MONEY SERVICE BUSINESS

2021 MONEY LAUNDERING AND TERRORISM FINANCING SECTOR RISK ASSESSMENT

EXECUTIVE SUMMARY

AMLC

EXECUTIVE SUMMARY

The money service business (MSB) sector has been a target of criminals to move and, at times, facilitate proceeds of criminal activities. In the Philippines' Second National Risk Assessment (NRA), the MSB sector was rated high in relation to the threat to money laundering and terrorism financing (ML/TF), particularly citing the involvement of 17 remittance companies and foreign exchange dealers in drug trafficking and illegal sex trade. One of the biggest bank heist cases in 2016 also affected the sector. In the case, three remittance companies and foreign exchange dealers facilitated the transfer of PhP3.8 billion from fictitious bank accounts to casinos, junket operators, and unidentified individuals.

The Philippines' Mutual Evaluation Report (MER), which the Asia Pacific Group on Money Laundering (APG) adopted in August 2019, noted a range of threats and offenses that exploit the cash- and remittance-based economy, including under-resourced authorities and legislative and the procedural hurdles that impede investigation and prosecution efforts. Further, the report highlighted the risk of unregistered MSBs that may contribute to the potential facilitation of illicit proceeds.

These impediments are continuously being addressed as seen from the significant improvements and efforts undertaken by the supervising agency—Bangko Sentral ng Pilipinas (BSP)—and the Anti-Money Laundering Council (AMLC). Measures and controls have been placed to mitigate threats, which impact the overall vulnerability of the sector.

Measures include amendments in the BSP's manual of regulations and the extensive registration process, which resulted in a significant restructure and consolidation of the sector. While the MSB sector's level of understanding of ML/TF risks and anti-money laundering and counter-terrorism financing (AML/CTF) obligations is developing, the newly structured MSB sector is seen to provide a strong framework for AML/CTF compliance.

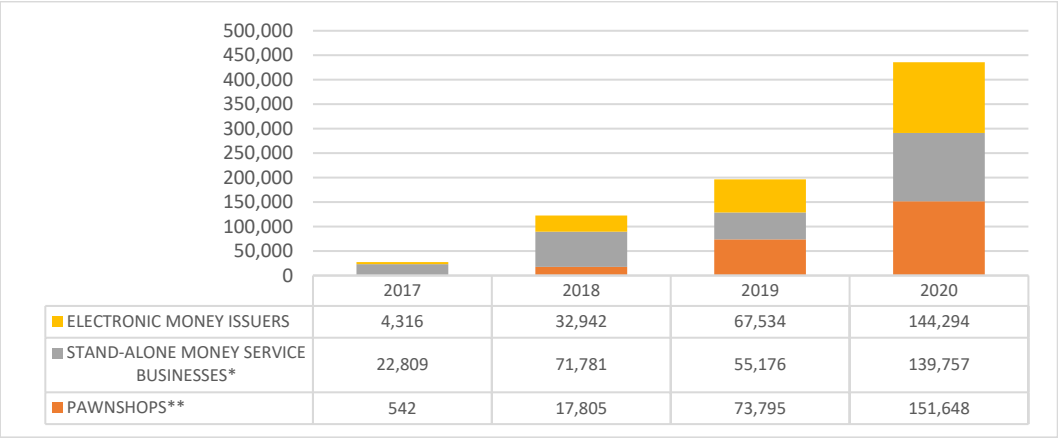
To monitor and identify emerging risks associated with the sector, the AMLC, with the assistance of the Australian Transaction Reports and Analysis Centre (AUSTRAC) and support of the BSP, undertook a risk assessment, using data from transaction reports, responses from the BSP, and survey results from relevant industries and other Philippine government agencies. This risk assessment shall serve as guidance for supervising agencies, financial institutions (FIs), and law enforcement agencies as regards policy issuances and risk-based strategies.

Summary of findings

In the analysis of transactions and investigations of cases, certain services or products catered by MSBs are being used by criminals for their illegal activities. Remittance services and cash transactions, including money changing facilities, were the primary means of moving illegal proceeds.

From 2017 to 2020, MSBs submitted 782,399 suspicious transaction reports (STRs) with an estimated STR value of PhP22.66 billion (USD453.13 million). This number includes transactions of pawnshops,[1] conducting MSB services (i.e., remittances and foreign exchange buying and selling).

