Central Bank of Sri Lanka

News Survey

Volume 43 Number 1 January - March 2023

IN THIS ISSUE

ISSN 1391-3589

9 770002 301030

ISSN 1391 3589

Implications of Mobile Payment Services (MPS)

Thamara Senarathna
Deputy Superintendent
Employees' Provident Fund Department

1. Introduction

Mobile Payment Services (MPS) have become a popular and convenient way of making payments in the current context, where the position of the mobile phone has strengthened in the financial services value chain. MPS are the services provided by financial institutions, mobile service providers or banks that offer their customers an opportunity to process financial transactions remotely using mobile devices such as smartphones or tablets[1]. Basically, MPS are used for banking, payments, fund transfers and marketing. Unlike the related internet banking, MPS uses software, usually called mobile applications, provided by banks, mobile service providers or financial institution for this purpose.

Overall, mobile services provide a more convenient and sophisticated way of executing payments with their customers. Therefore, the end-users see mobile devices as a sophisticated and desirable technology that they can easily use to make their financial payments. However, applications of advanced and sophisticated technologies on payments are always linked with high risk factors. Therefore, a proper regulatory framework is required to combat and mitigate possible risks and threats associated with such state-of-the-art applications used in MPS.

2. Technologies of Mobile Financial Services and Mobile Products

2.1 Mobile Payment Technologies

As described in the IT Examination Handbook of Federal Financial Institutions Examination Council (FFIEC) published in April 2016, mobile service providers offer MPS using the technologies stated below.

2.1.1 Short Message Services (SMS)

The short text messaging services, provided by the Participating Financial Institutions (PFIs) or service providers to its' customers through mobile devices are identified as Short Message Services (SMS) and they are used to send or receive instructions of financial transactions among users and financial institutions (e.g. financial institutions request customer verification of transactions, communicate one-time passwords for activating online banking, sending account alerts… etc.).

1. Federal Financial Institutions Examination Council (FFIEC), IT Examination Handbook, 2016, April

2.1.2 Mobile-Enabled Web Sites

For the purpose of enhancing the customer experience based on the mobile device that they use (e.g. mobile phone, i-Pad), most of the financial institutions offer their customers to browse mobile-enabled web sites, in addition to their official websites. It provides a user-friendly, convenient and most appropriate format for viewing the web pages via mobile devices that the customer can use.

2.1.3 Mobile Applications

Downloadable software applications designed by mobile service providers or financial institutions, especially for handling financial transactions via mobile devices can be identified as mobile applications. It facilitates users to retrieve their transaction details, account balance inquires, utility bill payments, fund transfers and all other financial transactions through the mobile device. This technology provides a more user-friendly, unique service for any kind of mobile services such as mobile banking or web-based online banking to improve customer convenience.

2.1.4 Wireless Payment Technologies

With the increasing trend of smartphone dependency in society, numerous technologies have been discovered to facilitate consumers to make their financial payments through the mobile phones. Accordingly, with the purpose of accomplishing the customer requirements, wireless/contactless payment technologies have been introduced by financial institutions. Payments made by waving or tapping the wireless device, i.e payment card or smartphone over a reader for processing the payment can be defined as wireless payment. Customers can use mobile phone or payment card to execute contactless payments at Point-of-Sale (POS) or Person-to-Person (P2P) payments. Some of technologies that facilitate to operate wireless payments are as follows.

- ***Mobile Person-to-Person (P2P) -*** An online technology that provides a facility to make payment through a mobile device using the mobile phone number, bank account number or any other identifier of the receiver that are authorized by the service provider. Accordingly, users can download the P2P software application from their bank or financial institution that facilitates making financial payments to other individuals who are involved or enrolled in such a system.

- ***Near Field Communication (NFC) -*** A wireless technology which allows a mobile device to collect and interpret data from another closely located mobile device is called as Near Field Communication. A smartphone can be swiped at an NFC reader (which are being installed near the cash register of a store) to make a contactless payment. Credit card information of a smartphone user can be transmitted through the NFC device. In this scenario, the smartphone works as an NFC device and reader is the NFC tag. NFC is considered as a secured means of payment since NFC should occur only among closely located devices.

- ***Carrier-based technology -*** This is another modern mobile payment technology that allows mobile users to make payment directly through their mobile carrier accounts. In other words, payments are directly billed to a user's mobile carrier

account by a merchant. Carrier-based mobile payment facility is available for the customers who are using smartphones and featured phones. Customers can direct their payments to the receiving end by simply sending SMS message via their mobile phone evading the traditional payment channel. For example, carrier-based payment method can be used when making payments for online medical channeling services.

