additional access points. About 85 percent of cities and municipalities without banking offices are being served by these providers¹¹².

5.6. The 2019 Financial Inclusion Survey showed that the share of Filipino adults with a formal financial account has improved from 23 percent in 2017 to 29 percent in 2019. Further, the goal of the BSP's Digital Payments Transformation Roadmap 2020-2023 is to convert 50 percent of the total retail transaction volume into digital form and onboard 70 percent of Filipino adults to the formal financial system. The BSP is optimistic to achieve these targets given recent developments such as the initial implementation of PhilSys Act which has enabled preregistration of 10.5 million Filipinos in 2020 as well as the accelerated use of digital payments and transaction accounts for various transactions as a result of the COVID-19 pandemic.

LEGAL AND REGULATORY FRAMEWORK

5.7. The legal and regulatory framework supporting financial inclusion includes the following:

| New Laws Enacted | Related Issuances |
|---|---|
| R.A. No. 11211 (amendments to the BSP Charter) strengthens the role of the BSP to pursue financial inclusion, financial education and consumer protection | <ul style="list-style-type: none"> Circular No. 1039 simplifies the registration requirements for pawnshop operators and MSBs Circular No. 1048 provides the rules on financial consumer protection to strengthen market conduct practices of BSFIs |
| R.A. No. 11127 or "The National Payment Systems Act" provides | <ul style="list-style-type: none"> Circular No. 980 operationalizes adoption of the NRPS Framework, paving the way for the development of the |

¹¹² Or 435 out of 510 unbanked cities and municipalities

| New Laws Enacted | Related Issuances |
|--|---|
| comprehensive legal and regulatory framework for the payment systems in the country; | <p>electronic payments industry. NRPS is a critical platform for delivering innovative financial products especially those designed for the low-income market</p> <ul style="list-style-type: none"> • Circular No. 1033 streamlines the process of securing licenses to engage in electronic payments and financial services • Circular No. 1049 requires the registration of operators of payment systems; • Circular No. 1055 promotes the adoption of a National Quick Response Code Standard |
| R.A. No. 11055 establishes the “PhilSys” as a national digital ID to promote financial inclusion | <ul style="list-style-type: none"> • Circular No. 1022 on AML/CFT regulations provides, among others, the use of PhilSys ID card as an official document for financial transactions and technology for CDD requirements |
| Others | <ul style="list-style-type: none"> • Circular No. 940 allows banks to contract retail outlets as cash agents where clients can avail banking services • Circular No. 987 provides guidelines in establishing branch-lite units through affordable licensing fees to entice banks to expand access points to serve MF clients • Circular No. 992 outlines the BDA framework which aims to liberalize customer onboarding and to increase access of the unserved and underserved to financial services |

FINANCIAL INCLUSION PRODUCTS

5.8. **MF LOANS.** These are small value loans targeted for the microentrepreneurs belonging to the basic sectors and low-income population. MF loan categories depend on the activity that is financed (i.e., microenterprise, loans to growing microenterprises or MF plus, housing MF and micro-agri loans). MF loans can be availed from MF institutions such as banks with MF operations, savings and credit cooperatives¹¹³ under the supervision of the Cooperative Development Authority, and MF NGOs registered under the SEC through the Microfinance NGO Regulatory Council¹¹⁴.

| Table 4. MF Loans | 2018 | 2019 | Growth |
|---|-------|-------|--------|
| Banks | | | |
| Number of Borrowers (in millions) | 2.0 | 2.4 | 21.3% |
| Outstanding Loans (in billions pesos) | 22.6 | 27.3 | 20.7% |
| Cooperatives | | | |
| Number of Member-Depositors (in millions) | 9.4 | 9.2 | -2.1% |
| Outstanding Loans (in billions pesos) | 276.0 | 307.7 | 11.5% |
| MF NGOs | | | |
| Number of Clients (in millions) | 4.2 | 5.2 | 22.9% |
| Outstanding Loans (in billions pesos) | 30.9 | 41.9 | 35.3% |

Source: BSP Financial Inclusion Dashboard

5.9. ML/TF risk for MF loans is generally **low** due to familiarity and low risk profile of clients, defined product features and existence of control measures to mitigate risks. MF loans are primarily available to resident Filipino citizens. BSFIs have reasonable understanding







¹¹³ Due to unavailability of data on cooperatives offering MF, figures for cooperatives cover all members and various types of cooperative loans