Chart A. STRs filed by the MSB sector, 2017 to 2020



	2017	2018	2019	2020
ELECTRONIC MONEY ISSUERS	4,316	32,942	67,534	144,294
STAND-ALONE MONEY SERVICE BUSINESSES*	22,809	71,781	55,176	139,757
PAWNSHOPS**	542	17,805	73,795	151,648

** Decrease in the number STRs filed by MSBs is associated with the decline in the suspicious transaction (ST) reporting by one remittance transfer company with virtual currency exchange services.*
***STRs filed by pawnshops in relation to remittances, money-changing and FX-dealing functions, and other MSB-related activities.*

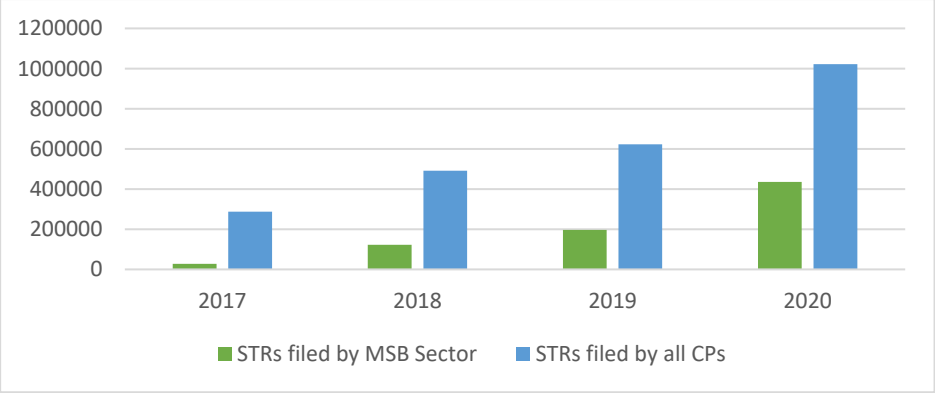
Generally, the volume of STRs follows an increasing trend with a yearly average percentage increase of 175% from 2017 to 2020. STRs filed by pawnshops (with corollary MSB-related activities and transactions) peaked in 2018 at 17,805 STRs, registering a percentage increase of 3,185% from only 542 STRs in 2017. Thereafter, STRs filed by pawnshops continue to exponentially increase, reaching 151,648 STRs in 2020.

A news article[2] published on 27 August 2020, indicated that the share of remittance operations to pawnshops' income should continue to rise as more institutions tap the services of pawnshops, due to their wider reach compared with banks and financial institutions.

The STRs filed by the MSB sector from 2017 to 2020 account for a relatively high share at 32% of the total STRs filed by all covered persons (CPs) within the same period, as presented in the chart below.

[1] Transactions of pawnshops such as precious stones-buying, redemption, and pledge loan release were excluded in the data presented.
[2] https://www.pna.gov.ph/articles/1113644, 27 August 2020

