Republic of the Philippines
Anti-Money Laundering Council

Understanding the Internet-Based Casino Sector in the Philippines: A Risk Assessment

March 2020

secretariat@amlc.gov.ph

EXECUTIVE SUMMARY

The importance of the Philippine casino and gaming industry to the economy is growing, following a gross gaming revenue[1] of PhP216.5 billion (USD4.3 billion) in 2018 from Php176.73 billion in the previous year.

In the first nine (9) months of 2019, property market and employment share of Internet-based casinos/offshore gaming sector reached PhP551 billion (USD10 billion). Shares of annual office and housing rentals are estimated at PhP11 billion (USD219 million) and PhP36 billion (USD 680 million), respectively. Employment share of the offshore gaming sector generated about PhP504 billion (USD9 billion) salary payments for the same period.[2]

The increasing demand for the offshore gaming sector or Internet-based casino operations may pose a potential threat and risk to money laundering. The 2017 Second National Risk Assessment rated the casino sector with a high level of risk to money laundering (ML). Among the factors that contributed to the high vulnerability of the casino sector include its cash-intensive business operations, high-risk client-base profile, and weak or deficient anti-money laundering/countering the financing of terrorism (AML/CFT) controls. It was only through the passage of Republic Act No. 10927 in July 2017 when casinos were designated as covered persons under the AML/CFT regime.

The Philippine Amusement and Gaming Corporation (PAGCOR), Cagayan Special Economic Zone (CEZA), and Aurora Pacific Economic Zone and Freeport Authority (APECO), also known as appropriate government agencies (AGAs), undertake the prudential regulation of Internet-based casino operations. In relation to AML/CFT regulations, the Anti-Money Laundering Council (AMLC) and AGAs jointly supervise Internet-based casinos. As of November 2019, 32 Philippine offshore gaming operators (POGOs) of PAGCOR, four (4) interactive gaming licensees (IGLs) of CEZA, and one (1) online gaming operator of APECO have registered with the AMLC. This study, however, focuses on PAGCOR- and CEZA-supervised Internet-based casinos and their respective service providers (SPs). APECO's online gaming operator has yet to commence during the conduct of the risk assessment.

Based on collaborative results among the AMLC and AGAs and based on risk factors, Internet-based casinos are **highly vulnerable to ML**. Among the contributory risk factors to ML are the high level of cash-based transactions; weak or deficient AML/CFT regulations; a high level of anonymity of customers/gaming account users and Internet-based casino operators; a high level of use of agents or professional intermediaries, such as SPs. Due to the lack of supervision of the SP sector, SPs are prone to abuse and exploitation for ML and other crimes. Existing cases and investigations, involving SPs of Internet-based casino operators, support the risk analysis.

[1] Gross gaming revenue (GGR) includes revenues from the Philippine Amusement and Gaming Corporation (PAGCOR) and the Cagayan Special Economic Zone (CEZA). PAGCOR recorded PhP215.84 billion in GGR in 2018, a 22.24% increase from PhP176.50 billion GGR in 2017, based on the 2017 and 2018 PAGCOR annual reports. CEZA's revenues recorded PhP706 million in 2018, a 203% increase from PhP233.1 million in 2017 (https://ceza.gov.ph/article/ceza-revenues-surge-p706-m-2018).

[2] Leechiu Consultants, Real Estate Market Insights, November 2019

In relation to the sector's vulnerability to terrorism financing (TF), the threat is generally low as there is no concrete evidence that links Internet-based casinos to terrorism and TF, based on available records.

Within the offshore gaming casino framework, consequential risk to ML occurrence as derived from inherent risk is moderate. Reputational, operations/compliance, and financial impact are among the consequential risks. The impact of reputational loss is high, while the impact of operations/compliance and financial loss is moderate.

OVERALL RISK

Considering the threat/vulnerability risk and consequential impact, the overall risk of the Internet-based casino sector is in the **upper medium level**. This requires a mitigation strategy to be executed immediately. A **moderately high level** of vulnerability risk is noted within the SP framework of Internet-based casino operations, resulting from targeted and macro-level approach analyses. Thus, a collective mitigation strategy with concrete actions must be applied to SPs and Internet-based casino operators. The mitigation strategy aims to reduce or prevent the occurrence of risks associated with the Internet-based casino operations framework.