¹¹⁴ The Microfinance NGO Regulatory Council is created to institute a system of accreditation for MF NGOs and monitor their performance to ensure compliance with the provisions of R.A. No. 10693

of their clients who typically reside within the vicinity of their operations. Borrowers of MF-oriented banks must open a deposit account before they are allowed to avail of the loan or make non-face-to-face transactions via the mobile application or internet. Hence, the anonymous use of the product is deterred. Furthermore, loan value thresholds are in place to prevent possible abuse of the product and available loan amounts are relatively low ranging from PhP8,000 to PhP33,000 per provider¹¹⁵. Lastly, there were no related ML/TF cases and STRs filed between the covered period.

- 5.10. **BDA.** BDA is designed to meet the needs of the unbanked for a low-cost, no-frills deposit account. Its features include simplified account opening requirements, minimal initial deposit amount (not more than PhP 100 or around US\$2), and no maintaining balance and dormancy charges. The reduced CDD feature has been emphasized to guide BSFIs in implementing risk-based measures.

Table 5. BDA Statistic

| Bank Deposit Account | Q3 2019 | Q3 2020 | Growth |
|---|----------|----------|---|
|  Banks Offering BDA | 119 | 130 | 9.2%  |
|  Number of BDAs | 3.1 Mn | 6.2 Mn | 99.3%  |
|  Total outstanding deposits in BDA | ₱ 2.7 Bn | ₱ 4.5 Bn | 64.9%  |

Further, to incentivize banks to market and offer it to the unbanked, BDA has zero reserve requirement¹¹⁶. These have gained traction with the growth of usage of BDA¹¹⁷ (Table 5). Moreover, cash agents have been a common access point for BDA transactions while the average amount per account is around PhP 1,845.

- 5.11. The ML/TF risk for BDA is *low* primarily due to low value threshold and existence of risk mitigants. BDA is exclusively offered by banks to resident Filipino citizens. Customers are subjected to reduced CDD and face-to-face requirement. While BDA can be opened through cash agents, the decision to approve the account opening remains with the banks. The average daily balance threshold of PhP50,000 must be observed, otherwise, BDA will be converted to a regular deposit account and subjected to additional CDD measures. Compliance with existing regulations of banks offering BDAs is monitored and verified during BSP onsite examinations. Also, there were no reported ML cases and STRs filed from 2017 to June 2020 involving BDA.
- 5.12. **MICRO-INSURANCE.** Micro-insurance, as defined in R.A. No. 10607¹¹⁸, is a financial product that aims to meet the risk protection needs of the poor where (a) the amount of contributions, fees or charges, computed on a daily basis, does not exceed 7.5 percent of the current daily minimum wage rate of a non-agricultural worker in Metro Manila (MM)¹¹⁹, and (b) the maximum sum of guaranteed benefits is not more than

¹¹⁵ Derived by dividing the “Total amount of loans” vs. the “Total number of borrowers” of MF Loans provided by Banks, Cooperatives and MF NGOs

¹¹⁶ BSP Circular No. 992 dated 01 February 2018

¹¹⁷ Data source is BSP Department of Supervisory Analytics

¹¹⁸ An Act Strengthening the Insurance Industry, further amending Presidential Decree 612, otherwise known as “The Insurance Code”, as amended

¹¹⁹ Based on current rate of PhP 537, maximum daily premium is PhP 40 or roughly PhP 1,200 a month

1,000 times of the current daily minimum wage rate for non-agricultural workers in MM¹²⁰. Like traditional insurance, microinsurance comes in several forms to cover a range of risks, such as health and property risks, death and natural disasters. Without any risk protection, the poor are susceptible to unforeseen circumstances that will prevent them from improving their lives and overcoming poverty once it happens.