Chart B. Comparative assessment of STR submissions, 2017 to 2020

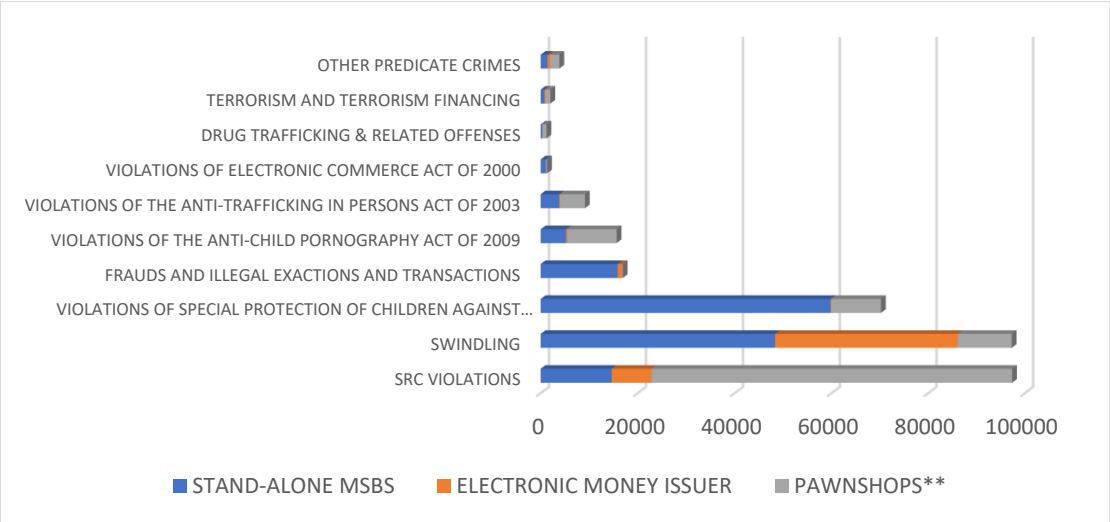


The study assessed three categories of the MSB sector based on the current classification available to the AMLC: (1) stand-alone MSBs (SA-MSBs); (2) electronic money issuers (EMIs); and (3) pawnshops in relation to MSB-related transactions.

The re-registration initiative of the BSP allows the consolidation of industry types related to MSB functions in one sector and contributes to the ease of monitoring and supervision of MSBs. In this study, remittance agents, foreign exchange dealers/money changers, and remittance and transfer companies (RTC) with virtual currency exchanges (VCEs) are lodged under the category SA-MSBs.[3]

From the STRs filed by MSBs from 2017 to 2020, child exploitation, child pornography, trafficking in persons (TIP), swindling/fraud, Securities Regulations Code (SRC) violations rank among the most number of suspicious transactions reported.

Chart C. Suspicious transaction reports, in terms of volume



[3] Based on the registration classification set by the BSP and adopted by the AMLC

Stand-alone money service businesses

For SA-MSBs, child exploitation is the most reported category of STRs. In terms of STR value, excluding transactions reported under the generic code [ZSTR],[4] trafficking in persons (TIP) has the highest value, estimated at PhP5.7 billion (USD114 million). Most suspicious transactions reported under TIP are related to child exploitation/pornography. From 2019 to 2020, the AMLC released its studies on child pornography, which contributed to the increase in STRs, particularly in the MSB sector.

The STRs under the category of "felonies/offenses of similar nature punishable by Penal Laws of other countries," rank second highest in terms of value. Most of these STRs are in relation to alleged syndicates involved in infusing funds in a certain foreign exchange corporation; and sex offenses and misdemeanor committed by foreign national.

Drug trafficking is likewise among the top crimes in terms of value, estimated at PhP86.25 million. This surmises that drug traffickers still prefer and continue to exploit the remittance facility of MSBs.

Electronic money-issuers

From the STR data set collected within the assessment period, there is a potential threat on the use of EMIs for fraudulent or suspicious transactions, as manifested by the increase in STR submissions from 4,316 STRs in 2017 to 144,294 STRs in 2020.

Eighty-one percent (81%) of STRs filed by EMIs are related to other suspicious indicators defined under 3b-1 of the Anti-Money Laundering Act of 2001 (AMLA), as amended. The remaining 19% of STRs is largely shared by swindling, SRC violations, frauds and illegal exactions, child pornography, TIP and terrorism and TF.

In terms of transaction value[5] per predicate crime, swindling and SRC violations rank with the highest estimated STR values at PhP283.36 million and PhP114.74 million, respectively. Other emerging threats or possible exploitation of EMIs are child pornography, TIP, terrorism and TF, and jueteng and masiao. STRs filed by EMIs in 2020 mostly noted the use of the sector in transacting proceeds of SRC violations and child pornography; and funds related to terrorism and TF.

[4] ZSTR is the generic code for STRs with no corresponding transactions. Covered persons usually use this code for attempted transactions, alerts, or additional account information of potential subjects of suspicion.
[5] STRs filed using the generic code ("ZSTR") for STR transactions are excluded in the assessment of suspicious transaction values.

Pawnshops with corollary money service business activities

For pawnshops with corollary MSB activities, 52.7% of the STRs are filed on other suspicious indicators; while 47.3% of the STRs are filed in relation to SRC violations, child pornography, swindling, drug trafficking, terrorism and TF, and other predicate crimes. In terms of transaction value per predicate crime, SRC violations, swindling, child pornography, and TIP share most of the alleged illegal proceeds.

Notably, robbery and extortion; and terrorism and TF with a combined share of PhP17.08 million in STR value are among the emerging threats affecting the pawnshop sector. Among the STRs filed on extortion, most pertain to the activities of a local terrorist/threat group.

Child exploitation and pornography, trafficking in persons, violations of Anti-Photo and Video Voyeurism Act of 2009

In the AMLC's 2019 and 2020 child exploitation and pornography studies, MSBs are identified as commonly used to further child online sexual exploitation (OSEC) activities.

