



BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR
FINANCIAL SUPERVISION SECTOR

MEMORANDUM NO. M-2021-005

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

Subject : **Report on the Risk Assessment of Cash, Cross-Border, and Cross-Sector Transactions**

The Monetary Board, in its Resolution No. 20 dated 7 January 2021, approved the attached report on money laundering (ML)/terrorist financing (TF)/proliferation financing (PF) risk assessment of cash, cross-border, and cross-sector transactions of 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 report on risk assessment of cash, cross-border, and cross-sector transactions is part of the broader sectoral risk assessment (SRA) being conducted by the Bangko Sentral. It represents the first phase of the SRA that focused on the assessment of risks attendant to cash, cross-border, and cross-sector transactions. The assessment seeks to understand, analyze, and assess the ML/TF/PF risks arising from cash transactions of banks and other BSFIs, the flow of suspected criminal proceeds through cross-border transactions, and the risks across certain sectors.

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: 2021.01.13
21:02:44 +08'00'

CHUCHI G. FONACIER
Deputy Governor

13 January 2021

Att: a/s

¹ Other BSFIs include non-bank financial institutions (NBFIs) namely, trust entities, non-stock savings and loan associations (NSSLAs), money service businesses, non-bank electronic money (e-money) issuers (EMIs), virtual currency exchanges (VCEs)/virtual assets service providers (VASP), pawnshops and operators of payment systems.



BANGKO SENTRAL NG PILIPINAS

**RISK ASSESSMENT OF
CASH, CROSS-BORDER
AND CROSS-SECTOR
TRANSACTIONS**

January 2021

TABLE OF CONTENTS

RISK ASSESSMENT OF CASH, CROSS-BORDER, AND CROSS-SECTOR TRANSACTIONS.....	1
ASSESSMENT METHODOLOGY AND DATA COLLECTION.....	1
THE PHILIPPINE FINANCIAL SYSTEM	2
1 CASH TRANSACTIONS ASSESSMENT	2
Level and Extent of use of Cash Transactions.....	3
Threat Assessment	3
Vulnerability Assessment.....	6
2 CROSS-BORDER TRANSACTIONS.....	7
Threat Environment.....	7
Vulnerability Assessment	10
3 CROSS-SECTOR ASSESSMENT	11
Threat Environment	11
Typologies on ML/TF and related Predicate Offenses	12
STR Statistics	14
Sectoral Threat and Vulnerability Assessment.....	15
CONSEQUENCE	16

RISK ASSESSMENT OF CASH, CROSS-BORDER, AND CROSS-SECTOR TRANSACTIONS

This report provides the key results of the money laundering (ML), terrorist financing (TF), and proliferation financing (PF) risk assessment relating to cash, cross-border, and cross-sector transactions of banks and other BSP-supervised financial institutions¹ (BSFIs). This exercise is part of the broader sectoral risk assessment (SRA) being conducted by the BSP. The SRA aims to identify and update the assessment of the level of ML/TF/PF risks in the sectors supervised by the BSP based on current risk and context information. The results of the SRA will inform the supervision strategies and priorities of the Bangko Sentral as well as the implementation of the enforcement actions.

The report represents the first phase of the SRA² that focused on the assessment of risks attendant to cash, cross-border, and cross-sector transactions. The assessment seeks to understand, analyze, and assess the ML/TF/PF risks arising from cash transactions of banks and other BSFIs, the flow of suspected criminal proceeds through cross-border transactions, and the risks across certain sectors³.

ASSESSMENT METHODOLOGY AND DATA COLLECTION

The methodology adopted for the SRA, including for cash, cross-border and cross-sector assessment, is largely shaped by the Financial Action Task Force (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. This assessment involved using informed judgment considering the risk and context information of the Philippines, pertinent anti-money laundering/countering the financing of terrorism (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. A structured questionnaire was used to gather relevant AML/CFT information from BSFIs. Focus group discussions and presentations from select BSFIs likewise formed part of this assessment.

¹ Other BSFIs include non-bank financial institutions (NBFIs) namely, trust entities, non-stock savings and loan associations (NSSLAs), money service businesses (MSBs), non-bank electronic money issuers (EMIs), virtual currency exchanges (VCEs)/virtual assets service providers (VASPs), pawnshops and operators of payment systems

² Phase 2 covers the overall results of the SRA

³ The use of more than one covered persons within a particular sector or across various sectors such as banks, MSBs, NBFIs (such as investment house, securities brokers/dealers, insurance companies/ brokers/ dealers) as well as designated non-financial businesses and professions (such as casinos, lawyers, accountants, company service providers) in laundering and layering the proceeds of crimes.

- **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, covered transaction reports (CTRs) and suspicious transaction reports (STRs) statistics, typologies, investigation reports, and ML/TF cases provided by the Anti-Money Laundering Council Secretariat (AMLCS), as well as available strategic AML/CFT studies.

THE PHILIPPINE FINANCIAL SYSTEM

The Philippine Financial System’s total resources as of 30 June 2020 amounted to PhP23.15 trillion,⁴ of which, PhP19.09 trillion or 82.5 percent is attributed to the banking sector. The banking sector’s assets represented 98.8 percent of the country’s nominal gross domestic product (GDP). This was mainly due to expansion of funds channeled to lending activities. Funding was principally sourced from deposits, bond issuances, and capital infusion. Universal and Commercial Banks (UB/KBs) held the largest share of the banking system’s total assets at 92.6 percent while Thrift Banks (TBs) and Rural and Cooperative Banks (RCBs) comprised 6.0 percent and 1.4 percent, respectively⁵. The remaining PhP4.05 trillion or 17.5 percent of the financial system’s resources is attributed to non-bank financial institutions (NBFIs). As of 30 June 2020, there are 1,250 NBFIs with 13,589 branches, and one (1) offshore banking unit.