- 5.13. The ML/TF risk is generally *low* due to small value transactions, well-defined product features suited to the target market, and existing risk mitigants. Premium payments are relatively small and customers are subjected to reduced CDD procedures. Transaction ceilings are in place and cross-border transactions and anonymous purchases are not allowed. Prior to offering to the public, these products must be approved by the IC. Agents are also duly licensed by the IC and must strictly adhere to both BSP and IC regulations. Moreover, there were no reported ML/TF cases and STRs filed from 2017 to June 2020.
- 5.14. *Pawning and remittance services of pawnshops.* In the Philippines, pawning¹²¹ is the usual mode of swiftly obtaining or converting property to cash especially in cases of unforeseen and immediate needs. It involves lending money on personal property delivered to the possession of a pawnshop operator as collateral. Pawnshop operators are required to implement risk-based CDD to ensure that transacting clients are the rightful owners of the personal property being pawned. As of the 3rd quarter of 2020, there were 14,553 BSP-authorized pawnshops nationwide.
- 5.15. Business model of pawnshops is evolving as it is increasingly becoming involved in corollary businesses such as remittance and foreign exchange. Available data show that income from corollary businesses compensates for the losses in pawning operations. A study also revealed that pawnshops dominate the money transfer market in the Philippines where 76 percent of users belong to class D (poor) and E (very poor)¹²².
- 5.16. ML/TF risk for pawning service remains to be *low* because loans are secured by personal properties. Loans obtained from pawning are usually short-term and involve small amounts, i.e., PhP 5,000 and below¹²³, while no limit has been placed as to the number of transactions a customer may have for a particular period. This is considered reasonable since pawnshops cater primarily to low-income groups. Nevertheless, common threat to pawning is the acceptance of illegally obtained personal property (e.g., robbery or theft). Strict adherence to CDD procedures must be observed to effectively mitigate the risk. Based on the complaints received from the public for the covered period, there were only thirteen incidents involving acceptance of stolen items by pawnshops, which are all considered closed/resolved. This is an indication that pawning is inherently less susceptible to ML/TF activities.

¹²⁰ About PhP 537,000 based on the PhP 537 minimum wage rate

¹²¹ Practice of lending money and accepting and/or keeping gold and other personal properties of value as collaterals.

¹²² BFA (2010). Demand study on domestic payments in the Philippines

¹²³ See Pawnshop Sector Assessment

- 5.17. On the other hand, ML/TF risk for remittance services by pawnshops is assessed as *medium* from low-medium in the 2017 NRA due to rising number of STRs involving low value international inward remittances covering various crimes such as OSEC and extortion schemes (See cases 22 and 23 below). Cross-border transactions are facilitated through the pawnshops' tie-ups with international remittance service providers. Actual amounts involved in these remittances are relatively low (i.e., 57 percent of domestic remittances involve transaction amounts of PhP 5,000 and below¹²⁴). Meanwhile, the average annual amount of financial assistance received from abroad is PhP 26,000¹²⁵ which is the typical value of remittances sent by Overseas Filipino Workers to their families.
- 5.18. Based on analysis of STRs, the following case typologies illustrate use of MSBs for ML/TF activities:

Case 22: OSEC. MSBs have been prevalently used to send low value remittances for OSEC activities¹²⁶. OSEC-related STRs increased to 10,397 in 2019 from 1,572 covering the period from 2015 to 2018¹²⁷. The increasing trend continued during the first half of 2020 with 20,245 STRs marking OSEC as one of the most prevalent crimes during the COVID-19 pandemic. The modus typically involves a male sender from other jurisdictions sending remittances ranging between PhP 1,000 to PhP 10,000 to multiple non-related beneficiaries in the Philippines.

Case 23: Various extortion schemes. MSBs were also used to receive payments for various extortion schemes (i.e., sextortion and extortion masked as donation) and fraud scams during the pandemic. Out of 52 sextortion related STRs, 29 percent were reported by MSBs¹²⁸. This illegal act employs deceit, intimidation, and threat towards the victim to extort money in exchange for not exposing salacious photos or videos publicly. Notable fraud scams involve hacking of social media or email accounts then asking the victims' friends or family members for monetary assistance. Other fraudsters pretend to be affiliated with government units soliciting COVID-19 donations from victims.

Case 24: TF activities. There were around 760 STRs filed related to TF totaling PhP 4.8 million¹²⁹. These STRs provide a red flag that pawnshops are likely to be used for TF activities.