Statistics show that MSBs are used more often compared with banks in moving funds intended for OSEC.[6] This provides a picture that majority of the offenders course their payments through MSBs, allowing suspected facilitators to claim the funds through the same financial platform.

Most of the STRs filed under the categories of TIP and violations of the Anti-Photo and Video Voyeurism Act of 2009 are related to child exploitation and cyberpornography cases. Low-value transactions, normally between PhP500 and PhP5,000, account for 70% of the STRs related to child exploitation, TIP, and pornography.

Terrorism and terrorism financing threats

Anecdotal intelligence and reports have previously identified MSBs for terrorism and TF. From 2017 to 2020, MSBs reported 2,007 STRs with an estimated STR value of PhP20 million. There is also an increase in MSBs' ST reporting on terrorism and TF with over 350% growth in 2020 compared with 2019.

The common range of TF-related funds is between PhP500 and PhP5,000 (below USD100). In the AMLC terrorism and TF risk assessment study,[7] over 6,000 STRs were reported by SA-MSBs, EMIs, and pawnshops that are possibly related to terrorism and TF from 2018 to 2020. Most of the STs

[6] Online Sexual Exploitation of Children: A crime with global impact and an evolving transnational threat, August 2020

[7] http://www.amlc.gov.ph/images/PDFs/2021%20JAN%20TF%20RA%20EXECUTIVE%20SUMMARY%20(WEBSITE).pdf

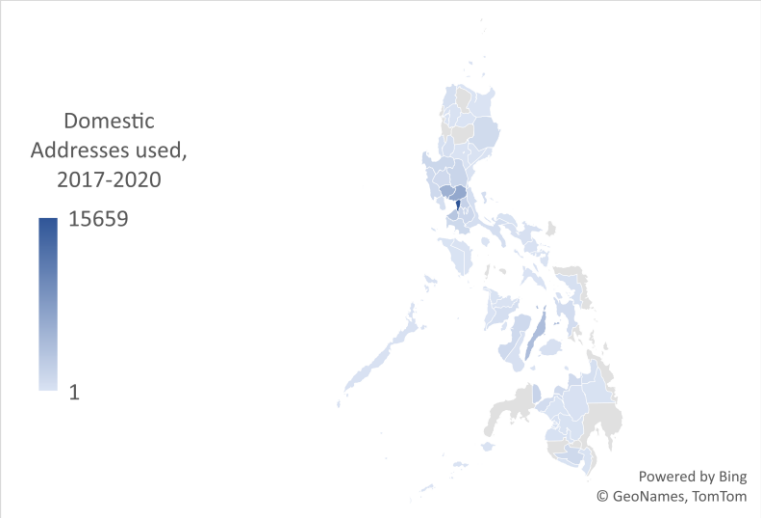
associated with terrorism and TF were reported under the category of suspicious indicators.[8] This may demonstrate quality issues and challenges for both the AMLC and covered persons in identifying terrorism- and TF -related transactions.

Geographical risk

MSBs provide essential financial services, often in underdeveloped regions or rural areas with limited or no banking services. In AMLC's child exploitation study and terrorism financing risk assessment, it was noted that domestic remittances moved across all regions. Child exploitation typologies also suggest that recipients/beneficiaries of proceeds are mostly located in rural or depressed areas.

In the sample STRs used in the study, 71,816 STR-international remittance transactions appear to have unique parties' addresses.[9] Domestic locations of STR subjects of international remittances are in Metro Manila (22%), Bulacan (9%), Pampanga (7.5%) , Cebu (6%), and Cavite (4.4%).

