



BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR
FINANCIAL SUPERVISION SECTOR

MEMORANDUM NO. M-2020-092

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

Subject : **Guidance Paper on Managing Money Laundering Risks Related to Online Sexual Exploitation of Children (OSEC)**

The Monetary Board, in its Resolution No. 1611 dated 10 December 2020, approved the issuance of the attached guidance paper, "*Managing Money Laundering Risks related to Online Sexual Exploitation of Children*". The guidance paper highlights good practices, relevant typologies, and red flag indicators related to OSEC. It likewise identifies areas for improvement to strengthen measures to detect, prevent, and mitigate risks arising from these activities.

BSFIs are expected to use this guidance paper in strengthening their AML/CFT processes in a manner that is consistent with and proportionate to their risk profile.

For information and guidance.

Digitally signed by Chuchi G.
Fonacier
Date: 2020.12.15 17:58:33 +08'00'

CHUCHI G. FONACIER
Deputy Governor

15 December 2020

Att: a/s

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE

RYA ROSE D. NUÑEZ
Manager, RMD

Administrative Services Department



Managing Money Laundering Risks Related to
ONLINE SEXUAL EXPLOITATION OF CHILDREN

Guidance Paper
December 2020

Bangko Sentral ng Pilipinas

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE


RYA ROSE D. NUÑEZ
Manager, RMD
Administrative Services Department

TABLE OF CONTENTS

1	Introduction.....	1
2	Executive Summary.....	1
3	Overview of the Focus of the Thematic Review.....	2
4	Good Practices and Areas for Improvement.....	4
	<i>Risk Assessment</i>	<i>4</i>
	<i>Customer Onboarding Due Diligence</i>	<i>4</i>
	<i>Sanctions Risk Management.....</i>	<i>5</i>
	<i>On-going Monitoring of Customers and Transactions.....</i>	<i>6</i>
	<i>Suspicious Transaction Reporting.....</i>	<i>8</i>
5	Typologies and Red Flag Indicators.....	9
6	Challenges.....	12
7	Conclusion	13

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE


RYA ROSE D. NUÑEZ
Manager, RMD
Administrative Services Department



1 INTRODUCTION

Thematic reviews form an integral part of the supervision tools of the Bangko Sentral ng Pilipinas (BSP). These pertain to focused assessment of a particular process or risk area that pose safety or soundness concern to the operations of a supervised financial institution or the financial system, as a whole.

The thematic review conducted in relation to anti-money laundering and combating the financing of terrorism (AML/CFT) supervision is informed by the results of the National ML/TF Risk Assessment (NRA) exercise and surveillance activities aimed at identifying emerging threats in the financial sector. This involves the conduct of horizontal or comparative assessment of relevant AML/CFT practices across BSFIs. The thematic reviews aim to enable the BSP to provide guidance to BSFIs to proactively curb the identified ML/TF risk.

2 EXECUTIVE SUMMARY

This thematic review disclosed that BSP-supervised financial institutions (BSFIs) recognize the risks posed by online sexual exploitation of children (OSEC) to their operations. The range of practices across BSFIs vary highlighting both positive or good practices and areas that warrant immediate enhancements.

Some examples of good practices are the established process for customer identification and verification and adoption of automated screening process. Further, BSFIs that participate in the Anti-Money Laundering Council's (AMLC) Public-Private Partnership Program (PPPP) are able to access information on certain personalities linked to OSEC and other unlawful activities that serves as a valuable source to identify customers or transactions that warrant further review or investigation.

On the other hand, areas necessitating enhancements to mitigate ML risks arising from OSEC activities include, among others, conduct of risk assessment, customer due diligence, on-going monitoring and suspicious transaction reporting.

It is essential that the Board of Directors and Senior Management set a proactive tone at the top and establish a culture of risk awareness and compliance within their organizations to ensure effective implementation of a robust AML/CFT framework that has the capability to detect and mitigate risks arising from OSEC-related transactions, among others.

This guidance paper defines the BSP's supervisory expectations in managing ML risks arising from OSEC. It does not impose new regulatory obligations but BSFIs are expected to understand and use this guidance paper to strengthen their AML/CFT processes in a manner that is consistent with and proportionate to their risk profile and their customers.