A. GENERAL FINDINGS AND CONCLUSION

Based on quantitative and qualitative assessments, the following are the results:

FINDINGS

1. Despite its recognition as among the significant contributors and drivers to the economic growth, the entire casino industry accounts for about less than 1.4% of the economy. Taking the gross revenues from 2017 to 2018, the Internet-based casino sector accounts for only about 2.5% of the gross revenues of the entire casino sector. Thus, the Internet-based casino sector represents only about 0.03% of the economy. By nature of business, financial transactions of Internet-based casinos are generally remittance-based and non-cash transactions.

2. The Internet–based/offshore gaming casino business framework covers SPs that render services to licensed operators. Ideally, SPs should not provide services to more than one operator. There are, however, links among SPs and several Internet-based casino operators.

3. Regulators and authorities have limited access to transactions and customer due diligence (CDD) records of Internet-based casinos and SPs.

4. Given the business nature of Internet-based casinos, the following transactions appear unusual:

    - Internet-based casinos receive funds from and send funds to local and foreign individuals through inter-account transfers, domestic remittances, and international remittances.

- Cash deposits and other cash-related transactions are not within the normal operations of Internet-based casinos. Cash deposits of POGOs and SPs of PAGCOR are more diversified in terms of bank and locational distribution, compared to IGLs and interactive gaming support service providers (IGSSPs) of CEZA.

5. Only a few Internet-based casinos are related to suspicious activities, such as the lack of underlying economic or legal justification to the transacting parties. Suspicious activities primarily relate to the transactions of SPs of Internet-based casinos.

6. Transactions of Internet-based casinos and SPs reveal a significant level of use of cash, which is susceptible to ML, considering that the ultimate source and the beneficiary of the funds are difficult to determine. Also, cash-based transactions tend to obscure the audit trail. There is also a high level of use of check-related transactions. Cash- and check-based transactions are considered unusual as these deviate from the business framework operations of Internet-based casinos.

7. Several transactions involve individuals with no clear connections with SPs.

8. Internet-based casinos and their SPs may be using money service business (MSB) accounts for foreign exchange (forex) transactions.

9. Highly substantial forex transactions appear in the transactions of SPs. Verification is needed to determine if these SPs engage in forex trading or if the transactions are related to business operations. Some of the SPs have nexus with previously identified entities alleged to be beneficiaries of fraud and drug-related money.

10. As of the study's publication, there are no incidences and reports, linking Internet-based casinos to terrorism and TF. Also, tactical analyses on the transactions of Internet-based casinos show no possible links to terrorism and TF.

CONCLUSION

1. LOW LEVEL OF AML/CFT AWARENESS AND REGULATION

Generally, POGOs and IGLs[3] pose a lesser threat compared to their SPs. Certain suspicious activities are within the realm of SPs and IGSSPs. PAGCOR and AMLC supervise POGOs, which are subject to the AML/CFT framework. In contrast, PAGCOR does not technically license SPs but merely accredits SPs to provide technical and operational services to POGOs in relation to gaming/gambling operations.

[3] PAGCOR supervises Philippine offshore gaming operators (POGOs), while CEZA supervises interactive gaming licensees (IGLs).

Due to jurisdictional issues, there is a low level of AML/CFT regulation on Internet-based casinos. Though foreign POGOs and IGLs may be subject to the AML/CFT framework of foreign jurisdictions where they are situated, AMLC and AGAs may still conduct onsite/offsite compliance-checking on these foreign Internet-based casinos through their representative/compliance offices or local agents.

2. LOW LEVEL OF BENEFICIAL OWNERSHIP IDENTIFICATION

- The level of anonymity of customers or gaming account owners is high, showing a lack of identification of ultimate beneficial owners of the accounts. Such accounts may be used for potential ML and other fraudulent activities. Moreover, customer identification can only be validated through onsite-checking.

- Likewise, there is a certain level of anonymity of beneficial owners of Internet-based casino operators and their respective representative offices or local agents. In an attempt to conduct onsite compliance-checking on POGOs, the findings are as follows:

    - The offices of the POGOs, local gaming agents, and authorized representatives do not exist at the registered addresses provided by PAGCOR. The SPs, however, are operating in the said addresses.