2.2 Mobile Products

Convenient and attractive mobile payment products have been introduced to fulfill the contemporary requirements of the customers for the current mobile banking platform. Accordingly, following products can be identified.

2.2.1 Mobile Wallet

This is an innovative product that allows its users to create an aggregate point of value from which to make purchases using a mobile device. It is somewhat similar to prepaid cards as it requires storage of value (money) prior to use and can be topped-up via cash payments at any participating bank or loading partner. Mobile wallet is a convenient way for a user to make in-store payments and can be used at merchants listed with the mobile wallet service provider. Once the funds are loaded the customers can make payments or transfer funds from their mobile wallet by using a mobile device.

2.2.2 Mobile Transfer

A facility given to customer who maintains a Mobile-Wallet to transfer funds to any recipient via mobile phone. Accordingly, sender can use the mobile device to manage, initiate or control fund transfers from his/her mobile wallet. This is a kind of extended facility of the mobile wallet that provides transfer of money to the receiver via mobile wallet in addition to make payments for goods and services. This would be a more convenient method of transferring money to receiver, where the sender can use the mobile phone to initiate, manage, track and control transfers from his/her mobile wallet. Receivers on the other hand can use their mobile wallet, prepaid card or bank account, to receive their remittances.

2.2.3 Mobile Voucher

This is an even more convenient and secure mobile product that can be used as alternative for paper-based money, off coupons and gift vouchers. Mobile voucher does not require carrying the physical voucher at the point of redemption and free from the risk of misplacing the same as it may be a text-based code sent through Short Messaging Service or secured encrypted code forwarded via Near Field Communications or a bar code sent through Multimedia Messaging Service (MMS) sent directly to mobile phone or mobile device.

However, caution must be exercised when using mobile based payments and messaging technologies in the current context, where innovation thrives across the world, as they are more prone to spams and cyber threats. Therefore, implementation of a proper regulatory framework with suitable security measures/controls to mitigate possible risks while ensuring customer protection and smooth functioning of the financial markets is essential in the current context.

3. Risks associated with Mobile Payment Services

The rapid rise in the usage of state-of-the-art technologies in the payment industry has increased

the exposure to various risks as the assailant is more vigilant on discovering weaker points of the payment process, to find opportunities to attack and grab undue benefits. Therefore, an appropriate strategic plan for timely identification and mitigation of possible risks associated with MPS is needed to establish a secured mobile payment system.

3.1 Operational Risk

Various types of risks such as SMS technology risk, mobile-enabled web site risk, mobile payment risk, mobile application risk can be identified when operating the various mobile financial services.

- ***SMS Technology Risk -*** Financial institutions, mostly use SMS notifications as part of two-factor authentication protocols or to convey one-time passwords. However, SMS technology consists of various security related risk factors. Messages are conveyed via broadly used networks allowing fraudsters to make various manipulations such as sending SMS messages to customers requesting for sensitive information, pretending that the messages were sent from formal institution. Accordingly, customers may be misled and once the sensitive information such as account information or other security information used to access the web pages or systems of financial institutions are revealed to the unauthorized person, it would aggravate the risks for the particular users.

- ***Mobile-Enabled Web Site Risk -*** As an extended service of the online banking platform, internet banking via mobile enabled internet browsers is becoming increasingly popular. Using the smartphone or tablet, customers can browse the websites. However, banking via mobile-enabled internet browsers also contains various vulnerabilities, such as malware attacks, fraudulent web applications…etc.

- ***Mobile Application Risk -*** Various types of custom-designed mobile applications have been installed into mobile devices by the manufacturers and those user-friendly applications can be downloaded onto the mobile smartphone or tablet. However, if a hacker or unauthorized third party may create fraudulent apps that are almost identical to the original application, customer may easily be misguided and that poses huge risks as fraudster can reach confidential sensitive information and screen entire communications/ transactions executes by such user.

  Further, many mobile applications gather and store personal details of users such as name, e-mail address, account number and any other confidential information along with user behaviors (location, payments patterns…etc) aiming to provide more convenient customer experience. However, attackers can make gain by grabbing such valuable sensitive information with the existence of unsecured mobile applications.

- ***Mobile Payments Risk -*** With the access of a fraudster to mobile phone or tablet, an unauthorized transaction (fund transfer, purchases, fraudulent payment requests…etc) can be occurred in any circumstance where a mobile device is stolen or misplaced as the confidential details of the customer are stored in such mobile device. Further, improper security features and controls in the process of mobile payment platform permits malicious

actors to make gains by creating fraudulent user accounts to execute fake transactions.

3.2 Strategic Risk

Risk factors associated with MPS and respective risk management strategies need to be included into the strategic plan of any financial institution and it is one of the major responsibilities of the governing body of any financial institution. Further, MPS that are planned to be offered by the banks or financial institution are required to be aligned with the goals and risk management strategies of the strategic plan, and failure of the same leads to heightened strategic risks.