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE

RYA ROSE D. NUÑEZ
Manager, RMD
Administrative Services Department



3 OVERVIEW OF THE FOCUS OF THE THEMATIC REVIEW

Trafficking in Persons (TIP) is one of the threats identified in the Second NRA (2017). It has been assessed as “medium” threat in the latest NRA due to actions taken to mitigate said risk. One of the forms of TIP is OSEC. OSEC refers to the production, for the purpose of online publication or transmission, of visual depictions of the sexual abuse or exploitation of a minor for a third party who is not in the physical presence of the victim, in exchange for compensation¹. Its pernicious effect to the society and well-being of innocent victims is undoubtedly a threat worth preventing.

Modus Operandi

“Predators/pedophiles target vulnerable children on social media sites. Usually, they befriend girls and offer financial support for school and for the family. Predators find targets by communicating with Filipina who offers cybersex on adult websites and other instant messaging platforms. At this instance, a predator can directly ask for younger victim since conversation is done privately. A Filipina facilitates in obtaining, offering, recruiting girls of younger age which fit the desire of the predator in exchange for money. Sexual exploitation of children depends on the desire of the predators.”

Source: Philippine National Police Women and Children Protection Center

Suspicious transaction reports (STR) related to OSEC were identified or tagged as relating to the following crimes:

- a. “Anti-Trafficking in Persons Act of 2003” or Predicate Crime (PC) 19;
- b. “Anti-Photo and Video Voyeurism Act of 2009” or PC30;
- c. “Anti-Child Pornography of 2009” or PC31; and
- d. “Special Protection of Children Against Abuse, Exploitation and Discrimination” or PC32.

4th

In 2019, PC32 ranks 4th among the predicate offenses, in terms of number of cases, cited in the STR submissions of BSFI². Aside from reviewing STRs related to OSEC, coordination with relevant government agencies was a crucial part of planning and scoping for this thematic review.

¹ International Justice Mission (IJM), in partnership with the U.S. Department of State Office to Monitor and Combat Trafficking in Persons (TIP Office), and the Philippine Inter-Agency Council Against Trafficking (IACAT), Online Sexual Exploitation of Children in the Philippines: Analysis and Recommendations for the Governments, Industry, and Civil Society, Page 6

² Source: AMLC’s STR Statistics

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE

2 | Page

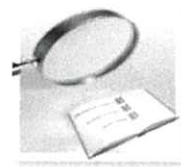
RYA ROSE D. NUÑEZ





Manager, RMD

Administrative Services Division



The thematic review on select Philippine banks and money service businesses (MSBs) covered an in-depth evaluation of the business models, policies, transactions, and supporting documents related to the following AML/CFT processes:



 Risk Assessment	 Sanctions risk management
 Customer on-boarding due diligence	 Ongoing monitoring of customers and their transactions and suspicious transaction reporting

4 GOOD PRACTICES AND AREAS FOR IMPROVEMENT

Active surveillance to identify emerging threats and typologies is essential in an evolving ML/TF landscape. The thematic review highlighted both good practices and areas for enhancements in managing risks arising from OSEC activities. These are discussed in detail in this section to provide guidance to BSFIs in strengthening measures to detect and mitigate risks arising from OSEC-linked customers and transactions.

RISK ASSESSMENT

BSFIs shall identify, understand and assess ML/TF risks arising from their customers, countries or geographic areas of operations both of the BSFI and its customers, products, services, transactions, or delivery channels.



Areas for Improvement

- Enterprise ML risk assessment exercises should be periodically conducted and should cover the evaluation of risks arising from OSEC activities for relevant businesses and customers.

CUSTOMER ONBOARDING DUE DILIGENCE

BSFIs shall maintain a system that will ensure the conduct of customer due diligence (CDD) which shall include, among others, identifying and verifying the true identity of the customer based on official documents or other reliable, independent source documents, data or information.



BSFIs shall specify the criteria and description of the types of customers that are likely to pose low, normal or high ML/TF risk to their operations, as well as the standards in applying reduced, average, and enhanced due diligence, including a set of conditions for the denial of account opening or services.