1 CASH TRANSACTIONS ASSESSMENT

- 1.1 Cash has been an attractive medium for ML primarily because of its fungible character that is interchangeable with another thing of value and leave little to no evidence trail. Thus, tracing the source of criminal proceeds would be very difficult for the authorities.
- 1.2 The Philippine economy is largely cash-based. According to the Philippines Digital Economic Report 2020, cash is the main medium of exchange in the Philippines despite its handling and safekeeping costs⁶. The BSP-accounted total peso notes and coins in circulation as of December 2019 amounted to PhP1.40 Trillion⁷, which is 7.17 percent⁸ of the GDP.
- 1.3 Nonetheless, the massive use of the internet and proliferation of financial technology innovations are accelerating the shift towards a cash-lite economy. Thus, the BSP’s Digital Transformation Roadmap for 2020-2023 aims to convert 50 percent of the total volume of retail payments into digital form⁹. In 2020, the country experienced rapid growth in digital

⁴ <https://www.bsp.gov.ph/SitePages/Statistics/StatisticsMetadataDisp.aspx?ItemId=11>

⁵ Report on the Philippine Financial System – First Semester 2020

⁶ <https://openknowledge.worldbank.org/handle/10986/34606>

⁷ [https://www.bsp.gov.ph/Statistics/Financial%20System%20Accounts/dcs.aspx /](https://www.bsp.gov.ph/Statistics/Financial%20System%20Accounts/dcs.aspx/)

⁸ Based on PhP19.516 Trillion GDP (<https://www.bsp.gov.ph/Statistics/keystat/sefi.pdf>)

⁹ https://www.bsp.gov.ph/Media_And_Research/Primers%20Faqs/Digital%20Payments%20Transformation%20Roadmap%20Report.pdf

payments due to the limited mobility amid the pandemic. The volume of PESONet and InstaPay (under the National Retail Payments System) transactions increased exponentially. For the first eight months of 2020, the value of InstaPay rose to almost 400 percent, while that of PESONet hiked by 100 percent year-on-year.¹⁰

Level and Extent of use of Cash Transactions

1.4 *Cash transactions ranked third in terms of value.* Based on the CTRs, cash transactions¹¹ amounted to PhP171.06 trillion, or 20.07 percent of the total value of all CTRs (Figure 1). These transactions ranked 3rd, next to wire transfers (PhP334.75 trillion) and check transactions (PhP284.01 trillion) and involved 32.19 million cash-related covered transactions processed by BSFIs.

1.5 *Half of low value STRs involved cash transactions.* STR analysis disclosed that 51.45 percent (as to value) and 30.70 percent (as to volume) of STRs involving amount of PhP500,000 and below are cash transactions. High value transactions are mostly done through checks and wire transfers.

1.6 *Cash transactions mainly involved current and savings deposits.* These represent 64.37 percent of the CTRs or PhP110.11 trillion (Figure 2). Cash inflows and outflows amounted to PhP90.94 trillion and PhP72.02 trillion, respectively.¹²

Figure 1. Transaction Types (Value in Trillions)

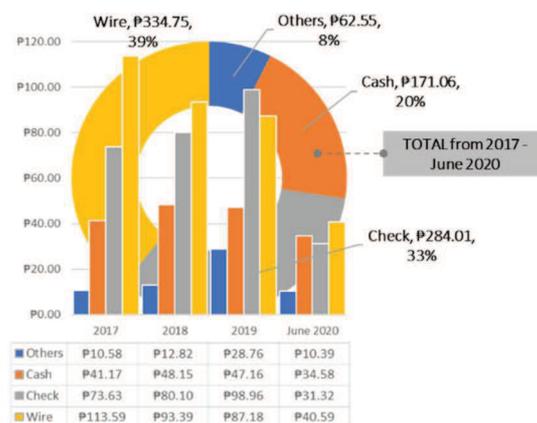
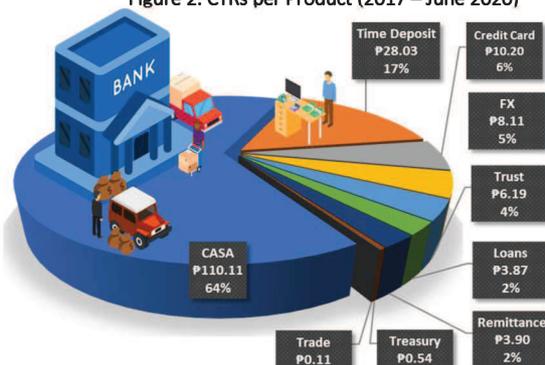


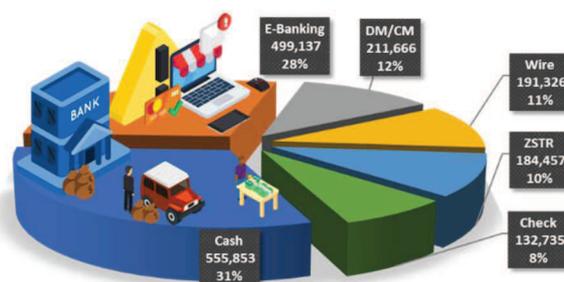
Figure 2. CTRs per Product (2017 – June 2020)



Threat Assessment

1.7 *The level of threat arising from cash transactions is high.* Criminals continue to use cash-based transactions to move illicit funds into and out of the financial system. Based on the number of STRs, cash transactions ranked first followed by electronic banking (Figure 3). These involved

Figure 3. STRs per Medium in Terms of Volume (2017 – June 2020)



¹⁰ Ibid

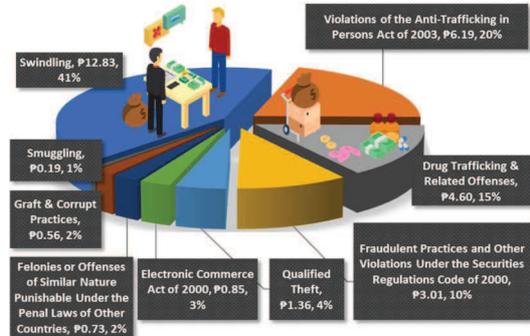
¹¹ This involves 84 cash-based transaction codes in the CTR.

¹² Excludes foreign currency buy and sell transactions

deposits to and withdrawals from savings or current accounts, termination of time deposits, and over-the-counter check encashments, among others.

1.8 *Swindling ranks first (at 41 percent), in terms of value, based on STRs involving cash transactions.* This was followed by trafficking in persons (TIP) (20 percent) and drug trafficking (15 percent) (Figure 4). Swindling cases mostly involved cash and check transactions. Sample typologies on these crimes using cash-based financial transactions are shown below.