3.3 Reputation Risk

It is the responsibility of the financial institution that provides MPS to enhance customer convenience, to ensure the security of the sensitive information and uninterrupted services. If third party services such as provision of technological facilities, data base management and network services are not properly provided accurately on a timely basis by the third party, the financial institution may be exposed to reputation risk. Therefore, the management team of a financial institution should consider the risk of reputation loss due to any failure of MPS provided by such institution.

3.4 Compliance Risk

Irrespective of any state-of-the-art technology adopted by the financial institutions to offer MPS for the enhancement of customer convenience that it is required to be comply with the rules, regulations, laws and regulatory expectations imposed by the regulator or governing body of such payment schemes. Proper regulations, policies and supervisory procedures need to be adopted in order to establish smooth operations of the MPS and ensure the security of both MPS provider and user. However, if financial institutions or the third-party service providers are not aware of or does not adhere to such regulatory requirements or supervisory guidelines issued by the regulator, compliance risks may arise.

4. Managing Risks of Mobile Payment Services

Risk management mechanism for mobile financial industry is critical compared to other financial services that may not be widely connected to the advanced technologies. However, mobile services consist of various players such as third-party service providers, application developers, network suppliers, mobile operators, manufactures of mobile devices…etc. and internal controls and other risk management strategies adopted by the service offering institution may not be sufficient for managing risks associated with MPS. Accordingly, proper risk management procedures and policies would need to be implemented to mitigate possible risks created with the interaction of all stakeholders who are engaging in providing MPS.

4.1 Managing Operational Risk

When offering MPS, the following operational risk mitigating measures would need to be considered by the financial institutions.

- ***Enrollment:*** Proper Know Your Customer (KYC) policy and controls need to be implemented when enrolling a customer into a mobile payment platform, supported by verification of customer credentials. Vigilance to avoid fraudulent activities is vital.

- ***Authentication and authorization:*** Depending on the type of technology used

and the associated risks, MPS providers should introduce a proper authentication and authorization process for executing mobile payments while mitigating fraudulent transactions. Biometric authentication process such as voice, facial recognitions, fingerprint or out of band authentication method such as authentication through one-time password forwarded through SMS can be used by the financial institutions to evade possible operational risks.

- ***Application security:*** Layered security measures or two factor authentication controls need to be imposed based on the volume and types of the transactions. Re-authentication process of the system can be mandated in circumstances, where the mobile device has not been in use in the MPS platform for a considerable time period.

- ***Contracts:*** As MPS consists of more players, appropriate legal contracts, terms and conditions among each of the players need to be well established to emphasize the responsibilities and tasks of each party to mitigate risks. Such contracts should clearly specify the types of information that are collected from customers and the types of data sharing mechanisms to manage possible operational risks.

- **Customer awareness, logging in and monitoring:** MPS providers should educate its users on secured means of operating mobile services while adhering to security standards prescribed by the regulator and service provider. Updated customer information to enable the download of mobile applications, to enable downloads only from reliable sources and the availability of links to download mobile applications that are approved by the service provider in their official web page, would help avoid browsing and downloading unauthorized fake mobile applications which permit fraudsters to reach sensitive customer credentials. Additional controls or validation to verify user access to web pages and execution of regular scanning process for vulnerabilities can also be imposed. The management of financial institutions should monitor all MPS activities regularly to evade unauthorized malicious attempts.

Further, considering the management of SMS technology risks, security of the Personal Identification Number (PIN) can be enhanced by mandating the requirement of changing PIN frequently. MPS providers can design mobile application to guarantee that sensitive information namely, credit card numbers, account numbers or passwords does not exist directly on a device.

Customers should be informed to secure their mobile device by setting complex passwords for both, the mobile device and the mobile applications. The auto-wipe mechanism after three attempts of failure in entering correct password need to be imposed as security control measures to mitigate MPS related risks. Further, introducing a "Regulatory Sandbox" i.e. testing environment provided by the regulator for new software applications to avoid possible risks related to malicious software applications and products would facilitate the mitigation of potential risks of MPS.

"Tokenization", i.e. considering the security of sensitive data, the method of substituting confidential customer credentials with a proxy value

as tokens can be used as security control measures to manage various MPS related application risks.

4.2 Managing Strategic Risk

Depending on the types of mobile services and products that are expected to be offered, a financial institution should give more weight for such MPS in their strategic plan. Appropriate risk management strategies are required to be incorporated in successive strategic plans with respect to software applications, designs, customer expectations, user limits and third-party involvement as service providers to manage potential strategic risks.