Risk Profiling Methodology – Criteria	
<ul style="list-style-type: none">• Nature of service/product to be availed of by the customers and the purpose of the transaction;• Source of funds/nature of business activities;• Country of origin/residence of operations or the fact that a customer came from a high-risk jurisdiction; and	<ul style="list-style-type: none">• Other factors as the BSFI may deem reasonable or necessary to consider in assessing the risk of a customer to ML/TF (such as the size of transactions, the regularity or duration of the transaction, and the relationship of sender to beneficiary particularly for remittances).

Good Practices

- Implementing well-articulated policies and procedures on customer identification. Customers are required to fill out a **Customer Information Sheet (CIS)**, among other requirements, and present valid identification document. The CIS contains the required

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE
4 | Page

RYA ROSE D. NUÑEZ
Manager, RMD
Administrative Services Department

customer information. In some MSBs, supplemental information such as the purpose of the remittance and relationship between parties of the transactions are obtained.

- **Automating the customer risk profiling system** that is interfaced with the on-boarding customer information system. This facilitates effective and consistent implementation across branches. Some BSFIs implement automatic tagging of customers as **high risk based on pay-out locations known for OSEC activities**, existence of suspicious transaction indicators related to OSEC, and results of watchlist screening.
- Adopting control measure through **issuance of cards to MSB** customers for ease of conducting future transactions and monitoring customer's activities. The card can also be issued in electronic/digital form with sufficient access controls.
- Employing **structured accreditation process for remittance sub-agents** primarily focusing on Know Your Sub-Agent (KYSA) processes.

Areas for Improvement

- **Inadequate controls** resulting in uneven implementation of (i) customer identification policies across branches and remittance partners, including establishing source of funds; and (ii) enhanced due diligence procedures for high risk customers.
- **Unsophisticated risk profiling methodology**, characterized by manual process and adoption of limited or incomplete factors, resulting in implementation and audit trail deficiencies. For some BSFIs, **purpose, expected activity on the account, frequency, volume and value of the remittances are not considered** in risk profiling. **Supplemental information (such as the country of origin, name and address of remitter, and relationship between parties of remittances)** that are useful in monitoring OSEC activities are not obtained and not considered in customer risk profiling.
- **Insufficient documentation by the correspondent bank of the assessment of respondent bank's AML controls** due to inadequate policy and process. *The result of the assessment, if documented, would have been a risk factor to support the understanding of respondent bank's activities.*

Added Value: *Proper assessment of customer risk profile will drive the conduct of suitable level of due diligence during on-boarding as well as throughout the life cycle of customer relationship.*

SANCTIONS RISK MANAGEMENT

BSFIs are required to develop clear, written and graduated customer acceptance and identification policies and procedures, **which shall include sanctions screening**. A risk-and-materiality-based on-going monitoring of customer's accounts and transactions, including **periodic sanction screening**, should be part of a BSFI's customer due diligence process.



CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE
5 | Page

RYA ROSE D. NUÑEZ
Manager, RMD
Administrative Services Department

Good Practices

- **System interfacing of watchlist database with international partners.** This enables automated screening of personalities subject of watchlist.
- **Updating of watchlist database to include those who are subject of referrals from the AMLC and tie-up partners.** These referrals help BSFIs flag and detect individuals that can be subject to further scrutiny during on-boarding and processing of transactions.
- **Sharing of watchlist database with the remittance agents/partner institutions by certain BSFIs and periodic referrals from international partners** to aid in the proactive and timely identification and detection of personalities related to OSEC. This includes issuance of regular advisories to these partners for updates to the list.
- **Implementing transactional denial on blacklisted personalities.**

Areas for Improvement

- **Inadequate controls to ensure that the watchlist database is complete, comprehensive and updated in a timely manner.** Certain BSFIs do not include existing customers with previously filed STRs and personalities subject of adverse or negative media reports in the watchlist database while others only include those referred by AMLC with exact name match, with secondary identifiers, or have transacted with the BSFIs. This practice is inadequate and limiting.
- **Screening in silos** as some BSFIs do not provide automated screening system to remittance partners for vetting of potential customers due to data privacy restrictions. *This results in failure to conduct appropriate due diligence or take prompt action on transactions of customers included in the watchlist.*
- **Policy gaps in terms of remitter screening and handling or disposition of sanctions alerts.** *This results in approval and processing of transactions of customers with sanction alerts without adequate justification.*

Effect: Delayed updating of watchlist database results in failure to identify and review transactions of customers subject of negative information.