Figure 4. Top Predicate Crimes in Terms of Value (in Billions) (2017 – June 2020)



Case 1. Community Ministry Case - Large and Multiple Cash Deposits of varying amounts several times a week funneled into the accounts of businesses registered under the name of relatives and close associates. (2017 to 2019)

A corporation registered with the Securities and Exchange Commission (SEC) conducts investment taking activity without authority. It recruited investors for as low as PhP10,000 with a promise that the investment will grow 30 percent per month for life. Some investments reached up to PhP2.0 million.



Funds were funneled into accounts of businesses registered under the name of the leader's immediate family and their close associates. These include a **large cash deposit of PhP25.0 million** without supporting documents and inconsistent with the expected transactions.



There were also bulk of **cash deposits of varying amounts several times a week** during the height of the solicitation activity. These funds were used to acquire and operate the businesses registered under the name of the leader and his wife. **Estimated cash amount in 50 bank accounts in 9 banks subject to freeze order amounted to PhP149.0 million.**

Case 2. Online Sexual Exploitation Case (2017)



Mr. B is an Australian national and a retired teacher. He resides in an upscale village in Iloilo. The subject's transactions involve a pattern of remittances, sending small amounts to 12 different female individuals over the course of 15 months, from June 2017 to August 2018. The remittances were claimed at different payout locations in Metro Manila, Davao, Iloilo, and Iligan.



In total, there were 42 remittance transactions amounting to PhP165,150, ranging from PhP900 to PhP40,000, and averaging PhP3,900. The customer identification documents show that the male foreign sender has no apparent ethnic or familial relationship with the multiple female beneficiaries.

Case 3. Drug Smuggling Case – Large and multiple cash deposits with inter-account transfers from different persons related to online gaming business. (2017)



A consultancy entity (Company A) facilitates immigration requirements of foreign clients, such as nationals of Country C. Company A is owned by one of the accused middlemen of a businessman (a national of Country C) involved in the PhP6.4 billion shipment of illegal drugs discovered by Bureau of Customs in 2017 based on an information from the Anti-Smuggling Bureau of the Country C.

Company A's transactions in one bank include cash deposits amounting to PhP399.51 million, check deposits of PhP8.67 million and inter-account transfers from at least 38 different senders who are related to online gaming business amounting to PhP245.29 million.



Case 4. Cash structuring case involving construction supplier– Multiple cash deposits with a little less than CTR amount (structuring); and corresponding cash withdrawal in more or less the same amount. (2017)

In October 2017, Anti-Narcotics agents arrested Mr. RB in Mindanao. The authorities recovered 9 packs of suspected shabu weighing around 45 grams and worth about PhP270,000, and a 9mm caliber pistol, a hand grenade and bullets. Identified bank transactions of Mr. RB and his wife include 139 transactions from December 2009 to September 2012 totaling PhP63.52 million which are not commensurate with their declared business or source of funds as construction supplier. Transactions include 79 cash deposits with an average of PhP423,462 (below the CTR threshold of PhP500,000) and with an aggregate value of PhP33.45 million. It also includes 60 over-the-counter cash withdrawals with an average of PhP501,149 and a total of PhP30.07 million.

Case 5. Islamic State of Iraq and Syria (ISIS) - Connected Case – Frequent cash deposits with large check encashment; and company managed by identified ISIS member. (2017 – 2018)

There were reports linking an arrested Kuwaiti national, suspected to be a member of the ISIS, to 8QW, a firm that once monopolized the provision of medical services to Overseas Filipino Workers (OFWs). 8QW's scheme enables it to earn PhP5 million to PhP6 million daily from OFWs by collecting PhP5,480. The operations manager of 8QW, Mr. HD, a Kuwaiti national, was reportedly part of ISIS and he had the same address with 8QW.



Identified transactions in one bank include a **large check encashment of PhP64 million in 2018 and multiple and frequent cash deposits of the same exact amount** and various check disbursements from 2017 to 2018.

Case 6. Possible bulk cash smuggling using banks and cruise ship (2019)

A land-based hotel and casino requested its bank to pick-up cash (via deposit pick-up arrangement or DPA) amounting to HKD74 million (PhP370 million) from a cruise ship docked at a Philippine port. The cash will be deposited in HKD account maintained in the bank. The amount involved is above the average daily HKD volume of the client [HKD 600,000 (PhP3 million)]. The client could not present any document as proof of source of funds and the amount was considered to deviate from the client's past transactions.

Vulnerability Assessment

1.9 *Inherent vulnerability of cash transactions to ML/TF/PF is high.* Cash remains widely used for banking transactions. About PhP169.84 trillion or 99.28 percent of cash-based covered transactions were from banks, with the rest reported by NBFIs. UBs reported the highest number of cash transactions processed at an average of 85.89 percent of the total, which is equivalent to PhP116.37 trillion from 2017-2019. Cash transactions are mostly used in the placement stage when funds are introduced in the financial system usually through deposits to accounts. Therefore, savings and current accounts have heightened vulnerability.

1.10 *ML/TF/PF risks controls.* BSFIs have adopted controls as part of their ML/TF/PF risk management framework to prevent cases of them being used as conduits of proceeds of illegal activities. These include the adoption of, among others, cash-related control measures such as:

Measure	Description
Customer Due Diligence	Identifying and verifying customers and the beneficial owners, including the conduct of on-going due diligence
Cash Transaction Limits	Using cash transaction thresholds to help identify and deter cash abuse, to complement covered and suspicious transaction reporting
AML/CFT Transaction Monitoring	Implementing a system to monitor customer's transactions and ensuring that these are commensurate with their declared financial profile
Suspicious Transaction Reporting	Identifying, investigating, and reporting suspicious transactions to AMLC

Considering the inherent vulnerability and the level of use of cash, as well as the existing mitigating cash controls, overall vulnerability is assessed as **Medium**.

1.11 *Scope for enhancement.* The above control measures may be further enhanced to reduce risks arising from cash-based transactions by: (a) strengthening customer verification procedures especially for those transacting in large amounts; (b) conducting periodic review of AML system capabilities and thresholds to ensure that these are relevant and suited to the BSFI's risk profile; (c) adopting risk-based prioritization to focus on high risk alerts such as those involving cash transactions; and (d) consistently implementing cash transaction limits.

1.12 Net risk rating for cash transactions is **Medium High**.

2 CROSS-BORDER TRANSACTIONS

2.1 *Remittances, trade, and investments.* Cross-border transactions generally involve remittances from OFWs, payments for trade transactions, and investments. From 2017-2019, total OFW remittances amounted to USD87.13 billion, while total exports and imports of goods stood at USD157.27 billion and USD297.77 billion, respectively.¹³ Top source and/or destination countries are United States of America (USA), Japan, China and Singapore. Payments for these transactions are primarily coursed through banks.