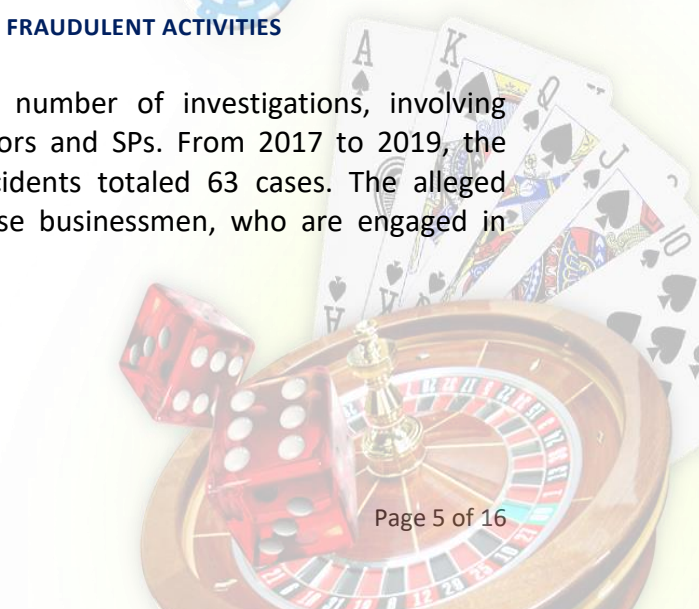
    - There are no actual local agents and/or authorized representatives in the Philippines. These local agents or authorized representatives are obligated to complete the documentary requirements during application for gaming operations.

    - The compliance officers of the POGOs cannot be located and contacted at the given address. The SPs are also unaware of the existence of these compliance officers. This may postulate that there is no coordination between the SP and local agent or authorized representative.

    - The POGOs have no AML/CFT compliance units.

3. INCREASING LEVEL OF THREAT TO ML AND OTHER FRAUDULENT ACTIVITIES

There is an increasing trend on the number of investigations, involving domestic Internet-based casino operators and SPs. From 2017 to 2019, the recorded casino-kidnapping-related incidents totaled 63 cases. The alleged kidnapping syndicate preyed on Chinese businessmen, who are engaged in online gaming.



4. HIGH NUMBER OF UNREGULATED OR UNSUPERVISED SPS

- As SPs are not within the realm of AML/CFT supervision, they are prone to abuse and exploitation by criminal organizations.

- In 2019 alone, local authorities closed down around 200 Internet-based casinos and SPs that illegally serviced online gaming operations. In the same year, the local government ceased the operations of one of the largest SPs for an Internet-based casino. The said SP was also the subject of a case study for alleged links with an individual and entity under AML investigation in relation to the Bangladesh Bank heist.

5. LOW LEVEL OF TF THREAT

- TF threat within the Internet-based casino sector is generally low. Based on available records, there is no concrete evidence that links Internet-based casinos to terrorism and TF.

B. RECOMMENDATIONS

The study recommends the implementation of the following:

INCREASE THE LEVEL OF AML/CFT EFFECTIVENESS OF COMPLIANCE AND SUPERVISION

1. Casino regulators or AGAs must continue and enhance the monitoring and supervision of Internet-based casinos. The AMLC and AGAs must also show effectiveness in supervising the Internet-based casino sector for AML/CFT purposes through the following:

    - Issue AML compliance guidelines for Internet-based casinos;
    - Create a manual on risk-based supervision/examination;
    - Conduct AML/CFT training to operators, domestic POGOs, and SPs; and
    - Check compliance or implement ML/TF preventive programs.

2. The supervision of Internet-based casinos must be revisited, taking into account the roles of SPs in the AML/CFT framework and know-your-customer (KYC)/CDD requirements. The AMLC and AGAs must also review the governing agreement between the Internet-based casino operator and the local agent/representative office. The local agent, who is authorized to represent and act on behalf of the Internet-based casino operator, functions as either a company service provider or management and operations service provider.[4]

[4] Republic Act No. 9160, as amended, includes the following as covered persons: *"(6) Company service providers, which, as a business provide any of the following services to third parties: (i) acting as a formation agent of juridical persons; (ii) acting as (or arranging for another person to act as) a director or corporate secretary of a company, a partner of a partnership, or a similar position in relation to other juridical persons; (iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; and (iv) acting as (or arranging for another person to act as) a nominee shareholder for another person; or (7) Persons who provide any of the following services: (i) managing of client money, securities or other assets; (ii) management of bank, savings or securities accounts; (iii) organization of contributions for the creation, operation or management of companies; and (iv) creation, operation or management of juridical persons or arrangements, and buying and selling business entities.*

Thus, the local agent must be covered under the AMLA, as amended. Other types of SPs with similar functions based on their Securities and Exchange Commission (SEC) corporate registrations shall also be considered covered persons under the AMLA.