ON-GOING MONITORING OF CUSTOMERS AND TRANSACTIONS

BSFIs shall establish a system that will enable them to understand the normal and reasonable account or business activity of customers to ensure that the customers' accounts and transactions are consistent with their knowledge of the customers, and the latter's commercial activities, risk profile, and source of funds and detect unusual or suspicious patterns of account activity.



On wire transfer requirements: BSFIs shall establish policies and procedures designed to prevent it from being utilized for ML/TF activities. BSFIs shall ensure that all wire transfers are always accompanied by the required information.

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE

6 | Page


RYA ROSE D. NUÑEZ

Manager, RMD

Administrative Services Department



Good Practices

- **Participating in the Public Private Partnership Program (PPPP) of the AMLC.** The program creates a collaborative environment among the participants to enhance the fight against money laundering and its predicate crimes by sharing information on certain personalities involved in unlawful activities. *This will flag the BSFIs on certain personalities linked to OSEC and other unlawful activities.* 
- **Supplementing electronic monitoring system with manual monitoring tools,** such as report on unusual activities at the branch level. *This contributes to identification of unusual transactions and to eventual filing of organized and complete reports and STRs.*
- **Adopting manual red flag indicators** on OSEC especially with regard to the behavioral indicators in the remittance sector.
- **Sharpening alert parameters** to capture unique attributes of OSEC activities, such as jurisdictions linked to OSEC, use of more than one international money remittance company to avoid detection, and frequency of transactions within a defined period (e.g., three or more remittances from a single sender to a single receiver weekly or monthly).
- **Complying with the travel rule requirement** on mandatory information that should accompany wire transfers, which is essential for monitoring customers and their transactions.
- **Sanctions screening on parties** of the remittance transactions particularly for cross-border transactions.
- **Regularly monitoring the performance of remittance partners and agents.**

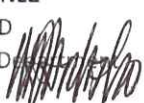
Areas for Improvement

- **Inadequate detection parameters and scenarios in the AML electronic monitoring systems** to capture transactions potentially linked to OSEC activities. These parameters should consider low value transactions, geographical locations (country of origin, destination in the Philippines) and profiles of sender and beneficiary (gender, nationality, and relationship of the parties).
- In terms of alerts management system, there were noted (a) **delays in disposing alerts** due to large volume of system alerts as well as inadequate resources to manage and resolve the alerts; and (b) **inconsistencies in alerts disposition** due to insufficient guidelines and maker-checker controls. *Information regarding the relationship, name and nature of business, and remitter/beneficiary information should be considered in the review of alerts.*
- **Inadequate controls to monitor the transactions and update the risk profile of customers who have been subject of previous STRs.** These are critical in flagging and

Consider the purpose of the transaction or certain word/phrases in the payment chain which can be potentially linked to OSEC activity, such as "happy times" or "good girl".

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE
7 | Page

RYA ROSE D. NUÑEZ
Manager, RMD
Administrative Services Division



investigating customers who continue to transact in similar but unusual patterns, and in deciding on further actions to be taken.

- **Absence of post-monitoring review on inward remittances processed for low value remittances** due to the challenge posed by large volume of low value transactions.



- For **correspondent banking relationships**, inadequate monitoring system by the correspondent bank or intermediary financial institution to understand the usual or expected activities of the respondent bank and detect any unusual or suspicious transaction pattern of activity that is inconsistent with the purpose of services provided. Requests for information (such as sender's information) are not sent to the respondent bank to facilitate thorough review and investigation of transactions potentially linked to OSEC activities. There are inadequate policies on when to execute, reject, or suspend wire transfers that lack the required information.

Certain international remittance partners do not provide the required originator information due to data privacy. This leads to some limitations in identifying and monitoring inward remittances possibly linked to OSEC activities. This should be considered in the periodic evaluation of the relationship with the remittance

SUSPICIOUS TRANSACTION REPORTING

BSFIs should report to the AMLC all suspicious transactions. The STR shall be submitted to the AMLC in a secured manner, in electronic form and in accordance with the reporting procedures prescribed by the AMLC. The BSFIs shall provide complete and accurate information of all the mandatory fields required in the report.