Figure 5. Remittance, Trade, and Investments
(Value in Billion USD)



On another note, the CTRs disclosed the following cross-border transactions (*based on relevant transaction codes*): (amounts in billion PhP)

Channel	Remittances ¹⁴		Trade		Investments	
	Inflows	Outflows	Inflows	Outflows	Inflows	Outflows
Bank	28,825.67	29,924.59	614.61	4,474.78	439.81	424.28
MSB	10.72	650.69	-	-	-	-
Total	28,836.39	30,575.28	614.61	4,474.78	439.81	424.28

Threat Environment

2.2 The exposure to use and abuse of cross-border transactions for ML/TF/PF activities is **high**.

2.3 In 2019, the AMLC released the report “A Risk Assessment on the Philippines’ Exposure to External Threats based on Submitted STRs”¹⁵. Key findings include:

- Illicit funding generated from (1) violation of environmental laws, (2) illegal trafficking of persons, (3) kidnapping for ransom (KFR), and (4) terrorism and conspiracy to commit terrorism, entered the Philippines.
- As to volume of STRs, majority of the inflows and outflows of the predicate crimes have been linked to the USA. As to value, majority of the incoming criminal proceeds were coursed through various banks in the United Kingdom (UK), while large amounts of outgoing illicit funds were mostly sent to Hong Kong.
- Majority of the predicate crimes such as illegal drugs, plunder and corruption, investment scams and estafa, smuggling, intellectual property rights violation, illegal manufacturing and possession of firearms, and web-related crimes use UB/KBs.

¹³ <https://www.bsp.gov.ph/Statistics/keystat/sefi.pdf>

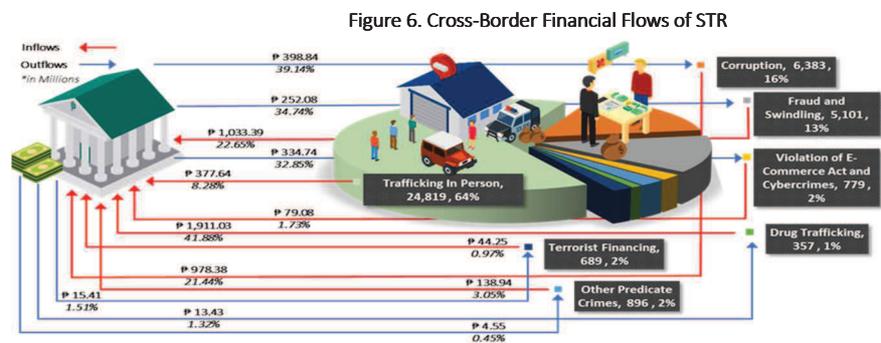
¹⁴ Includes all types of international remittances coursed through banks or their correspondent banks

¹⁵ <http://www.amlc.gov.ph/images/PDFs/AMLC%20EXTERNAL%20THREATS%20STUDY.pdf>

2.4 Estimate of criminal proceeds laundered globally per year is from USD800 billion to USD2 trillion¹⁶ or from PhP40 to PhP100 trillion. In the Philippines, estimates of criminal proceeds include: (a) PhP670 billion to PhP752 billion¹⁷ for corruption; (b) PhP11 billion¹⁸ for drug trafficking (for first half of 2020 only); (c) PhP100 billion¹⁹ for smuggling; (d) PhP31.9 billion²⁰ for intellectual property violations; (e) PhP50 billion²¹ for environmental crimes; and (f) PhP75 billion²² for tax evasion.

2.5 The 2019 Philippines Mutual Evaluation Report (MER) cited that the geographical landscape and vast maritime borders and seaports make the Philippines susceptible to smuggling of illicit goods and cash, trafficking of persons, and other cross-border issues.²³ Attention should be given to transnational movement of criminal proceeds and funds used for foreign terrorist fighters.

2.6 *Top crimes.* STRs disclosed 39,024 reports involving cross-border transactions. These included suspected illicit fund inflows of PhP4.56 billion and outflows of PhP1.02 billion, majority of which were reported by banks (93.2 percent). In terms of number of suspicious incidents reported, *TIP*, *corruption*, *fraud* and *swindling* are the most prevalent. As to values involved, major crimes are *drug trafficking*, *fraud/swindling*, *corruption*, and *TIP* (Figure 6).



a. **Drug Trafficking.** Less than one percent of the inflows of PhP1.91 billion were traced to be subsequently sent to various foreign jurisdictions, leaving 99 percent of said amount in the country or possibly leaving the country through other avenues.

Case: 51 STRs involving identified drug traffickers involved inward remittances from Australia, Germany, UK, Hong Kong, Singapore, and USA totaling PhP1.82 billion. Two outward remittances were observed going to Liechtenstein in the total amount of PhP8.86 million.

¹⁶ <https://www.unodc.org/unodc/en/money-laundering/globalization.html>.
¹⁷ <https://cnnphilippines.com/news/2019/8/16/Government-corruption-loss-deputy-ombudsman-Cyril-Ramos.html?fbclid=IwAR2OQ90yWJXFHgar4ID17irm9FsuzE6--DirV0A1PmTn9fM3YHtxripGx8>.
¹⁸ <https://www.pna.gov.ph/articles/1108055>.
¹⁹ <http://www.fpi.ph/fpi.cms/Research/uploads/Addressing%20Smuggling%20in%20the%20Philippines.pdf>
²⁰ 2019 Serious and Organized Crime Threat Assessment (SOCTA).
²¹ <https://www.adb.org/publications/addressing-illegal-wildlife-trade-philippines>.
²² <https://www.bir.gov.ph/index.php/transparency/bir-annual-report.html>.
²³ 2019 Philippines MER. Par. 9, page 21

- b. **Fraud and Swindling.** Suspected criminal proceeds primarily came from UK and USA and about 13 percent thereof returned to said countries. Of the PhP1.03 billion involved, 24 percent were traced as being sent abroad through banks.
- c. **Corruption.** Out of the PhP978.38 million suspected criminal proceeds linked to corruption, 40 percent were traced to be sent abroad. For suspected criminal proceeds from Singapore, the Philippines appears to have served as mere transshipment point since 58 percent of inflows were also remitted back to Singapore.
- d. **TIP.** Suspected criminal proceeds related to TIP²⁴ originated from Belgium and USA, among others. The Philippines appeared to be the final destination of suspected criminal proceeds from this crime group with proceeds of PhP377.64 million.