As a covered person under the AMLA, the local agent/representative office is required to perform the following AML obligations:

- Prepare and implement a Money Laundering/Terrorism Financing Preventive Program (MLTFPP);
- Conduct KYC and necessary CDD procedures;
- Report suspicious transactions;
- Report covered cash transactions, exceeding PhP5,000,000.00; and
- Keep records of transactions.

The AMLC, in coordination with AGAs, may also need to issue or revise the guidelines clarifying the classification of SPs, including local agents/representative offices as reporting entities under the AMLA.

ENHANCE COORDINATION AND ENFORCEMENT ACTIONS

3. AGAs need to re-evaluate licenses and/or certificates of authority/accreditation issued to Internet-based casino operators and to SPs, respectively, and require the cancellation of licenses of casinos and SPs with derogatory records. Violations or non-compliance with the Republic Act (RA) No. 9160 or the AMLA, as amended, RA No. 7922, RA No. 9490, RA No. 9728, and other issuances of the AMLC and AGAs should warrant the cancellation of licenses/certificates of authority or accreditation to cease the operations of these Internet-based casinos.

4. AGAs shall closely coordinate with the AMLC, particularly in sharing derogatory information on Internet-based casino sector players (i.e. POGOs, IGLs, SPs, IGSSPs, etc.) prior to the issuance of licenses or certificates of authority or accreditation.

5. Regulatory assessment and enforcement actions must be conducted on PAGCOR-accredited SPs and CEZA's IGSSPs identified as potentially high threat. PAGCOR and CEZA may need to engage law enforcement authorities and the AMLC in imposing sanctions against criminals and unregulated SPs/IGSSPs.

6. The supervisors—Bangko Sentral ng Pilipinas (BSP), SEC, and Insurance Commission (IC)—may issue guidance to their respective covered persons (CPs) to conduct enhanced due diligence on high-risk Internet-based casino operators, including their SPs, and to implement additional measures before opening accounts with financial institutions.

7. AMLC, in coordination with AGAs, must conduct AML/CFT training to domestic POGOs or licensees, master licensors, and SPs to enhance AML/CFT risk understanding, reporting obligations, and KYC/CDD procedures.

8. AMLC and other regulators must create a typologies report and a list of ML indicators for the guidance of CPs and the public.

9. Regulators must conduct or update their own sectoral risk assessments on ML and TF, including emerging threats and linkages to other financial sectors.

10. AMLC and AGAs must continue the assessment-scanning of Internet-based casino operators and SPs and must identify other segments and emerging risks, involving the offshore gaming casino sector.

11. The AMLC must disseminate the study to supervisors and AGAs. Supervisors may need to issue regulations addressed to their respective supervised CPs to monitor or to conduct enhanced due diligence when dealing with Internet-based casino operators, primarily focusing on their SPs, including their local agents or representative offices.

C. STRATEGY AND ACTION PLAN

Considering the gaps and deficiencies identified in the Internet-based casino sector, the following are recommended actions to be accomplished or addressed within the timeframe.

Action Plan	Primary Agency	Secondary Agency	Timeline
AML/CFT Effectiveness of Supervision and Oversight • Issue AML compliance guidelines for Internet-based casinos • Create a manual on risk-based supervision/examination • Conduct AML/CFT training to operators, domestic POGOs or licensees, master licensors, and SPs • Check compliance or implement MLTFPP • Regulators to conduct in-depth analysis of ML risk of Internet gaming, e-junket, and other electronic-based products or services • Monitor transaction reporting of AMLC-registered Internet-based casinos; and create guidelines for	AMLC PAGCOR CEZA APECO	Casino operators, master licensors	2019 – October 2020

Action Plan	Primary Agency	Secondary Agency	Timeline
covered and suspicious transaction reporting • AGAs to enhance or develop an AML/CFT framework • Create a list of ML indicators for the guidance of covered persons			
Effectiveness of Compliance Function of the Organization • Prepare and implement MLTFPP • Check compliance and effectiveness of the MLTFPPs of Internet-based casinos • Revisit Internet-based casino and SP framework	AMLC PAGCOR CEZA APECO		2019 – June 2020
Coordination and Enforcement • AGAs to execute memoranda of agreement with law enforcement authorities, AMLC, BSP, and other relevant agencies • Conduct awareness/outreach programs to domestic POGOs, PAGCOR-accredited SPs, CEZA's IGSSPs, and APECO • Enforce cancellation of licenses or certificates of authority or accreditation of Internet-based casinos with derogatory records or with serious or grave AML/CFT or regulatory findings	AMLC PAGCOR CEZA APECO	BSP, law enforcement agencies (LEAs), and other identified relevant agencies	2019 – 1st Q 2020 Continuous
Risk Assessment • Create a typologies report • Conduct or update sectoral risk assessments on ML and TF, including emerging threats and linkages to other financial sectors	AMLC PAGCOR CEZA APECO	Other relevant agencies	2019 – 2nd Q 2020