Chart D. Domestic locations based on STRs, 2017 to 2020



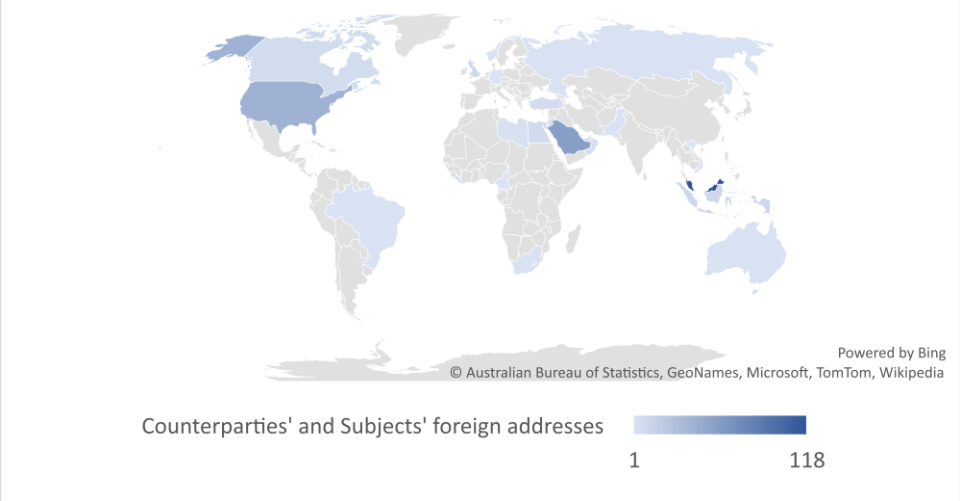
Countries with high number of international remittance-related STRs based on addresses, either as counterparty- or beneficiary-jurisdictions, include the United States of America [USA] (39%), Saudi Arabia (11%), Australia (6%), Canada (6%), United Kingdom (4%), and United Arab Emirates

[8] Suspicious circumstance indicators such as *"the transaction is similar, analogous or identical to any for the foregoing;" "the amount involved is not commensurate with the business or financial capacity of the client;" "there is a deviation from the client's profile/past transactions;" "there's no underlying legal or trade obligation , purpose, or economic justification;" and "the client is not properly identified."*

[9] The 71,816 international remittance-related STRs contain distinct subjects', account holders', beneficiaries', and counterparties' addresses per international remittance transaction. Thus, if subjects/accountholders who have the same addresses have remittances to one beneficiary address, then these transactions are grouped into one address.

[UAE] (3%). STRs are mostly related to child exploitation and pornography, trafficking in persons, and fraud.

Chart E. Countries identified in the international remittances based on STRs, 2017 to 2020



Cash-related transactions

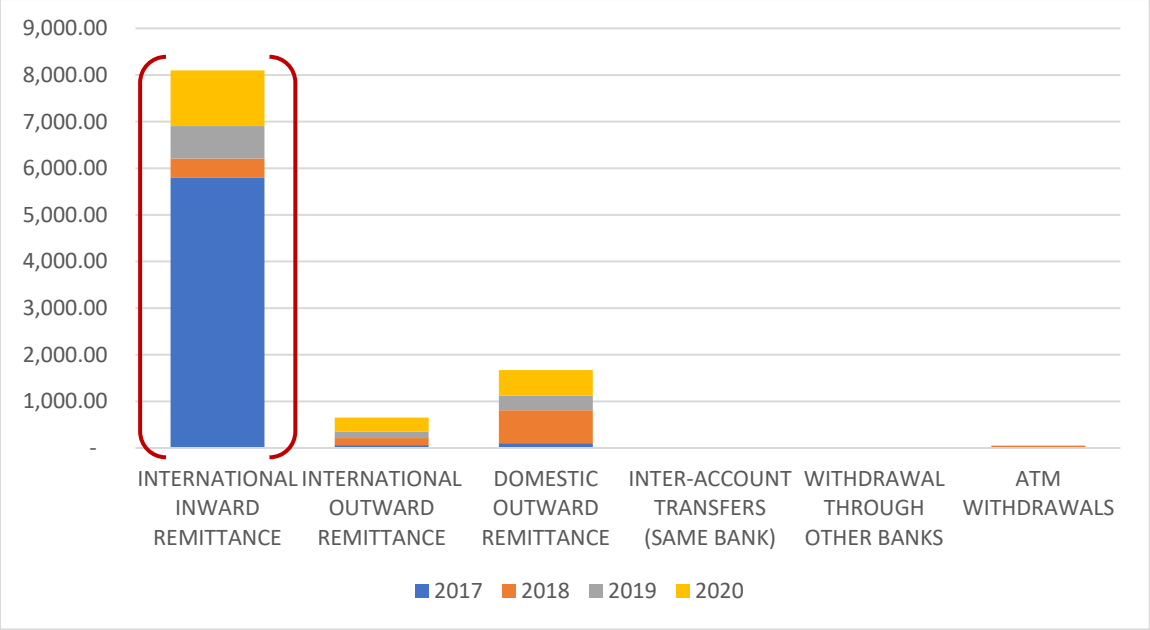
From the STR population subject of the study, 134,105 STRs are associated with cash transactions with an estimated STR value of PhP5.12 billion. This accounts for 31% of the total estimated value of the STR data set. This poses a threat as cash conceals the source of funds, making it difficult to determine the nexus of the source of cash and the underlying illegal or unlawful activity.