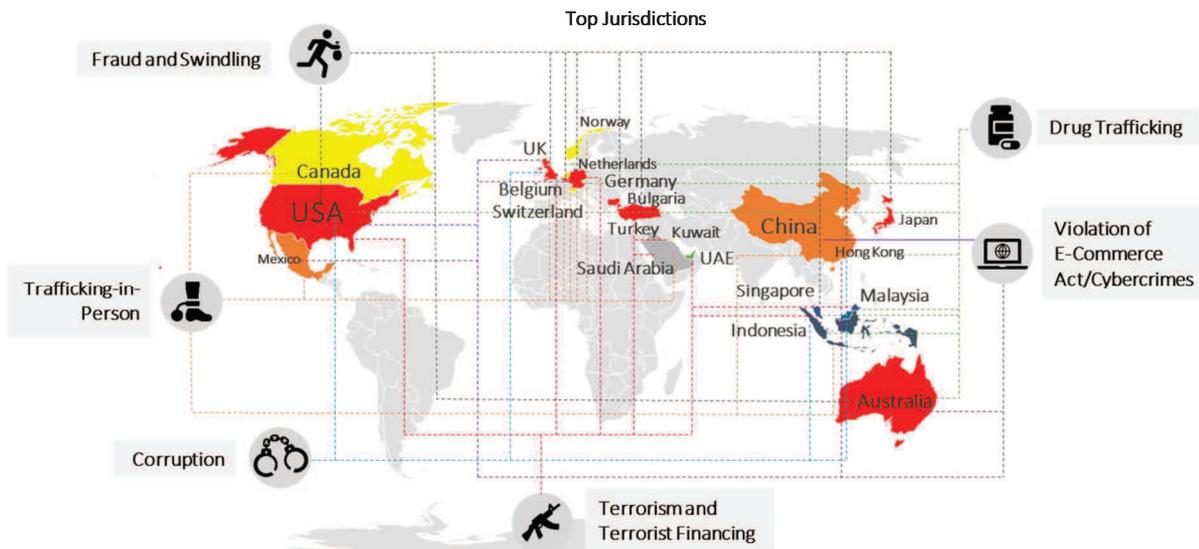
Case: Seven STRs reported an account used to pay out women for voyeurism and production of sex videos. The account was funded by inward remittances from Belgium aggregating PhP163.89 million.

- e. **Violation of e-Commerce Act and Cybercrimes.** Data showed that suspected criminal proceeds were either generated within the country and sent primarily to the USA, Hong Kong, Mexico, and UK, or the Philippines only served as a transshipment point. About 24 percent of the suspected illicit inward financial flow of PhP334.74 million principally came from USA and UK.

2.7 *ML/TF Financial Investigations.* ML and TF investigations conducted in coordination with various foreign jurisdictions consisted of 470 requests for information (RFI) and spontaneous disclosures through the Egmont Secured Web (ESW) and Mutual Legal Assistance (MLA). These involved PhP881.54 billion estimated suspected criminal proceeds. In terms of number of information-sharing done, *TIP, fraud and swindling, and terrorism and TF* ranked as the most prevalent crimes. Most of the suspected criminal proceeds investigated in the ESW and MLA requests were linked to fraud and swindling (97.8 percent).

2.8 In total, as to origin of suspected criminal proceeds, Australia, Germany, Singapore, UK, and USA are the top countries. Top destinations of suspected illicit funds are Hong Kong, Singapore, and USA. Meanwhile, Germany, Isle of Man, and UK were identified in relation to forgeries, qualified theft, and KFR, respectively. For major crimes involved in cross-border transactions, the top foreign jurisdictions observed to be the sources or destinations of suspected criminal proceeds are the following:

²⁴ TIP as a crime group, includes trafficking-in-persons under R.A. No. 9208, child abuse and exploitation under R.A. No. 7610, child pornography under R.A. No. 9775, and photo voyeurism under R.A. No. 9995.



Vulnerability Assessment

2.9 *Financial Services Used.* Banking services commonly used in cross-border transactions are international wire transfers/remittances and trade finance which were usually coursed through correspondent banking as well as private banking and wealth management. In addition, the use of virtual currencies in illicit transactions, primarily in international drug trafficking and payment for contraband items pose serious concerns to the law enforcement agencies (LEAs)²⁵. Moreover, the LEAs discovered a pyramiding scheme using bitcoins and a virtual currency exchange platform as a channel to accept investments and disburse interest payments. Smugglers also utilize paperless transactions and cryptocurrencies to facilitate smuggling and avoid being tracked by the authorities.²⁶

2.10 *AML/CFT Controls and Measures.* Cognizant of the material risks arising from cross-border transactions, BSFIs implemented several preventive measures commensurate with the inherent risks posed by their products and services with cross-border elements. Measures include the conduct of customer due diligence upon on-boarding as their first line of defense, customer and transactional sanctions screening and on-going monitoring/alerts management, and suspicious transaction reporting. The vulnerability of cross-border transactions is assessed as **Medium**.

Scope for enhancement. Given the evolving nature of cross-border crimes and financial transactions, there is a continuing need to strengthen measures to proactively identify suspicious cross-border transactions, particularly in the areas of ongoing transaction monitoring, sanctions screening, and suspicious transaction reporting.

2.11 Overall, the ML/TF risk of cross-border transactions is **Medium High**.

²⁵ 2019 SOCTA.