Typologies and Suspicious Indicators

TYPOLOGIES

The study identifies typologies and several suspicious indicators, relating to possible money laundering (ML) activities to guide covered persons (CPs) in assessing client risk profile. The typologies are gathered from the suspicious transaction reports (STRs) filed by various CPs and requests for information (RFIs) included in the study.

Several registered/accredited Internet-based casinos and service providers (SPs) figured in 1,031 STRs filed by CPs from 2013 to 2019. The total value of STRs that involve these Internet-based casinos is estimated at PhP14.01 billion. The STRs are classified, taking into account the reason for filing and narrative of the STRs as indicated by the CPs.

Total Volume and PhP Value of STRs filed on Entities used in the Study, 2013 – 2019

Predicate Crime / Suspicious Indicator	Volume	PhP Value (in millions)[1]
Electronic Commerce Act Of 2000	17	4,941.19
No Underlying Legal Or Trade Obligation, Purpose, Or Economic Justification	565	4,073.77
Deviation From The Client's Profile/Past Transactions	34	2,419.55
Amount Involved Is Not Commensurate With The Business Or Financial Capacity Of The Client	363	2,226.77
The Client Is Not Properly Identified	36	231.75
Fraud (Swindling)	9	121.09
Drug Trafficking And Related Offenses	6	.000006[a]
Adverse Media	1	.000001[a]
Grand Total	**1,031**	**14,014.13[1]**

[a] The suspicious transactions were reported by Covered Persons (CPs) using ZSTR code.
The code ZSTR is used if the subject is not an accountholder of the CP or is an accountholder but has no monetary transaction with the CP at the time the suspicious activity is determined.
[1]Difference in total is due to rounding-off.

Most of the STRs filed are based on the suspicious indicator "*no underlying legal or trade obligation, purpose, or economic justification*," which accounts for 55% of the total STRs filed on the Internet-based casinos and SPs considered in the study. In terms of value in PhP-equivalent, STRs filed under the predicate crime on violations of the Electronic Commerce Act of 2000 ranked first with PhP4.94 billion, accounting for 35% of total value of the STRs used in the study.

On one hand, four (4) SPs figured in a prior RFI from a foreign jurisdiction as purported beneficiaries of funds from two (2) foreign nationals, who are being investigated for alleged involvement in illicit drug trafficking. The following table shows SPs who allegedly received funds; their accreditation type; and reported remittance transactions.

Alleged Recipients of Drug Proceeds

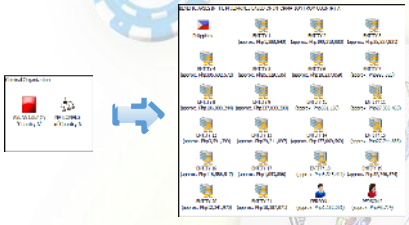
Entity	Type of Accreditation	Alleged Approximate Amount Received based on Foreign RFI (PhP)	Reported Remittances[5] (PhP)
Service Provider 1	Live studio and streaming provider	27 million	61.56 million (2009 and 2014)
Service Provider 2	Strategic support provider	117 million	304.45 million (2013 – 2014)
Service Provider 3	Strategic support provider; and live studio and streaming provider	12.3 million	20.41 million (2014)
Service Provider 4	Customer relations service provider	33 million	No matching transaction
Grand Total		**189.3 million**	**386.42 million**

Data shows that the four (4) SPs allegedly received PhP189.3 million of drug proceeds. Results of analysis, however, show that a total of PhP386.42 million was remitted to the four (4) SPs between 2009 and 2014, all originating from the two (2) foreign nationals.

TYPOLOGIES

1. **Drug trafficking and related offenses and the use of designated non-financial businesses and professions (DNFBPs) in setting up entities alleged to have received funds from illicit activities, based on the foreign RFI.[6]**

In 2018, Country Y requested assistance from the Philippine government in relation to an ongoing investigation on two of its nationals alleged to have funneled funds to other jurisdictions, including the Philippines. The case concerns an ML investigation on Country Y nationals, JT and RW, who were allegedly involved in illicit drug trafficking. The matter was referred to the Philippines for appropriate action.