From the sample STRs, cash sale of foreign currencies ranks as the highest estimated proceeds at PhP2.18 billion, followed by cash deposits at PhP1.81 billion. Notably, cash purchase of foreign currency is another potential means to transfer value of proceeds by criminals. Proceeds from cash purchase of foreign currency are estimated at PhP893 million for the assessment period of 2017 to 2020.

Remittance transactions

The NRAs and MER noted that the remittance-based nature of the economy poses both as a threat and vulnerability of the Philippines for ML/TF. From the chart below, it may be gleaned that the Philippines is a destination of proceeds from other foreign jurisdictions.

Chart F. Suspicious transaction reports in terms of volume



Considering the value of STRs, 2017 has the highest reported STR value at PhP5.8 billion. PhP5.7 billion of the proceeds are associated with TIP and cyberpornography activities. Moreover, the estimated volume of withdrawals/outward remittances or inter-account transfers could not account for the value of inward remittance transactions. This may indicate that there were undetected disbursements, withdrawal, or transfer transactions associated with illicit activities.

Money laundering/terrorism financing cases involving money service businesses

In 2020 alone, the AMLC caused the filing of petitions for freeze order on seven cases predicated on illegal drugs (4 cases), violations of the Electronic Commerce Act of 2000 (1 case), violations of Customs Modernization and Tariff Act (1 case), and violations of the Securities Regulation Code (1 case). Sixteen (16) MSBs were identified in the said 10 cases. Twelve (12) of the 16 MSBs were impleaded as parties in the said cases. Three (3) MSBs were also involved in at least two cases. The value of proceeds from the ML cases amounted to PhP258.69 million.

TYPOLOGIES

Virtual currency exchange typologies

Terrorism and terrorism financing

1. A foreign national reportedly engaged in terrorism and TF sent funds to several individuals through a remittance transfer company (RTC). The RTC, upon verification of the accountholders, reported several suspicious transaction movements. The accountholders were able to cash-in about PhP50,000 to PhP200,000 (USD1,000 to USD4,000) within two

months from the creation of the accounts; and converted the funds to bitcoins (BTC) before sending to several unlabeled wallet addresses. Further investigation on the blockchain platform revealed that most BTC were forwarded to a wallet address associated with BTC transfers linked to a certain terrorist organization.

Investment fraud

2. The account was allegedly used in a multi-level marketing (MLM) scheme. The account user allegedly facilitated the MLM scheme by receiving payments from entry packages and then sending payouts to alleged members of the group. These movements showed the use of accounts as pass-through platforms.

3. Another STR case was triggered by cumulative cash-ins, totaling PhP500,000 (USD10,000) and cash-outs within 24 hours. The high-value cash-ins were converted to BTC and were sent to multiple users or to an unlabeled external wallet. A portion of the funds was likewise cashed-out to multiple recipients associated with a binary options investment platform.

OVERALL MONEY LAUNDERING/TERRORISM FINANCING RISK

Since the First and Second NRAs, the MSB sector has been regarded as high risk to ML threat although there was limited discussion regarding the involvement of the sector to TF.

The updated MSB risk assessment has identified emerging threats since the first two NRAs. Based on investigations and cases, MSB sector is most at risk to drug trafficking. Nonetheless, other criminals engaged in child exploitation, TIP, terrorism, and TF are seen exploiting MSBs to facilitate and to expand their network of illicit activities. Proceeds of child exploitation/pornography and TIP, SRC violations, and TF widely use remittance, foreign exchange dealing, and electronic money transfer services of the MSB sector.

The increase in ST reporting demonstrates how MSBs are widely used to facilitate movement of proceeds. The frequent low-value transactions with multiple senders and beneficiaries and the use of cash pose threats as these transactions conceal the source of funds, making it difficult to identify the nexus of funds with the unlawful activity.

The extent of threat and emerging risks, showing how MSBs are used extensively by criminals to move illicit funds, warrant a **high ML/TF threat rating** for the sector.