- 5.19. *E-money.* E-money industry plays a critical role in advancing digital financial inclusion¹³⁰. In the Philippines, e-money has empowered untapped segments such as women, low-income households, farmers in rural areas and migrants and their families in using digital financial services. In addition, e-money has been a vital access point in the efficient delivery of humanitarian cash assistance and cash subsidy programs by the government. The industry was tapped for the digital distribution of the 2nd tranche of the Government's SAP for poor families affected by COVID-19. Consequently, 78

¹²⁴ PSA (2018). National Migration Survey

¹²⁵ Based on 2018 National Migration Survey conducted by PSA and University of the Philippines

¹²⁶ Inclusive of pawnshops with MSB operations

¹²⁷ Pages 11 and 17, AMLC's ML/TF risk assessment entitled: "Online Sexual Exploitation of Children: A crime with global impact and an evolving transnational threat"

¹²⁸ Page 15, AMLC's study entitled: Analysis of Financial Crimes Trends During COVID-19, Series 1 (Oct 2020 Update)

¹²⁹ Based on STR submissions by Pawnshops from 2017 to June 2020

¹³⁰ State of the Industry Report on Mobile Money 2019, GSMA

percent of the 7.3 million accounts opened for SAP beneficiaries were e-money wallets¹³¹. Moreover, at the height of the ECQ between 17 March and 30 April 2020, four million new accounts, including e-money, were opened digitally¹³². As of June 2020, there are 51 EMLs, comprised of 27 banks and 24 non-banks. The usage of e-money from 2013 to 2019 for non-bank EMLs posted an average annual growth of 64.1 percent (almost twice for banks) while the number of transactions totaled 274 billion in 2019¹³³.

- 5.20. The ML/TF risk for e-money is *medium* due to the increasing level of STRs filed involving the use of e-money as mule accounts as well as for other financial crimes. Also, the capability to transfer funds internationally through the use of digital products makes it an attractive vehicle to move funds for terrorism. The development and timely adoption of appropriate strategies need to be enforced to effectively manage emerging ML/TF typologies and other financial crimes within the e-money space.

Mule accounts. COVID-19 pandemic has caused disruptions in the financial system forcing criminals to exploit the use of digital financial services. During the ECQ period, EMLs filed a total of 16,535 STRs related to use of suspected mule or pass-through accounts. These STRs involved multiple high value transfers to third-party bank accounts totaling PhP 198.9 million. The EMLs cited the possible abuse of digital CDD process to create suspected pass-through accounts¹³⁴. Furthermore, ECQ samples disclosed that EMLs reported 5,372 STRs related to unauthorized transactions such as skimming and phishing. These illegal acts often involve unauthorized online transfers from victim's bank account to perpetrator's e-money accounts¹³⁵.

- 5.21. As to customer experience, the number of complaints received from the public regarding the use of e-money platform significantly increased from 85 cases in 2017 to more than 1,500 cases in 2019. Most cases were committed through online channels as people shift to electronic platforms.
- 5.22. Nevertheless, policies and controls are continuously updated to prevent the use of e-money accounts as vehicle for ML/TF activities. Although gaps still exist in monitoring possible suspicious transactions, EMLs are progressively learning to identify various threats and are able to report suspicious transactions. E-money transactions continue to have a low value threshold as the BSP placed an aggregate monthly load limit on e-money instruments amounting to PhP 100,000, unless a higher limit is approved by the BSP. There is also an electronic system in place aided by manual processes to perform adequate customer profiling. Further, non-bank EMLs continue to strengthen measures to mitigate the threats arising from ML/TF activities.

¹³¹ Data Source: Department of Social Welfare and Development as presented in the 9th Financial Inclusion Steering Committee (FISC) Meeting on 06 October 2020

¹³² BSP Technology Risk and Innovation Supervision Department

¹³³ Page 112 and Appendix 7 of the Report on the Philippine Financial System (First Semester 2020)

¹³⁴ Pages 10 to 11, AMLC's study entitled: Analysis of Financial Crimes Trends During COVID-19, Series 1 (October 2020 Update); and Page 14, AMLC's study entitled: Analysis of Financial Crimes Trends During COVID-19, Series 2 (October 2020 Update)

¹³⁵ Page 19, AMLC's study entitled: Analysis of Financial Crimes Trends During COVID-19, Series 1 (October 2020 Update)

6 TERRORIST FINANCING RISKS



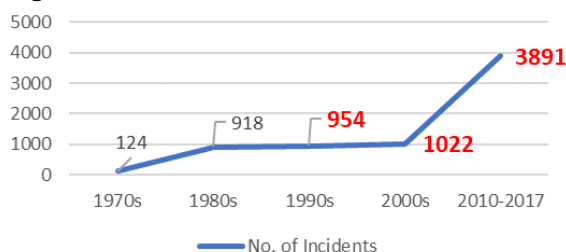
- 6.1. The threat posed by TF to the sector is *high*. This is primarily driven by the presence of insurgent and terrorist groups in the country with systematic and established method of raising funds for their operations. These include using illegal means to raise funds, such as KFR and extortion, and resorting to legitimate means to finance their activities. BSFIs, particularly banks and MSBs, are being used to move their funds for terrorist activities.