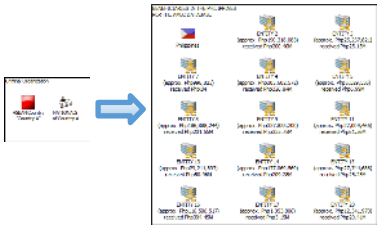


It was stated that JT and RW conducted large and suspicious money transfers to various jurisdictions, involving fictitious import of goods from the Philippines. The subjects allegedly transferred proceeds from illicit drug trafficking to various beneficiaries, comprising 21 entities and two (2) individuals in the Philippines, totaling approximately PhP1.53 billion. Of

[5] Values represent the estimated remittances from the reported transactions on JT and RW, foreign nationals who were allegedly involved in illicit drug trafficking. The remittances are in various currencies, but for the purpose of the study, the PhP equivalents are used for comparing values with the alleged amounts indicated in the foreign RFI.

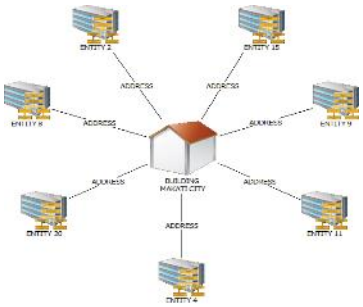
[6] The typology on the use of DNFBPs is published on the AMLC website. http://www.amlc.gov.ph/images/PDFs/TYPOLOGY%20ON%20THE%20USE%20OF%20DNFBPs.pdf.

this figure, PhP189.3 million were allegedly remitted to the four (4) subject SPs.



A total of 23 entities and individuals were listed as alleged beneficiaries in the Philippines of the remittances, originating from JT and RW. Results of the analysis based on the transaction reports, however, showed that only 14 entities from the list appeared as beneficiaries of funds with an estimated value of PhP1.77 billion. It is possible that the remittances to the other entities named in the request are below the reporting threshold. Of the PhP1.77 billion, PhP386.42 million were credited to the four (4) SPs.

Seven (7) entities in the foreign RFI have a common contact person or officer/director based on registration documents filed with the Securities and Exchange Commission (SEC). DO, a Filipino lawyer, was the identified contact person of six (6) entities. He is also one of the officers/directors of SP1. The nationalities of the partners/incorporators of the seven (7) entities are mostly from foreign jurisdictions, Countries Y, Z, and A.

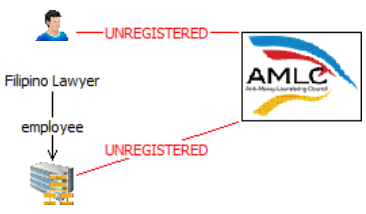


The case also revealed that the seven (7) entities affiliated with DO have several addresses. All, however, have a common address in a Makati Building. This is likely the registered office or business address provided by the law firm or lawyer, who acted as the formation agent of the entities.

Further, based on reportorial submissions with the SEC, five (5) of the entities provided the corporate e-mail address of DO, likely for electronic correspondences. Based on the corporate e-mail address of DO, DO appeared to be connected with a certain law office.