The MSB sector is likewise inherently vulnerable to ML/TF, considering its cash-intensive business, use of agents, small-value remittances, customer diversity, and vast network and geographical scope. The frequent and small-value remittances and use of cash pose a threat to the sector as these transactions add another layer of anonymity or obscurity.

Major developments and progress in regulating MSBs have been established since 2017. The consolidation of the MSB sector for consistent monitoring; information-sharing between the BSP and the municipal or local governments in identifying unregistered MSBs; improvements in AML registration and stringent surveillance of the sector; and the regular outreach significantly affect the vulnerability of the sector. Moreover, the regular review of the prudential and AML regulations to address supervisory gaps and to be consistent with the international standards aims to further strengthen the corporate governance structure of MSB and to maintain an effective AML/CTF compliance framework.

While regulatory controls are effective mechanisms, they are confronted with limited enforcement powers due to organizational and operational challenges, such as lack of manpower complement, and enabling law providing authority to the BSP to impose administrative sanctions on unregistered MSBs.

Considering the inherent risk and the availability of controls, the level of vulnerability risk of MSBs has improved from the Second NRA but remains within the **medium high** level.

As for consequential risk, the two MSBs involved in the cases raised several concerns in the entire MSB sector, further exposing the vulnerabilities to ML and TF. These incidents also caused additional scrutiny and imposition of stricter controls from the international community on the sector.

Considering the foregoing, **the overall ML/TF risk of MSBs is medium high**, with the primary focus on TF. A collective mitigating strategic actions or a whole-of-government approach should be implemented from short to medium term. Moreover, regulators or supervising agencies need to determine all associated risks and apply risk-based supervision. MSBs and other financial institutions must likewise re-assess their risk procedures and customer and geographical profiling; and apply commensurate customer due diligence measures to existing and emerging vulnerabilities to ML/TF.

GENERAL FINDINGS AND CONCLUSION

Based on quantitative and qualitative assessments, the following risks and gaps exist in the sector:

1. MSBs appear as the preferred channel to facilitate proceeds of crime, particularly fraud, SRC violations, child exploitation, TIP, drug trafficking, terrorism, and TF. Criminals exploit MSBs due to the wide reach, speed, and anonymity characteristics.

2. The financial transaction trend shows usual transactions of criminals/suspects below PhP5,000, which is around 46% of the STR data set. This is consistent with the criminal trend in ST reporting, where transactions involving SRC violations, fraud/swindling, child

exploitation, child pornography, TIP, terrorism, and TF ranged between PhP500 and PhP5,000.

3. Suspicious cash-based transactions are also prevalent within the sector, with an estimated STR value of PhP5.12 billion. This accounts for 31% of the total estimated value of the STRs used in the study. Cash poses a threat, as it conceals the source of funds, thus making it difficult to determine the nexus of the source of cash and the unlawful activity.

4. Emerging threats on the use virtual currency and/or cryptocurrency are likewise observed. While only four RTC-VCs reported 35,846 STRs, the estimated STR value is substantial at PhP2.3 billion. Most of the filed STRs were predicated on fraud/swindling and SRC violations.

5. Drug traffickers exploit the MSB sector to facilitate illicit proceeds, based on case investigations. In 2020 alone, 11 MSBs figured in the four cases investigated for illegal drugs. Estimated value of assets/proceeds frozen from these cases totaled PhP257.15 million.

6. The characteristics of MSB transactions, such as frequency of transactions and small values of remittances or wire transfers, present challenges to the covered persons in detecting suspicious transactions.

7. MSB products or services offered through agents or through non-face-to-face appear to pose higher risks as these may entail difficulty in identifying owners or beneficial owners and transactors of the accounts.

8. While the BSP and the AMLC are continually developing means to effectively monitor MSBs' compliance with regulatory and AML/CTF requirements, supervisory challenges are still present due to the large number of offices/branches and small MSB players.

9. There are challenges in ST reporting, as reporting is concentrated at head office level. Branch level reporting is essential in determining actual occurrence or location of transactors. Moreover, a considerable number of STRs have incomplete or lacking subjects' and counterparties' addresses. This presents financial intelligence and law enforcement concerns in determining the locations of potential subjects/persons of interest and criminal activities.

10. The limited action on identifying unregulated MSBs allows criminals to further their illicit activities. In some anecdotal reports, criminals create or employ unregistered MSBs to facilitate the movement of proceeds.