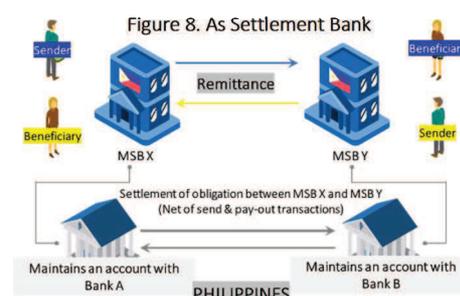
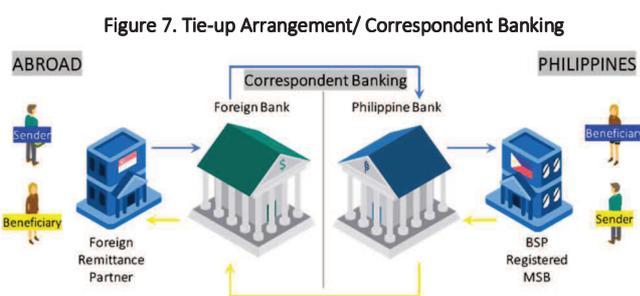
²⁶ *Ibid.*

3 CROSS-SECTOR ASSESSMENT

3.1 The banking sector is at the core of the Philippine financial system. It serves as the clearing and settlement²⁷ point of all financial transactions. The deposit accounts maintained in banks serve as the linkage of the different sectors. Movement of funds to and from the other sectors can be done through, among others, wire/fund transfers and check clearing.



3.2 Meanwhile, MSBs also play an integral part in the movement of funds from one sector to the other through the remittance facility. MSBs enter into tie-up arrangements with banks and other MSBs to facilitate transfer of funds or distribute remittances within and outside the country. The usual arrangements between banks and MSBs are described below:



Threat Environment

3.3 There is a **high level** of cross-sector transactions (within the Philippines) between (a) banks and other sectors such as MSBs, Securities and Exchange Commission (SEC)-regulated entities (e.g., brokers), and designated non-financial businesses and professions (DNFBP) (e.g., casino, lawyer, jewelry dealers); and (b) MSBs, including VASPs, with other sectors such as DNFBPs.

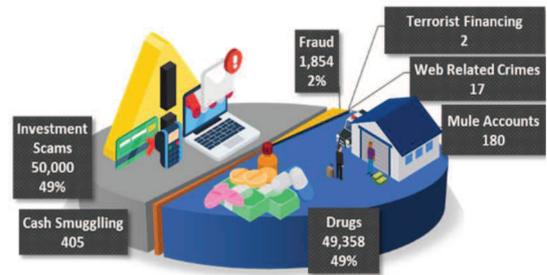
3.4 Typologies and cases analyzed disclosed that 14 out of 22 instances that involved around PHP102.0 billion possible proceeds of crimes had cross-sector element.

²⁷ 2017 Financial Stability Report, BSP

3.5 These crimes include *investment scams, drugs and related offenses, fraud, cash smuggling, use of mule accounts, web-related crimes, and TF.* (Figure 9)

3.6 Proceeds of these crimes were funneled and layered using several sectors. The sectoral transactions mainly used deposit accounts maintained in banks, wire transfers, and funds in electronic money (e-money) accounts.

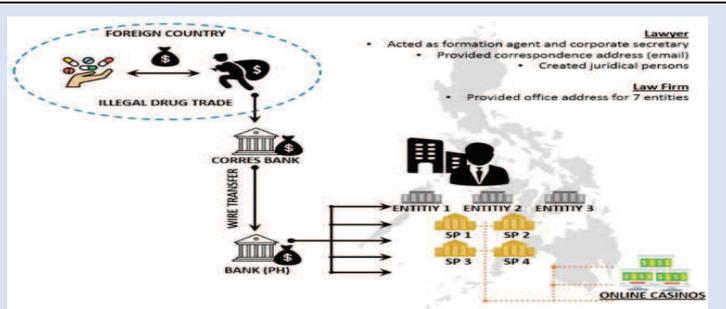
Figure 9. Top Crimes Based on Value (in Millions PhP)



Typologies on ML/TF and related Predicate Offenses

a. Drug trafficking and related offenses. Company service providers (CSPs) were used in setting up entities alleged to have received funds from drug trafficking through banks.

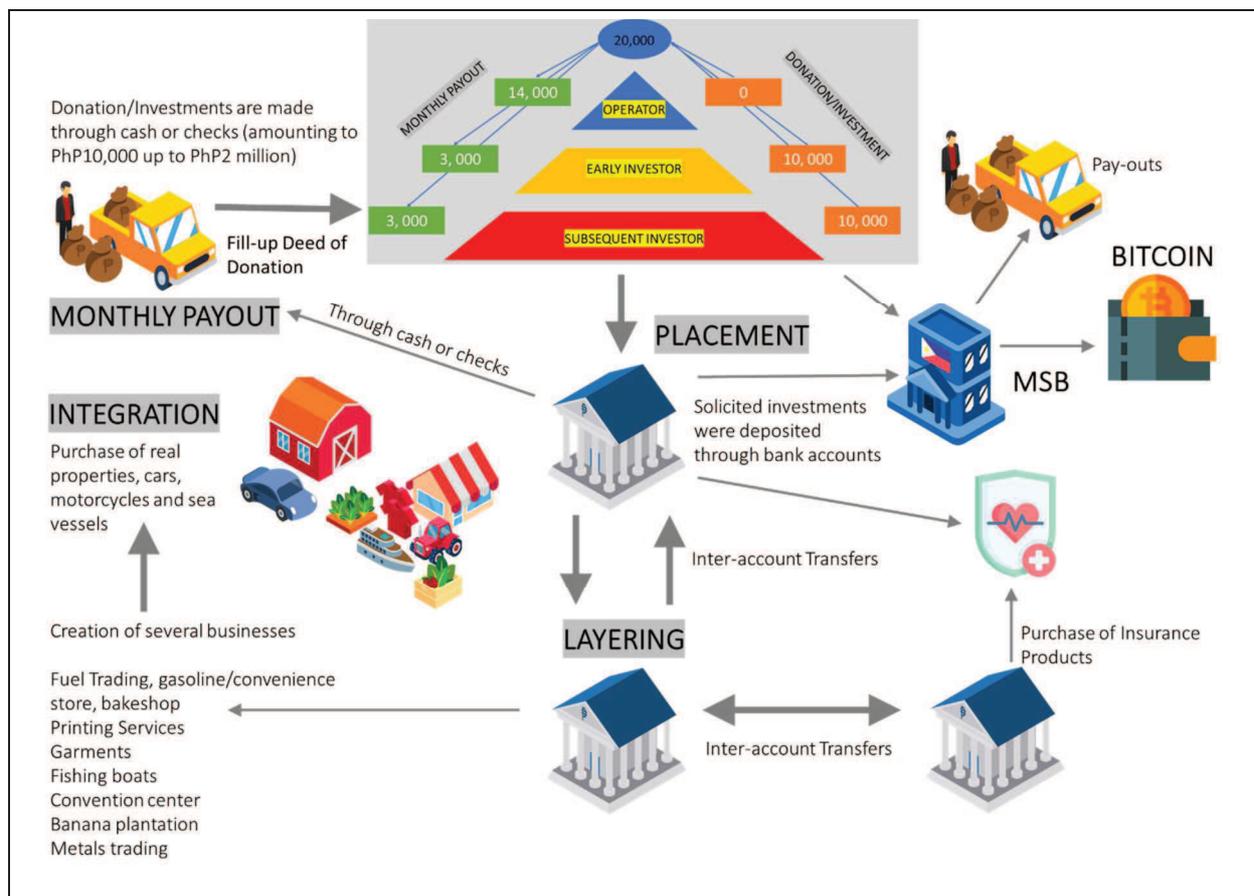
Case: *International inward remittances of around PhP1.77 billion were alleged to be proceeds of illegal drug trafficking abroad. These were received through banks by several beneficiary-entities in the Philippines. Said beneficiaries are service providers of e-casinos, in which the company registration was facilitated and business address provided by a certain Filipino lawyer and a law firm. (2018)*