4.3 Managing Reputation and Compliance Risk

Financial institutions should ensure proper security control measures to secure sensitive information of customers and security of mobile applications provided by formal service providers, mitigate fraudulent activities related to MPS, develop and implement contingency plans to ensure uninterrupted services and mitigate potential risks of MPS to protect the reputation of the financial institutions.

In order to mitigate compliance risk of a financial institution that offers MPS, measures and procedures to examine full accessibility of applicable disclosure requirements on the mobile phone or tablet, review the existing legal and compliance management procedure related to MPS, determine regulatory and legal requirements/ amendments that are applicable to innovative mobile services and products offered by such financial institution on regular basis to comply with regulatory standards and enhance awareness and train staff of the financial institution on possible implications of compliance issues of MPS can be implemented.

5. Regulatory Measures on Mobile Payment Services in Sri Lanka

Central Bank of Sri Lanka (CBSL) has taken several measures to regulate MPS and mitigate potential risks associated with mobile financial services in Sri Lanka. Accordingly, both customer account based mobile payment systems providers (mobile phone banking) and mobile phone-based e-money system providers are required to obtain licenses from the CBSL to provide mobile financial services in Sri Lanka. Utilization of payment related mobile applications has become popular in the current context. Therefore, in order to standardize information security measures adopted by MPS providers who introduced mobile applications and to establish minimum acceptable security arrangements to secure transactions carried out using mobile applications, CBSL issued minimum compliance standards for mobile applications that provide financial services. Accordingly, all MPS providers who introduced mobile applications are required to perform their functions adhering to the minimum compliance standards for payment related mobile applications imposed by the CBSL.

Further, the following Regulations and Guidelines were issued by the CBSL[2] to ensure smooth and proper functioning of MPS in Sri Lanka and all MPS providers are required to comply with such regulatory requirements.

- Payment Cards and Mobile Payment Systems Regulations No. 1 of 2013
- Mobile Payments Guidelines No.1 of 2011 for Bank-led Mobile Payment Services
- Mobile Payments Guidelines No.2 of 2011 for Custodian Account Based Mobile Payment Services

2. Central Bank of Sri Lanka, Payments Bulletin (2022): Second Quarter

- Guideline No.1 of 2018 (revised in 2020) on Minimum Compliance Standards for Payment related Mobile Applications
- Payment and Settlement Systems Circular No. 13 of 2020 – Mandating Licensed Commercial Banks incorporated in Sri Lanka and Licensed Operators of Mobile Phone Based E-money Systems to join LANKAQR

In addition, the CBSL conducts on-site and off-site supervisions to examine whether the mobile financial service providers are complying with the regulatory requirements imposed by the CBSL. Further, CBSL evaluates various financial solutions proposed by MPS providers in order to establish sound and stable mobile payment system while ensuring the safety of customer credentials and the entire payment network.

6. Conclusion

Financial institutions have introduced a wide array of mobile financial services that consist of innovative products and state-of-the-art technologies to accomplish modern customer needs and enhance their convenience. Since advanced technologies and user-friendly mobile applications are more prone to risks and fraudulent activities, risk identification, risk assessment, implementation of appropriate and effective risk management strategies and conducting on-site and off-site supervision are vital for the safeguard of both MPS users and providers and ultimately establishment of a sound mobile financial service platform to ensure financial system stability.

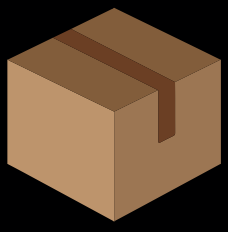
References:

Central Bank of Sri Lanka, Payments Bulletin, various issues.

Federal Financial Institutions Examination Council (FFIEC), IT Examination Handbook, (2016): April.

DON'T FALL FOR SCAMS!

Parcel scam



- Valuable gifts
- Messages from a stranger
- Requests payment of multiple fees

Lottery scam

- Unexpected winnings
- Messages from a stranger
- Requests payment of fees and charges

Employment scam

- Perfect job with great benefits
- Ready to hire immediately
- Asks for cash to start off

Romance scam

- Promises to marry
- Plans to build a house
- Asks for financial help

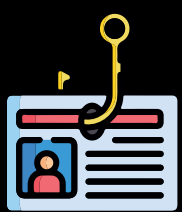
Product scam

- Benefits too greater than costs
- Unwilling for physical inspection of goods
- Asks for advance payments

Charity scam

- A charity too-good-to-be-true
- Requests for urgent donations
- Asks for personal financial information

Identity theft



- A stranger asks for personal information
- Missing identification documents
- Attempted unauthorized access to financial data

Cryptocurrency scam

- Quick benefits within a short time
- Marketing at its best
- Not under any regulatory authority