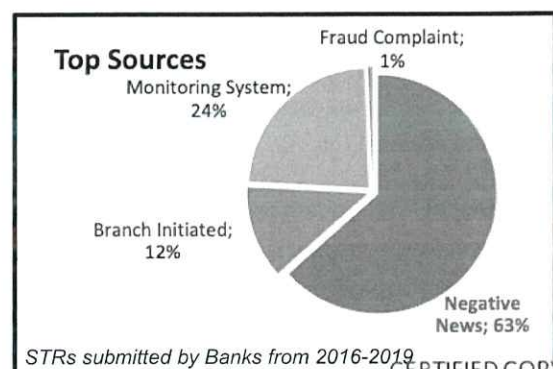


Good Practice

- **Submission of meaningful STRS** with relevant details, such as the complete profile of the account holder or customer, substantial narrative of events pertaining to OSEC, parties involved in the transaction, and reason for filing. *These are helpful to the AMLC and other authorities in their analysis and investigation of OSEC-related financial transactions.*

Areas for Improvement

- STRs on OSEC were largely sourced from negative media reports and AMLC referrals.



STRs submitted by Banks from 2016-2019

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE
8 | Page

RYA ROSE D. NUÑEZ
Manager, RMD
Administrative Services Department

5 TYPOLOGIES AND RED FLAG INDICATORS

TYPOLOGIES. Some of the OSEC typologies noted in the review are presented here to aid the industry in fully understanding the schemes and activities of OSEC. Based on these typologies, red flag indicators were developed for the guidance of BSFIs in identifying and detecting OSEC-related financial transactions.

Case 1.

A certain Mr. A residing in London, United Kingdom sent remittances to Ms. X, a Filipino housewife in Taguig City, from June 2013 to October 2015, totaling Php406,699. Amount per transaction ranges from Php450 to Php11,000. The two has no clear familial relationship. The sender was identified as suspected to be involved in online child exploitation activities. Upon investigation, the beneficiary disclosed that the sender is a friend, and the remittances were for allowance and food expenses.

Case # 2

Ms. M, a Filipina, unemployed and a resident of Davao City, received various international inward remittances totaling Php344,381 from eighteen male foreign national senders located in the United States (43%), Denmark (25%), Norway (16%), and others such as Australia, Italy, Russia and United Kingdom. The amount of remittances ranged from a low of Php 130 to Php 21,750. The sender has no known relationship with the beneficiary, and transactions have no underlying legal or trade obligation.

Case #3

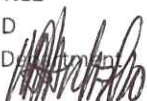
Mr. B, a British National from London, sent 79 remittance transactions to 15 different individuals in Cavite, Bulacan, Metro Manila and Rizal, totaling PhpP89,617 from July 2012 to October 2015. Amount of remittances ranged from Php250 to Php11,000. The sender has no apparent familial or ethnic relationship with the beneficiaries. Also, there is no legal or trade obligation, purpose or economic justification for the transactions.

Case # 4

Mr. B, an Australian national and a retired teacher, resides in an upscale village in Iloilo. Analysis of his remittance transactions disclosed a pattern of 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 aggregating Php165,150, ranging from Php900 to Php40,000. The sender has no apparent ethnic or familial relationship with the beneficiaries and no economic justification for the transaction.

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE
9 | Page

RYA ROSE D. NUÑEZ
Manager, RMD
Administrative Services Division



INDICATORS. BSFIs should be sensitive to the following red flag indicators when processing remittance transactions, especially incoming remittances, as these could indicate potential link to OSEC activities. These red flags are not exhaustive and the presence of one indicator does not necessarily mean that there is certainty that the transaction is related to OSEC. Using a combination of these red flag indicators is recommended especially in adopting detection parameters and scenarios in the AML systems to generate meaningful alerts.

PARTIES TO THE TRANSACTION

- Parties are purely individuals, usually with male senders from other jurisdictions;
- Single sender to multiple beneficiaries. Some beneficiary customers may have the same address or same barangay;
- Multiple senders to single beneficiary or to a group of related individuals or within the same family or locality;
- Senders are usually aged 21 to 40 years old (45 percent). There are also senior citizens aged 61 to 70 comprising 17 percent of the total STR submissions;
- Beneficiary customers are usually unemployed aged 21 to 40 years old (70 percent);
- No familial or ethnic relationship between sender and beneficiary or unknown or unjustified relationships between the parties; and
- Most of the time, the use of facilitators is evident in receiving remittances for the benefit of minor victims.