RECOMMENDATIONS AND MITIGATION STRATEGY

To mitigate the emerging threats and vulnerabilities based on the results of this risk assessment, the following strategies may be considered or implemented:

Enhance regulatory controls

1. The AMLC and BSP must re-evaluate supervisory policies and enhance reportorial and registration requirements. The AMLC and BSP may also need to maintain a database of MSBs and their branches and officers with derogatory records and non-compliance issues with existing laws and regulations. Further, the AMLC and BSP should generate better data collection through public and private sector efforts.

   The AMLC and BSP, subject to data privacy provisions or any information-sharing agreement, may grant access to law enforcement agencies and other competent authorities to support parallel investigations on ML/TF and predicate crimes.

2. The BSP should continue to strengthen its conduct of onsite/offsite examinations of MSBs. Challenges presented can be addressed by assessing the manpower complement and applying risk-based prioritization of MSBs.

3. Gaps still exist in identification of suspicious trends of other high-risk crimes. Although MSBs proactively report on certain crimes due to the sharing of studies of the AMLC, the AMLC and BSP should still regularly conduct AML/CTF registration and reporting, and typology seminars to assist the MSB sector in identifying high-risk suspicious transactions.

4. The AMLC, BSP, Department of Interior and Local Government (DILG), and municipal governments should work closely to reduce regulatory uncertainties and to provide clear guidelines to MSBs and other financial institutions. MSBs should increase their efforts in implementing and demonstrating effective compliance systems.

Promote effective coordination mechanisms and enhance enforcement actions

5. The BSP and AMLC should further enhance coordination with covered persons and other law enforcement agencies to more effectively address risks associated with MSBs.

   a. The BSP and AMLC can utilize the National AML/CTF Coordinating Committee and National Law Enforcement Agency Coordinating Committee, including their sub-committees, in proposing action plans and implementing the same to mitigate risks associated with MSBs.

   b. The AMLC should continue its regular quarterly meetings with MSBs (through the Association of Remittance Company Compliance Officers) and consider expanding the network to other industry associations. The AMLC should likewise continue to

operationalize its Public-Private Partnership Program (PPPP) and promote effective intelligence information-sharing.

c. The AMLC, BSP, and other MSB industry associations should also encourage other MSBs to participate and enter into membership with the industry associations.

d. The BSP and AMLC should monitor the implementation and compliance of financial institutions with the BSP Memorandum[10] on applying appropriate diligence when dealing with MSBs classified as high-risk.

6. The BSP should maximize its engagement with the DILG and local government units to identify unregistered MSBs and to ensure protection to the public and consumers against illicit activities posed by illegal MSBs.

7. The BSP, AMLC, and DILG must continuously update and determine all emerging risks associated with MSBs.

   a. Supervising agencies (BSP and AMLC) should monitor transactions, particularly on MSBs located in high-risk areas.

   b. The BSP and local government units may need to revisit regulations on the conduct of fit and proper screening as certain types of MSBs can be exploited for criminal activities.

8. There is a need for a better cooperation among the BSP, AMLC, DILG, and the MSB sector to prevent funds/money from going to criminals/launderers, while allowing money to flow efficiently to support financial inclusivity for all consumers.

Enhance understanding on money laundering/terrorism financing risks

9. The AMLC and BSP must conduct massive awareness campaigns and AML/CTF trainings to MSBs, particularly those in high-risk areas, and raise awareness of potential risks and sanctions. In this manner, MSBs improve their risk understanding, reporting compliance, and KYC/CDD procedures.

10. The AMLC and BSP should issue regular reports on typologies and ML/TF indicators for the guidance of MSBs, other covered persons, and the public.

    The AMLC and BSP should continue to further their analysis and understanding of overseas trends and include the same in information-sharing with the covered persons as well as

[10] Memorandum No. M-2019-029 on 12 December 2019 amending Memorandum No. 2016-004 on the Reminder on Sound Risk Management Practices in Dealing with FXD/MC/RTC.

with global AML/CTF authorities and supervisor partners (i.e., foreign financial intelligence units and central banks).

11. The BSP may conduct or update its own sectoral risk assessments, integrating emerging threats faced by MSBs and cross-sector threats to other financial institutions.

12. The AMLC should disseminate the study to the supervising agencies, appropriate and relevant government agencies, PPPP-information sharing partners, and law enforcement authorities.

----------END----------