b. Investment fraud. In 2020, there were 115 investment frauds²⁸ recorded by the SEC. Banks reported a total of 5,878 STRs related to PONZI Schemes and 112,766 STRs on unlicensed investment companies. Based on cases analyzed, proceeds related to investment scams are usually funneled through deposit accounts. Some funds were used to buy real estate properties and insurance policies. Certain typologies also involved the use of MSBs and VASPs to facilitate their transactions.

²⁸ SEC Advisories (January – September 2020)

Case 1. Banks vis-à-vis SEC unregistered entities, and insurance products (2017-2019)



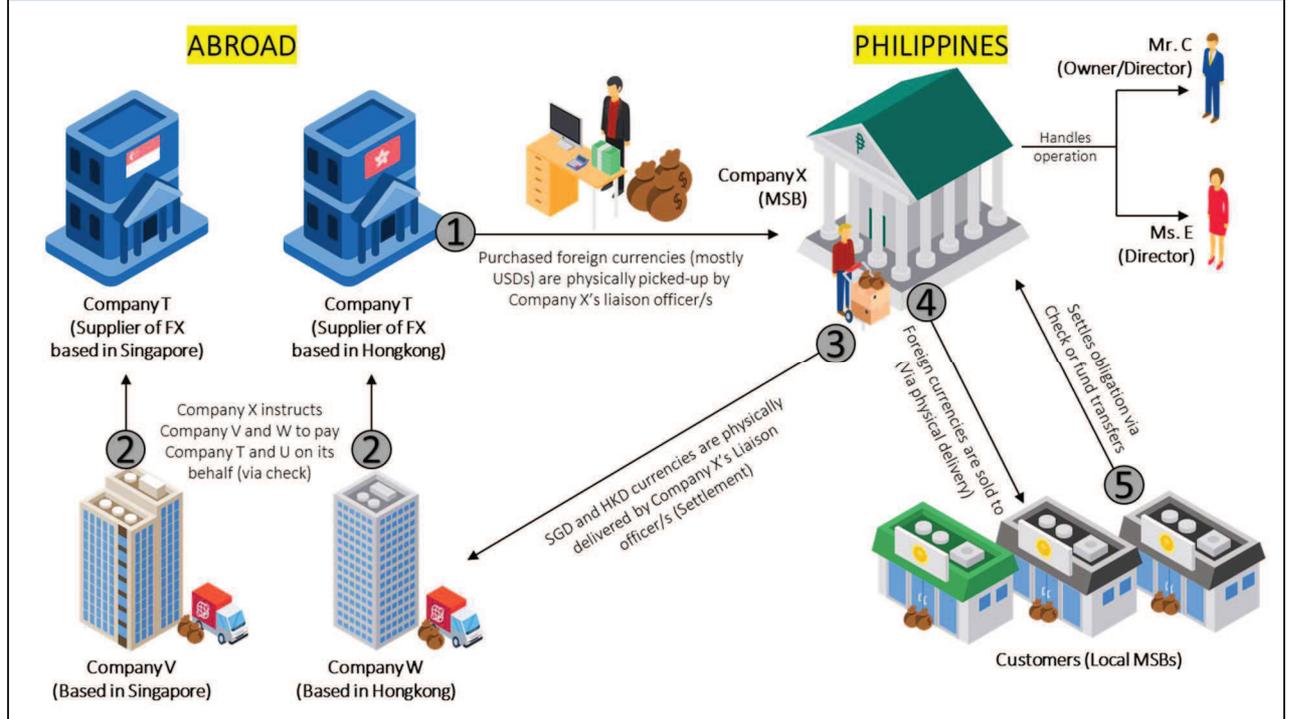
An estimated five million people were defrauded by a company soliciting unauthorized investments from its members amassing an approximate amount of PhP50 billion. A family member of the leader of the organization (Ms. X) administered and transacted the funds using various banks. She opened several bank accounts which facilitated the inter-account transfers and acquired several insurance policies and properties, including real estate.

Case 2. Banks vis-à-vis real estate properties vis-à-vis other legitimate businesses (2017-2019)

Further to the previous case, Ms. X's accounts (around 50 accounts with several banks) were used to integrate the proceeds of illegal investment scheme into acquired businesses related to education, metal trading, quarrying, fishing, gasoline trading, and wellness, among others. She also used the proceeds to purchase personal luxury items and clothes. Proceeds were also used to purchase real estate properties, motor vehicles, and fishing vessels.

- c. **Swindling/Fraud** - Proceeds are being funneled from banks to other sectors, such as securities broker/dealer, and lawyers/law firms, using deposit accounts.
- d. **Web-related crimes** - Proceeds are being channeled from banks to other sectors such as EMIs and MSBs.
- e. **Cash Smuggling** - Criminals employ banks and MSB services in the facilitation of cash smuggling schemes thru DPA of banks and foreign exchange service of MSBs.