GEOGRAPHICAL LOCATIONS

- Remittances are coming from countries known for OSEC activities, and these were claimed or withdrawn in the Philippines from locations known or reported to be hotspots for OSEC.

Top 10 Sending Countries for OSEC (Based on volume)

1) Philippines, 2) United States of America, 3) United Kingdom, 4) Australia, 5) Canada, 6) Norway, 7) Germany, 8) Netherlands, 9) Denmark, and 10) New Zealand.

Based on 2,482 STRs of MSBs 2019 to June 2020.
Using sender's address in determining country of origin

Top 10 Destination of Remittances (Based on volume) 1) Cebu, 2) Lanao Del Norte, 3) Bulacan, 4) Cavite, 5) Taguig City, 6) Zamboanga, 7) Pampanga, 8) Samar, 9) Metro Manila, 10) Leyte

Based on 11,378 STRs of MSBs, 2019 to June 2020.
Using beneficiary's address in determining destination

Top 5 Countries Hosting Child Sexual Abuse Material: 1) United States of America, 2) Netherlands, 3) Russian Federation, 4) France, 5) Canada.

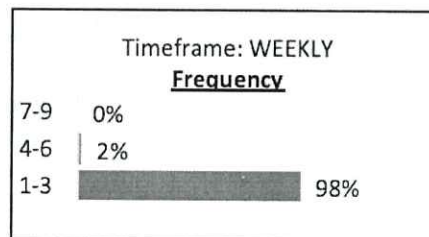
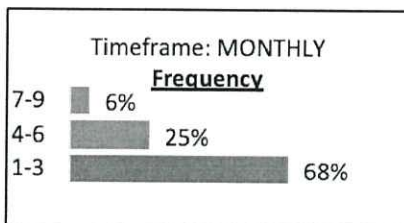
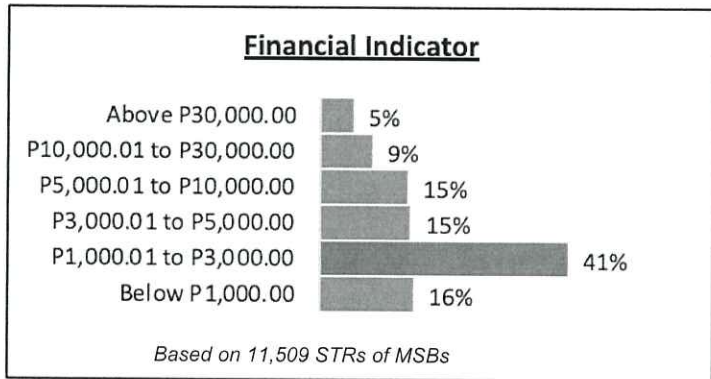
Source: *Online Sexual Exploitation of Children in the Philippines: Analysis and Recommendations for Governments, Industry, and Civil Society (IJM)*

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE
10 | Page

RYA ROSE D. NUÑEZ
Manager, RMD
Administrative Services Department

TRANSACTIONS

- Low value or amount per transaction;
- No underlying legal or trade obligation, purpose or economic justification;
- Suspicious payment messages (*good girl and happy times*);
- Use of more than one international money remittance company to avoid detection; and
- Frequency, e.g., one to three transactions per week or per month (*based on top 20 senders of more than 1,200 STRs*).



BEHAVIORAL³

- The beneficiary customer:
 - behaves like they are being controlled by someone ("*handler*");
 - is accompanied by another person. The beneficiary customer picks up a remittance and immediately hands the funds over to someone else;
 - appears fearful, anxious, depressed, submissive, tense, nervous, paranoid, or avoid eye contact;
 - seems to lack knowledge of their whereabouts or what city they are in; or
 - does not know the name of the sender;
- An adult, including senior citizen, claims a remittance on behalf of a minor;
- Use of a dummy beneficiary customer. Someone else speaks for the customer, yet puts the transaction in latter's name rather than his/her own;
- Beneficiary customer receives remittance using "*friends*" as relationship;
- Purpose of transaction is not clearly established;
- Commonly indicated purpose of transactions are "*family living/sustenance or expenses*" and "*allowance or gifts*"; and
- Multiple smaller amount transactions sent within a short time frame by multiple senders to a common receiver.