Corporate scam

- Spam emails
- Hacked databases
- Stolen or manipulated assets

Think twice before trusting

Protect your personal data

Ask questions

Don't get caught up in trends

Know what happens to your money

Seek help

A message from the Financial Intelligence Unit of the Central Bank of Sri Lanka

www.fiusrilanka.gov.lk ☎ 0112 477125 / 0112 477509

Necessity of an Independent Fiscal Institution for Sri Lanka

K.A.U.S.K. Thilakarathne
Deputy Superintendent
Public Debt Department

Background

Governments run on revenues collected from various sources and rely on borrowings to meet their deficits. Government revenue in Sri Lanka, as a percentage of the Gross Domestic Product (GDP), has continuously declined over the past three decades. This has been identified as one of the main reasons for the current economic crisis faced by Sri Lanka. Government revenue and grants as a percentage of GDP, which recorded 24.0 percent in 1989 had dropped to 17.2 percent by 2000, and has declined further to 8.3 percent in 2021; categorizing Sri Lanka among the ten lowest government revenue earning countries in the world in 2021.[1]

Although Sri Lanka's government revenue remains abysmally low by global standards, its government revenue has always been forecasted at a high level in the budgetary estimates and the medium term macro fiscal frameworks developed from time to time. Although government revenue collection declined significantly compared to the budgetary estimates, there was no commensurate decrease in government expenditure but remained closer to the planned level; leading to larger budget deficits than expected. As a result, the Government was forced to rely on borrowings to finance the budget deficit; which in turn, caused a significant increase in the level of government debt. In order to overcome this unfavourable situation, an institution should be set up with an official mandate to review all considerable deviations of the fiscal performance from the forecasted values and prevent expenditures from ballooning over time. Such an institution would be entrusted to provide information about deviations from the targets to fiscal authorities, to help identify the required reforms and to introduce them efficiently to convert the fiscal position again to a better level, on a continuous basis. It would also be responsible for analyzing the fiscal policy independently, streamlining and prioritizing them. Accordingly, the establishment of an Independent Fiscal Institution (IFI) would be beneficial for Sri Lanka in the current context, as it would help prioritize fiscal policies and ensure the fiscal expenditures are maintained within the stipulated limits.

[1] International Monetary Fund, 2022

Introduction of Independent Fiscal Institutions

IFIs / Councils are non-partisan, technical bodies entrusted with a public finance watchdog role.[2] Otherwise, IFIs are defined as independent, non-partisan agencies with an official mandate to assess fiscal policies, plans, rules and performance.[3]

Evolution of Independent Fiscal Institutions

High Council of Finance established in Belgium in 1936 is considered as the world's first IFI.[4] By 2021, 51 IFIs were functioning in 49 countries of the world (Table 1). Around two thirds of these institutions were established after the 2007-2010 Global Financial Crisis. It is evident that IFIs have been established in developed countries, in emerging economies such as Brazil, Chile, Iran, Peru and Uruguay as well as in developing countries such as Kenya and Vietnam.

Main functions of Independent Fiscal Institutions[5]

1. Independent analysis, review and monitoring of government's fiscal policies, plans and performance
2. Developing or reviewing macroeconomic and/or budgetary projections
3. Costing of budget and policy proposals, including possibly, election platforms
4. Advising policy makers on policy options

Principles for Independent Fiscal Institutions[6]

The 22 principles for IFIs are grouped under 9 broad headings.

1. Local Ownership

Necessity of an IFI requires national ownership and, there should be commitment and consensus across the political spectrum. Moreover, determination of functions of the IFI should be based on the fiscal framework of the country and specific issues that need to be addressed.

2. Independence and Non-Partisanship

Analysis of IFI should not be presented from a political perspective. Moreover, appointment of heads/leadership of the IFI should be based on competency and technical skills, without political interference. The term of office of heads and the number of years that the heads of the IFI may serve should be clearly specified in legislation, while the term of office should be different from that of the election cycle. The position of the head of the IFI should be a full time job and should be a remunerated. The head of the IFI should have full freedom to hire and dismiss employees in accordance with applicable labour laws. Employees of the institution should be recruited based on merit and technical competency without reference to political affiliation.

3. Mandate

The mandate of the IFIs should be clearly defined in higher level legislation of the country. The general types of reports and analyses they are to produce, who may request for reports and analyses and associated timelines before their release, should be clearly specified. Further, the IFI should have the scope to provide reports and analyses at their own initiative, provided that they are consistent with their mandate. Clear links to the budget process should be established within the mandate. This

---

[2] Beetsms R. and others, 2018

[3] International Monetary Fund, 2017

[4] George G. and Bogdan C., 2020

[5] International Monetary Fund, 2013

[6] Organisation for Economic Co-operation and Development

might include economic and fiscal projections, baseline projections, analyses on budget proposals, monitoring compliance with fiscal rules or deviations from budgetary targets, costing of major proposals and analysing selected issues.