The BSFI sector is inherently vulnerable to TF activity, due to its wide range of products and services, and expanded geographic reach. BSFIs have controls in place directed to mitigate such activities, although scope for enhancements are still noted on certain aspects of CDD and transaction monitoring. In this regard, BSFI's overall vulnerability to TF is assessed as *High*.

THREAT ASSESSMENT

- 6.2. Based on publicly available data¹³⁶, there was a significant increase in the number of recorded terrorism incidents in the last three (3) decades from 1990s to 2017 (Figure 30).

Figure 30. Number of Incidents



LEAs recorded increase in terrorism incidents from 1,039 in the 2nd NRA to about 2,660 incidents from 2017 to 30 September 2020. Over 50 percent of the incidents occurred in the Mindanao region, while 16 percent transpired in the Bicol Region¹³⁷.

- 6.3. Attacks carried out by terrorist organizations and local threat groups indicate the presence of funds and material support for terrorist activities. They use illegal means to obtain funding. These include KFR and extortion. They also resort to legitimate means and among the fund-raising methods utilized is the use of NPOs¹³⁸ mainly for soliciting donations, family funding and legitimate business fronts. The funds are generally used

¹³⁶ Data retrieved from <https://www.start.umd.edu/gtd> University of Maryland. Website was accessed on 16 December 2020.

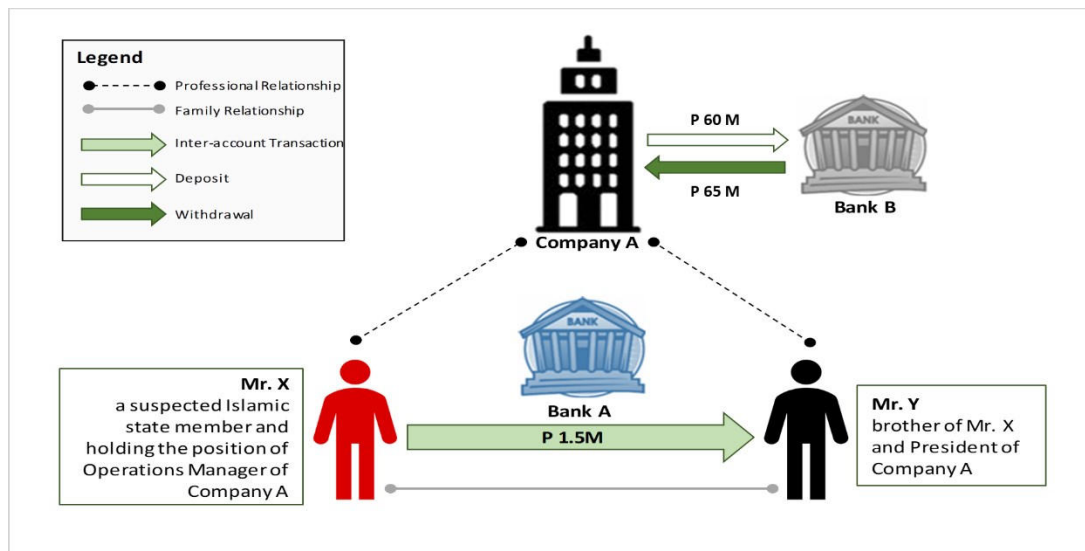
¹³⁷ AMLC 2021 Terrorism and Terrorism Financing Risk Assessment.

¹³⁸ NPO Risk assessment 2018

for logistics and operational purposes, such as purchase of arms and vehicles. Part of the funds raised were used to support the communities where they operate¹³⁹.

Terrorist organizations and threat groups in the Philippines use a variety of methods to move funds. 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 thru 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 VC and/or cryptocurrency. There are also anecdotal incidents that terrorist groups had utilized crypto-assets in the Marawi siege¹⁴⁰.

- 6.4. Banks as channel in the facilitation of transactions of corporate and individual customers in possible financing of terrorism activities is shown in *Case 25* below:



¹³⁹ 2nd NRA 2017, page 282.

¹⁴⁰ AMLC 2021 Terrorism and Terrorism Financing Risk Assessment.