Case: Local MSB purchased foreign currencies from abroad which were distributed to other local MSBs. Transactions were not supported with appropriate documents. (2020)

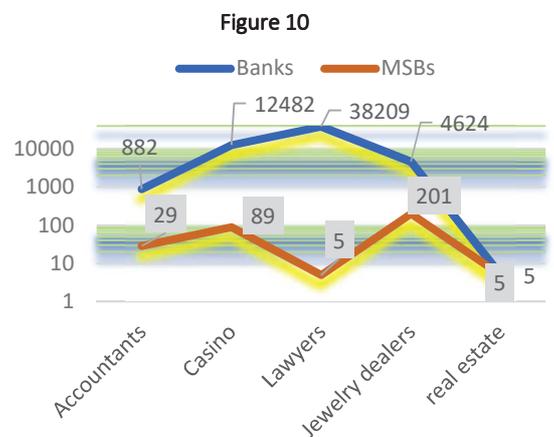


- f. **Mule Accounts** - Mule networks use several financial institutions such as banks and EMIs to funnel proceeds of crime.

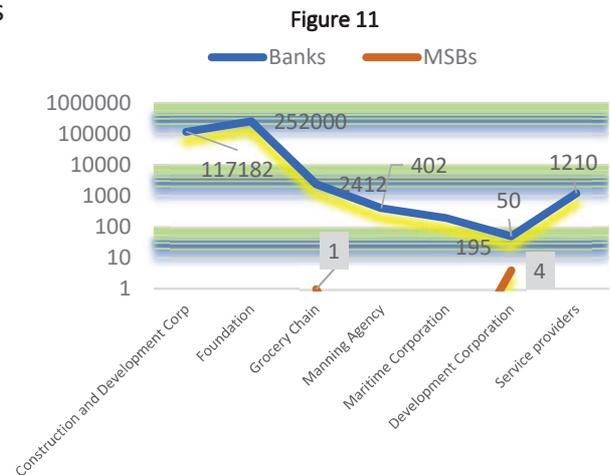
STR Statistics

3.7 Several registered or accredited internet-based casinos and service providers (SPs) figured in 1,031 STRs filed by covered persons (CPs) from 2013 to 2019. The total value of these STRs was estimated at PhP14.01 billion. Also, 83 percent of the STRs filed by VASPs involved transactions coursed through banks (41 percent) and EMIs (42 percent).

3.8 STRs involving transactions of CPs with different sectors/entities showed that a significant number of suspicious transactions were reported by banks (39 percent), other BSFIs, in particular MSBs (38 percent) and EMIs (9 percent). Dealings of banks and MSBs with accountants, casinos, lawyers, jewelry dealers, and real estate companies were also apparent in those STRs as shown in *Figure 10*.



3.9 Likewise, several STRs filed by banks and MSBs involved clients engaged in certain cash intensive businesses. These include manning/maritime agencies, grocery chain, hardware, and trading companies. Other types of juridical persons such as those involved in the construction business, foundations, and service providers figured in STRs with large amount of funds (Figure 11).



Sectoral Threat and Vulnerability Assessment

3.10 *The inherent vulnerabilities of deposits and wire transfer services for cross-sector risks are high.* Deposit products are highly vulnerable as these are the initial gateways to the banking system allowing account holders to conduct financial transactions. Meanwhile, wire transfer involves rapid movement of funds within a short period of time within and outside of the country. E-money wallets' vulnerability is **medium** as these are being used at a lesser extent than deposits but are considered as emerging channels that warrant attention.

3.11 For the other sectors, inherent vulnerabilities are summarized below:

Sector Involved	Inherent Vulnerabilities
Remittance Companies/ Pawnshops with Remittance License	<ul style="list-style-type: none"> • Cash-intensive nature business; • Low cost remittance; • Cross-border element; • Transactions with walk-in and one-off customers; and • Swiftiness of processing a large number of transactions²⁹
EMIs	<ul style="list-style-type: none"> • Swift transfer of funds; and • Use of outsourced/third party for cash-in and cash out transactions
VASPs	<ul style="list-style-type: none"> • Cross-border element; • Capacity for fast settlement; • Use of peer-to-peer exchange, decentralized platforms, and exchanges; and • Potential for increased anonymity and obfuscation of transaction flows and counterparties.
Casinos	<ul style="list-style-type: none"> • Cash-based transactions; • Anonymity of customers/gaming account users; and

²⁹ See pages 180 to 182 of 2nd NRA Report (i.e., vulnerability assessment for MSBs)

Sector Involved	Inherent Vulnerabilities
	<ul style="list-style-type: none"> • For internet-based casino operators, use of agents or professional intermediaries, such as service providers
Other DNFBPs	<ul style="list-style-type: none"> • A CSP creating companies or acting on behalf of third persons who are the ultimate beneficial owners; and • Cash based transactions, some involving large amounts

3.12 *AML/CFT controls across CPs vary.* Banks have established more structured AML/CFT frameworks while preventive and control measures of MSBs, DNFBPs, and other CPs are still developing. It is important that CPs that serve as entry or transit points of funds implement AML/CFT measures that are commensurate with their risk profile to mitigate ML/TF/PF risks arising from cross-sector movement of proceeds of illicit activities. As such, cross-sector vulnerability between banks, MSBs, and DNFBPs, and between MSBs and VASPs and DNFBPs, particularly casino and jewelry dealers, is **high**. These sectors are intricately linked as they use their deposit accounts to settle and process their transactions. Customers use these linkages to swiftly move their money across entities and boundaries. The flow of transactions in and between these sectors allows several layering of funds which can complicate audit trail and hide ultimate beneficiaries.

3.13 *Net cross-sectoral risk among banks, MSBs and other DNFBPs is high.* Banks remain to be at the front and center of settlement of all transactions. Net cross-sectoral risk between MSBs and other DNFBPs is also assessed as **high** considering that their AML/CFT controls are still developing amid the already high level of threat. Meanwhile, net cross-sectoral risk between banks, MSBs vis-a-vis other sectors under securities and insurance commissions is **medium**.

CONSEQUENCE

ML/TF/PF activities pose adverse effects across the financial ecosystem, specifically on the individual customers, the financial institution and sector concerned, the financial system, and the country. At the customer level, the impact of ML/TF/PF activity is **medium** which may involve financial losses, reduced trust in the financial institutions, and risk to physical safety. Impact to the financial institutions, the financial system, and the country is assessed as **high** as ML/TF/PF activities will significantly result in reputational damage and financial losses that pose safety and soundness and financial stability concerns. These illegal activities threaten the integrity and reliability of the financial system. They can also damage national security, harm the country's reputation, and undermine economic growth.