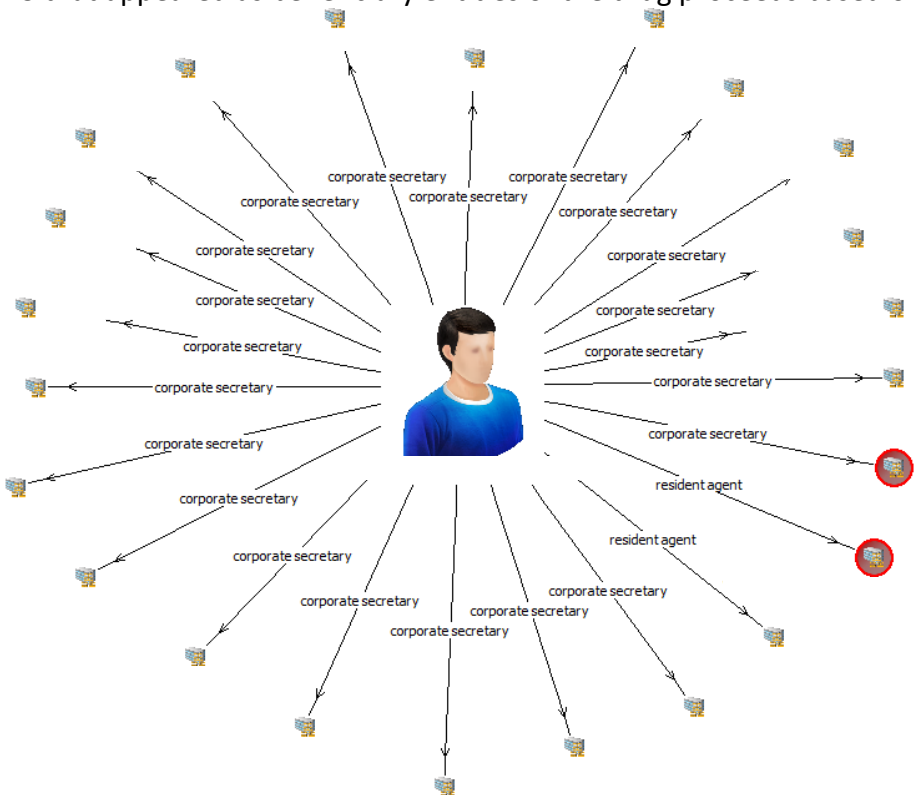
Based on the findings, it appears that DO and the law office provide services that are within the scope of the DNFBP guidelines, such as:

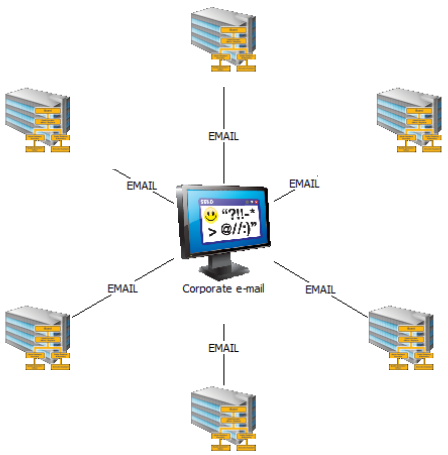
- Acting as formation agent;
- Acting as a corporate secretary;
- Providing a correspondence address (e.g. similar e-mail address); and
- Creating juridical persons.



DO, who appears to act as a formation agent or authorized representative, is not registered with the AMLC. The law firm, where he is connected with, is also not registered with the AMLC.

Further, the study revealed that DO facilitated the incorporation of 23 SPs, which include SP1 and SP3 that appeared as beneficiary entities of the drug proceeds based on the RFI.





In addition to the 23 SPs associated with DO, six (6) SPs in the study declared the corporate e-mail address of DO and another presumed employee of the law office.

The 29 SPs associated with DO and the law office figured in 40,583 CTRs and 334 STRs filed by various CPs between 2010 and 2019. These SPs were registered with the SEC between 2005 and 2018. Combined cash transactions of the 29 SPs totaled PhP29.09 billion in cash deposits and PhP11.39 billion in cash-outs.

This typology shows that some of the SPs have nexus with suspected/convicted drug traffickers from other jurisdictions as beneficiaires of international remittances from these foreign drug traffickers. This raises the possibility that SPs may be laundering or facilitating the laundering of drug proceeds. Further, there is an apparent use of DNFBPs (same lawyer as corporate secretary) in setting-up several SPs, some of which were alleged to have received funds from illicit activities.

The transactions involving the SPs also revealed a high level of cash-based transactions, which are highly susceptible to ML considering that the ultimate source and beneficiary of funds are unknown. Cash-based transactions tend to obscure the audit trail. It is,

therefore, possible that the SPs are being used to launder proceeds from illegal activities, considering that the substantial use of cash-based transactions (totaling in PhP billions) is not in line with its business model.

2. **Violations of The Electronic Commerce Act of 2000**

   In 2016, several STRs, totaling PhP4.8 billion, were filed on WG and EH, an Internet-based casino and SP. WG and EH were among the alleged recipients of funds from the B Bank heist (BBH). Several remittances and cash transactions were noted on the accounts of EH, which mostly originated from a money service business (MSB) suspected to have facilitated the transfer of proceeds from the BBH. A part of the transfers from the MSB to EH was presumed to have originated from WG.