³ Behavioral indicators are presented to guide BSFs in dealing with unusual customers at the time of processing of the transaction. This is usually applicable to MSBs during payout of remittances and banks for transactions processed over-the counter.

6 CHALLENGES

The thematic review recognizes the challenges faced by the BSFIs in enhancing their existing AML/CFT framework to detect OSEC-related transactions. These include:

- **Inclusion in the watchlist of AMLC-referred persons of interest with incomplete or limited information, and personalities from negative media reports with no secondary identifiers.** There are instances when only the names are available and provided by the competent authorities. These may lead to numerous false positive alerts and pose difficulty in resolving the alert. To manage this concern, BSFIs need to have an internal process for the disambiguation and further evaluation of the customer, which may include conducting research, review of CDD information and historical transactions, and other available information. This largely depends on the robustness of CDD and adequacy of customer information obtained.

Collaborative measures to combat OSEC are being undertaken by various agencies, such as the AMLC, Philippine National Police, National Bureau of Investigation, DOJ, other organizations and non-government sectoral agencies [such as the Philippine Internet Crimes Against Children Center (PICACC), Inter-Agency Council Against Trafficking (IACAT)], to produce sufficient intelligence risk information to be shared to BSFIs.

- **Incomplete information on ultimate senders of inward transaction.** Some originating institutions, particularly foreign remittance tie ups, do not indicate the names of ultimate senders. Instead, they include the name of the sending institution in the payment chain. AML/CFT standards and regulations⁴ require that the originating and intermediary institutions should pass on the complete sender information. Intermediary and beneficiary BSFIs should ensure that complete ultimate sender information is received⁵ to have a meaningful analysis of customer transactions. There should be a mechanism to identify transactions that lack the required ultimate sender information, and implement processes in executing, suspending, or rejecting incoming remittance transactions that lack the originator information. Periodic review of relationships with remittance partners and tie-ups should be an integral part of ongoing due diligence.
- **Limitation on intelligence information relating to OSEC.** Participating in the Public-Private Partnership Program of the AMLC is an important step toward strengthening practices to combat OSEC related activities. In this program, the AMLC as well as other stakeholders are able to share information, through Information Sharing Protocol, on certain personalities especially those involved in unlawful activities. 
- **Large volume of low value transactions** makes it more difficult to detect OSEC activities. The presence of one red flag indicator does not necessarily ascertain that the transaction is related to OSEC. The use of a combination of OSEC red flag indicators is encouraged to reduce alerts and efficiently identify and mitigate risk of low value OSEC financial transactions.

⁴ Aligned with the requirements of Financial Action Task Force (FATF) Recommendation 16 on Wire Transfers.

⁵ Subject to rules governing the National Retail Payments System

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE
12 | Page

RYA ROSE D. NUÑEZ
Manager, RMD
Administrative Services 

7 CONCLUSION

The threat of Online Sexual Exploitation of Children (OSEC) and related crimes pose significant reputational risk on the BSFIs as well as on the integrity of the financial system and the country. OSEC has pernicious and devastating effects to the innocent victims and the society in general. In this regard, measures should be taken to ensure that the Philippine financial system will not be used to perpetuate these illegal activities. BSFIs must remain vigilant to prevent these illicit activities from happening.

BSFIs are expected to establish and maintain a robust ML/TF risk management framework to effectively manage risks arising from OSEC activities and to disrupt the financing of this criminal activity. This should be anchored on robust risk assessment and proactive customer and transaction monitoring. The BSFI's Board of Directors should lead in shaping a strong culture of risk awareness and compliance. BSFIs should re-calibrate existing AML/CFT processes to incorporate the learnings from this thematic review and adopt follow-up mechanisms to ensure that the revised policies are effectively implemented.

BSFIs are encouraged to pursue collaborative engagements such as the Public-Private Partnership Program of the AMLC to participate in information sharing arrangements. On its part, the BSP will continue to be actively involved in partnerships and cooperative arrangements with concerned sectors, relevant government agencies, and other stakeholders to strengthen measures to identify, prevent, and report potential OSEC activity.

CERTIFIED COPY OF
ELECTRONIC RECORD ON FILE
13 | Page

RYA ROSE D. NUÑEZ
Manager, RMD
Administrative Services Division