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 an alert 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.

- 6.5. MSBs as channel in the facilitation of transactions of individuals with apparently wide network of transactions and involved in terrorist activities is shown in *Case 26* below:

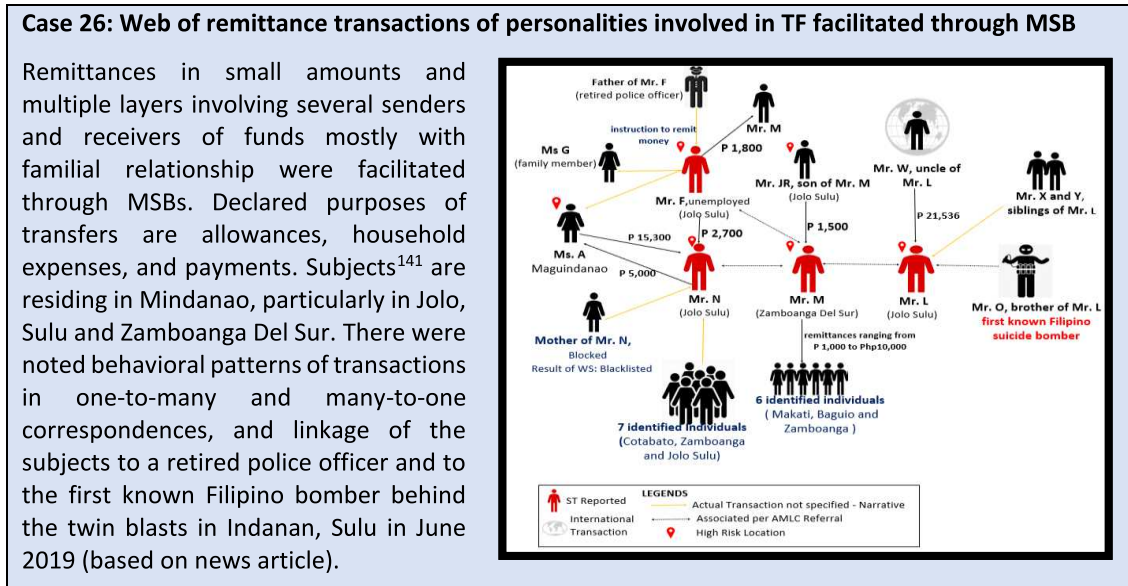
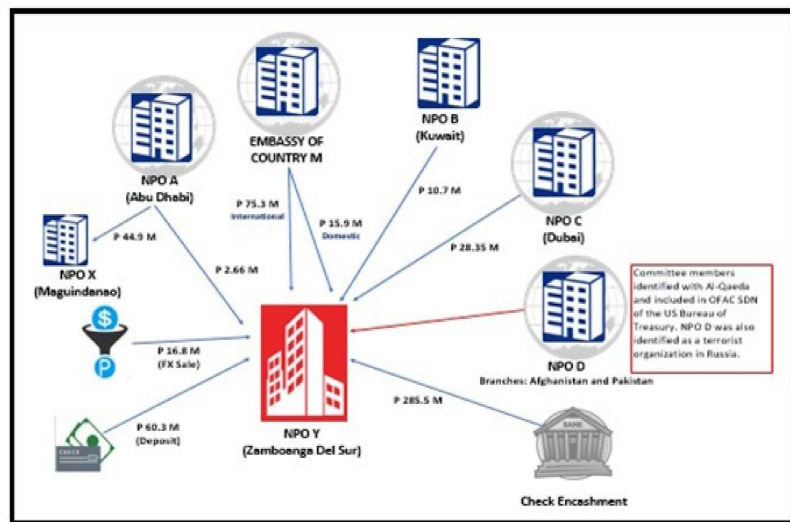


Figure 31. Use of Banks by NPOs in the facilitation of TF

- 6.6. Based on the NPO risk assessment in 2018, there were nine (9) STRs filed by banks involving NPOs related to possible terrorism/TF. *Figure 31* depicts the use of banks by NPOs. Review of the transactions/records disclosed that the client is a charitable institution receiving funds through remittances from various NPOs. Declared purpose is for building mosque, schools and provide allowances for Islamic teachers. US Department of the Treasury designated and



¹⁴¹ 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.

blocked the assets of NPO D, remitter of funds to NPO Y, due to its committee members' identification with Al-Qaeda and inclusion in OFAC SDN List.