4. Resources

The resources allocated to the IFI must be commensurate with their mandate. These allocations should be published. Multiannual funding commitments may provide additional protection from political pressure.

5. Relationship with the Legislature

Sufficient time should be provided to IFI to carry out analyses required for parliamentary work. Additionally, the relationship between the IFI and parliamentary committees should be clearly established in legislation.

6. Access to Information

The law must ensure the ability to obtain any relevant information on a timely basis, including methodology and assumptions underlying the budget and other fiscal proposals. Further, any restrictions to access government information should be clearly defined in legislation. These safeguards may be put in place to ensure protection of privacy and sensitive information in the areas of national defense and security.

7. Transparency

Full transparency in the work and operations of the IFI provides the protection of the independence of the IFI and allows them to build credibility with the public. Further, the reports and the analyses of the IFI should be published and made freely available to all. The release dates of major reports and analyses of the IFI should be formally established in order to coordinate them with the release of relevant government reports and analyses. The IFI should release reports and analyses in their own name.

8. Communications

IFIs should develop effective communication channels with media, civil organisations, and the other stakeholders.

9. External evaluation

IFI should develop a mechanism for external evaluation of their work by a local or international party.

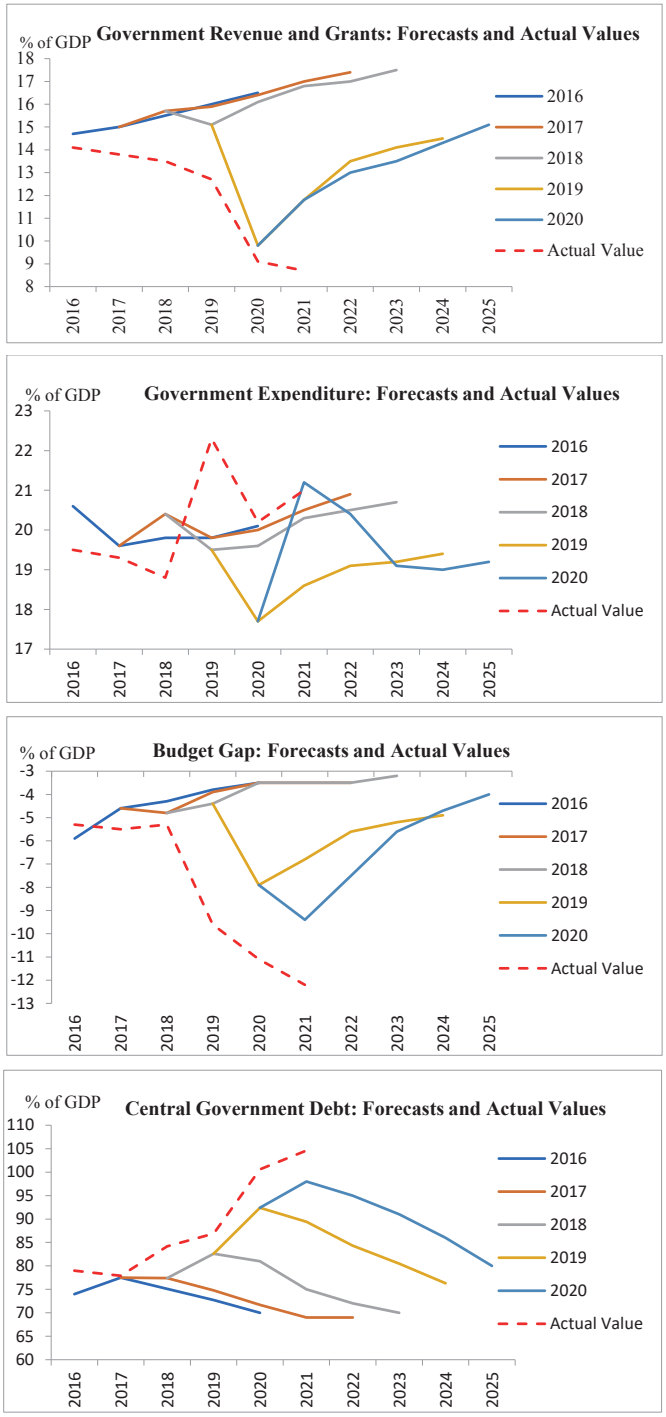
Does Sri Lanka need an Independent Fiscal Institution?

Weak actual performance compared to the budgetary forecasts is one of the major issues faced by Sri Lanka pertaining to fiscal sector.