3. **No underlying legal or trade obligation, purpose, or economic justification**

   Various Internet-based casinos and SPs made substantial remittances and cash transactions, totaling PhP4.07 billion. Majority of the STRs share similar typologies largely relating to the inability of providing sufficient supporting documents to justify multiple and significant remittances and cash transactions.

   a. In the case of CS, the bank reported that based on CS's submitted accreditation certificate, it is authorized to operate in a property in Pasay City. CS's customer information record with the bank, however, contained a Pasig City address. Further, the branch manager visited the declared business address, but the place was empty. CS made significant cash deposits, totaling PhP10.56 million from October to December 2018. Cash transactions range from PhP1 million to PhP3 million. The bank requested supporting documents, but CS failed to provide any.

   b. In another case, BC received various remittances, totaling USD14.99 million (PhP714.51 million) from 24 August 2015 to 14 November 2016. The CP views that the said remittances have no economic justification. The CP further narrated that BC claimed that the remittances came from authorized payment service providers. The CP, however, could not validate such claim. BC's account was also noted to have the same signatories as SI, who was also a subject of several STRs for having the same transaction pattern as BC. Both BC and SI are SPs.

4. **Deviation from the client's profile/past transactions**

   Between 2016 and 2019, the STRs filed on Internet-based casinos and SPs in relation to the aforementioned suspicious indicator amounted to PhP121.1 million.

   a. In one case, TD was the subject of two (2) STRs filed in March 2019, involving one (1) check encashment of PhP16.37 million and one (1) cash deposit of PhP18 million. The bank narrated that both transactions deviated from TD's usual transactional pattern of below PhP5 million. The bank further narrated that a TD representative allegedly said that the substantial deposit came from borrowings from a friend but did not provide any supporting documents.

5. **Amount involved is not commensurate with the business or financial capacity of the client**

The STRs filed using the above reason totaled PhP2.23 billion.

In 2018, VG, an SP, was the subject of several STRs involving various transactions from 2017 to 2018, particularly eight (8) check in-clearing transactions (PhP30.74 million), 122 cash deposits (PhP431.06 million), 58 check deposits (PhP247.15 million), 13 inter-account transfers (PhP119.75 million), and 1 ZSTR[7]. The bank narrated that it is closely monitoring the transactions of VG due to the large transactions being made, which range from PhP256,000.00 to PhP89 million. The bank further narrated that the client advised that the transactions are lease payments of various individuals and entities. The client, however, was unable to present supporting documents to justify the disclosed reason. The transactions were perceived as not commensurate with the client's declared source of funds.

6. **Client is not properly identified**

STRs related to suspicious indicator "client is not properly identified" totaled PhP231.75 million. The CPs narrated failure of the Internet-based casinos and SPs to provide minimum KYC information (e.g. incomplete registration documents, non-submission of gaming license, no minimum information on primary officers and beneficial owners).

7. **Fraud (swindling)**

Between 2013 and 2019, the STRs filed on Internet-based casinos and SPs in relation to fraud amounted to PhP121.1 million.

a. In one case, TRI, an SP, reportedly provided a loan agreement as supporting document for its remittance (USD50,000.00 or PhP2.49 million) to CTI, also an SP. Upon further inquiry, however, the client admitted that the real purpose of the remittance is for payment of a currency swap.

b. In another case, HI, an Internet-based casino, reportedly received three (3) remittances, totaling EUR625,250.00 (PhP36.87 million), from BK. Inconsistencies were noted on the address of BK (remitter) versus the document provided. Based on the remittance instruction, the remitter's address is in the United Kingdom (UK), but the service level agreement (SLA) provided by HI shows a Seychelless address. HI's representative initially implied that the Seychelles office of BK was a branch of the UK office. The bank, however, concluded that BK-UK and BK-Seychelles are two different entities. HI then submitted supporting documents, which were signed after the inward remittances. Also, when advised of the irregularities with the dates, they produced another SLA. The bank views the supporting documents as fabricated.

[7] The ZSTR code is used if the subject is not an accountholder of the covered person (CP) or is an accountholder but has no monetary transaction with the CP at the time the suspicious activity was determined.

SUSPICIOUS INDICATORS

- Large cash transactions
- Transaction seems to be inconsistent with the customer's apparent financial standing or the usual pattern of activities
- Activity is inconsistent with what is expected from the declared business
- Conflicting reasons and supporting documents for substantial transactions (wire transfer or cash-based)
- Unclear large foreign exchange transactions, which appear inconsistent with the SP's business model
- Use of formation agents that are not registered as DNFBPs with the AMLC
- International inward remittances from individuals in countries, where online gaming is prohibited (e.g. China)