VULNERABILITY ASSESSMENT

- 6.7. BSFIs, particularly banks and MSBs, are highly vulnerable to TF due to their broad geographic reach, complex products and services, and variety of delivery channels. This is mitigated and continuously being addressed by the existence of CFT legal, regulatory and institutional frameworks, such as the R.A No. 10168 or the TFPsA of 2012 and its IRR and the newly enacted R.A. No. 11479 or the Anti-Terrorism Act of 2020. In addition, enhanced continuing collaboration and cooperation of the LEAs, intelligence agencies, CPs, supervisors and the AMLC were instituted in response to said high TF vulnerability¹⁴². These are complemented by BSFIs' processes for dealing with TF and related transactions. Banks and MSBs have established necessary control measures particularly on risk assessment, conduct of CDD, transaction monitoring, ST reporting, trainings, and compliance with freeze orders.
- 6.8. *Scope for enhancements* in this respect include: (i) adoption/enhancement of the IRA to consider the TF risk assessment in the national/sectoral level; (ii) conduct of in-depth customer profile and verification process on connected parties; (iii) improvement of customer risk assessment methodology to consider relevant factors, such as nationality, geographic location and origin; (iv) expansion of watchlist databases; (v) adoption of TF-related alert parameters, participation in the PPPP or information sharing protocol (ISP) with the AMLC and enhancement of the quality of STRs; and (vii) improvement of learning modules relating to TF, including obligation to freeze funds under TFS.

¹⁴² AMLC 2021 Terrorism and Terrorism Financing Risk Assessment (www.amlc.gov.ph)

7 IMPACT ASSESSMENT

- 7.1. Considering the overall high threat posed by ML/TF/PF activities and the inherent vulnerabilities of the sector, the overall consequence is rated *high*. ML/TF/PF activities adversely affect the financial ecosystem, specifically the customers, the financial institutions, the financial system, and the country.

INDIVIDUAL/CUSTOMER LEVEL

- 7.2. The consequences of criminal threats or ML/TF/PF activities to customers are assessed to be *medium*. Customer trust is fundamental in promoting a vibrant, safe and sound financial system. Perceived risks in using financial products and services due to unlawful activities may become an obstacle in building such trust, especially for those who were victims of the crimes or illegal schemes. Further, the public/customers may sustain losses from ML/TF/PF activities such as financial losses from fraud or from rebuilding damaged properties due to an attack. Predicate crimes and terrorist attacks pose physical, safety and security risks to the people. ML/TF/PF risks may also undermine the private sector or companies in the form of loss of trade or income due to uneven competition posed by shell or front companies with capital sourced from illegal activities and mainly used by criminals to hide the illicit origin of their funds

- 7.3. The consequences of criminal threats or ML/TF/PF activities to BSFIs are assessed as *high*. BSFIs are intricately linked through banks, which act as the nexus of transactions in the financial system. Banks are the principal channels in facilitating financial transactions in the country. In this respect, banks and other BSFIs involved in reported ML/TF/PF incidents may suffer from reputational risk which will undermine the confidence of the public not only on the concerned institution but also on the financial sector, as a whole. BSFIs may also suffer subsequent loss of income or business, incur legal expenses and be liable for monetary penalties for non-compliance with AML/CFT requirements. Actions to mitigate ML/TF/PF threats warrant resources and costs considering the evolving ML/TF/PF landscape.

FINANCIAL SYSTEM

- 7.4. The consequences of criminal threats or ML/TF/PF activities to the Philippine financial system are assessed as *high*. Criminals continue to explore opportunities to use the financial system for the proceeds of their illegal activities, including the use of technology for financial transactions which allow rapid movement of funds. If not properly and immediately mitigated, these may adversely affect the sector's financial performance and reputation, and consequently affect financial stability.

NATIONAL/COUNTRY LEVEL

- 7.5. The consequences of criminal threats or ML/TF/PF activities to the national/country level are assessed as *high*. Locally, the prevalence of crimes and terrorist incidents threaten national security, peace and order and safety of the people. Internationally, it affects the reputation of the country which has a cascading effect on related industries, such as tourism and trade, including inflow of foreign direct investments for legitimate businesses and cross-border transactions. Further, high ML/TF/PF threats translate to increased social cost, higher cost of doing business and more government resources dedicated for law/regulatory enforcement and crime prevention. All of these will impact on the country's economic growth.