According to the data, it is evident that budgetary estimations and the projections included in the medium term macro fiscal framework lack reliability. Further, it is apparent that although Sri Lanka has initiated fiscal rules, country has deviated from those targets most of the time and the level of government debt ranks higher compared to the other similar countries.

Currently the reasons discussed above have led to the establishment of IFIs in a number of countries in the world. However, in order to establish an IFI, political consensus and commitment is required. Further, attention should be paid to the principles that should be adhered for establishing such IFIs. In addition, introduction of fiscal rules is essential for the success of the IFIs and financing the deviations of the budgetary targets through borrowings could be minimised using fiscal rules.

Figure 1
Budgetary Estimates and Actual Values



Source: Central Bank of Sri Lanka, Annual Reports

Hence, establishing an Independent Fiscal Institution in Sri Lanka would not be a short term measure to resolve the current economic crisis of the country, however, it would be beneficial if it is incorporated as a part of the long term macroeconomic restructuring process.

Table 1
Independent Fiscal Institutions

Country	Independent Fiscal Institutions
Australia	Parliamentary Budget Office
Austria	Fiscal Advisory Council
Bahamas	Fiscal Responsibility Council
Belgium	High Council of Finance - Public Sector Borrowing Section
Belgium	Federal Planning Bureau
Brazil	Independent Fiscal Institution
Bulgaria	Fiscal Council
Canada	Parliamentary Budget Office
Chile	Autonomous Fiscal Council
Colombia	Comite Consultivo para la Regla Fiscal
Costa Rica	Consejo Fiscal Independiente (Independent Fiscal Council)
Croatia	Fiscal Policy Commission
Cyprus	Fiscal Council
Czech Republic	The Czech Fiscal Council
Denmark	Danish Economic Council
Estonia	Fiscal Council
Finland	National Audit Office of Finland
France	High Council of Public Finance
Georgia	Parliamentary Budget Office
Germany	Independent Advisory Board to the German Stability Council (Unabhängiger Beirat des Stabilitätsrats)
Greece	Parliamentary Budget Office
Grenada	Fiscal Responsibility Oversight Committee
Hungary	Fiscal Council
Iran	Public sector Directorate of Parliament (Majlis) Research Center
Iceland	Fiscal Council
Ireland	Irish Fiscal Advisory Council
Italy	Parliamentary Budget Office
Kenya	Parliamentary Budget Office
Latvia	Fiscal Discipline Council
Lithuania	National Audit Office
Luxembourg	National Council of Public Finance
Malta	Malta Fiscal Advisory Council
Mexico	Centre for Public Finance Studies
Netherlands	Netherlands Bureau for Economic Policy Analysis
Netherlands	Raad van State
Panama	Fiscal council
Peru	Consejo Fiscal
Portugal	Portuguese Public Finance Council

Romania	Fiscal Council
Serbia	Fiscal Council
Slovak Republic	Council for Budget Responsibility
Slovenia	Fiscal Council
South Africa	Parliamentary Budget Office
Korea	National Assembly Budget Office
Spain	Independent Authority of Fiscal Responsibility
Sweden	Swedish Fiscal Policy Council
Uganda	Parliamentary Budget Office
United Kingdom	Office for Budget Responsibility
United States	Congressional Budget Office
Uruguay	Consejo Fiscal Asesor
Vietnam	National Assembly Financial and Budgetary Committee

Source: Fiscal Council Dataset, International Monetary Fund

References

Central Bank of Sri Lanka *Annual Reports*. Central Bank of Sri Lanka, Colombo 01.

Beetsma R. *et al*. (2018) *Independent Fiscal Councils: Recent Trends and Performance, Working Paper*. International Monetary Fund, Washington, D.C.

George G. and Bogdan C. (2020) *Fiscal Councils in European Union: A short retrospective review and current challenges in terms of functionality and effectiveness, Working Paper*. Romanian Fiscal Council

Hamid R. *et al*. (2022) *Fiscal Rules and Fiscal Councils, Working Paper*. International Monetary Fund, Washington, D.C.

International Monetary Fund. (2022) *Fiscal Monitor, APR 2022*. International Monetary Fund, Washington, D.C.

International Monetary Fund. (2013) *The Functions and Impact of Fiscal Councils*. International Monetary Fund, Washington, D.C.

International Monetary Fund. (2017) *The Fiscal Council Dataset: A Primer to the 2016 Vintage*. International Monetary Fund, Washington, D.C.

Trapp L. and Nicol S. *Designing effective independent fiscal institutions*. OECD

A message from the Central Bank of Sri Lanka

PYRAMID RACKETEERS GET PUNISHED!

It is a criminal offense to initiate, introduce, advertise, publicize, maintain and invest, manage or direct prohibited pyramid schemes.

Violators face heavy fines and up to five years imprisonment.

DON'T GET CAUGHT UP IN THE PYRAMID SCHEMES.

Save your hard-earned money!
Protect Yourself!

Director
Resolution and Enforcement Department
Central Bank of Sri Lanka

Contact
☎ 0112 477262, 0112 477157
0112 477748
dred@cbsl.lk

Regulating the Casino Sector, Post-Covid-19

Dr. Ayesh I Ariyasinghe
Deputy Director
Financial Intelligence Unit

1.1 Introduction

A vibrant gaming and entertainment sector is a magnet to attract tourists in search of entertainment tourism. Casinos play a large role in 'pulling' tourists[1]seeking to be entertained (Carvalho, et al., 2022), and tourists who want to spend money to get larger benefits that are difficult to attain under real life circumstances (FinanceMonthly, 2019). Sri Lanka stands to gain from such attractions offered, increasing the revenue from tourism. However, the absence of a supervisory mechanism may lead casinos and gaming sector to be abused by money launderers and other criminal elements. Criminals could use casinos to transform their illegal proceeds to appear as earned through gambling earnings. Historically, there are many global examples of casinos being used as a front organization for criminal syndicates to launder ill-gotten wealth. While casinos offer policymakers a rich avenue of revenue to utilize, and attract more tourists to Sri Lanka, it is important to have in place necessary safeguards, proper licensing, regulatory oversight, occasional supervision, and streamlining of support services utilized by casinos.

The Financial Action Task Force- more widely known as FATF, as the global anti money laundering and countering financing of terrorism (AML/CFT) policymaking body, requires casinos in any jurisdiction to be under AML/CFT regulatory oversight. However, lack of proper regime to licensing, and entry of COVID-19 pandemic has placed restrictions on casino sector oversight as required by the FATF. As the AML/CFT supervisor of casinos in the island, the Financial Intelligence Unit of the Central Bank of Sri Lanka (hereafter, FIU), is vested with the AML/CFT supervisory responsibility as casinos come within the Designated Non-Finance Businesses (and Professions) (DNFBPs for short) category under the Financial Transactions Reporting Act, No. 6 of 2006 (FTRA).

Since of 2018, the FIU-Sri Lanka has been carrying out three types of supervisory oversight and related activities called onsite supervision, off-

[1] 'push' and 'pull' factors often provide the backbone for studies surrounding tourism literature.

site supervision, and thematic or spot supervision - among the DNFBP sector. However, the COVID-19 pandemic has posed several challenges for the regulators in performing regulatory oversight examinations effectively.

The world had come to terms and tried to adapt to the mutation phases of the SARS-CoV-2 virus, by application of newly developed vaccinations, social distancing and limiting contact as cited as a preventive mechanism(Shereen, et al., 2020). This had been termed as the "new normal" for businesses to function by taking necessary preventive precautions. The pandemic had required the regulators to revise their tried and tested oversight mechanisms to fit the "new normal" to best suit the supervisory functions, and to be carried out in stages according to the intensity of the pandemic, while ensuring personnel and operational restrictions are safeguarded and precautions are adopted to face the mutations observed during the COVID-19 pandemic. Considering the casino and related gaming sector, COVID threat looms ever so large due to the close contact gaming environs, face-to-face interactive nature of the playing customers. Globally, casinos had been hard hit by the social distancing regulations issued by the medical authorities as a precaution (Centers for Disease Control and Prevention, 2020). Due to restrictions, most jurisdictions have required casinos and gaming institutions to be closed, while handful of jurisdictions have allowed gaming activities to continue by maintaining distancing policies during operations. Sri Lanka too restricted the casinos, from carrying out face-to-face gaming activities. However, the "new normal" popularized online gambling operations, and casinos are reported as carrying out such activities although being closed for regular customers. This new trend had prompted the AML/CFT regulator to keep close track of casino operations, using different supervisory techniques.

1.2 Casino sector in Sri Lanka and the regulatory environment

In the past, Sri Lanka has had several establishments dedicated to "gaming and recreation", as it was known at the time. Gaming had been limited to cards, played for money, with some early records referring to the Colombo Recreation Club, and to the Atlanta Club. Since economic liberalization in 1977, casino gaming was carried out by three casinos called the Ritz, W. Bros Casino and the Palm Beach Club casino. These casinos issued their own gaming tokens, made from brass or nickel cuprite mixed alloy, with tokens valued at Rs. 10 or Rs. 20[2].

Furthermore, the casino sector was brought under a levy applicable through the Betting and Gaming Levy Act introduced in 1988. The Betting and Gaming Levy Act[3] identified what constitutes as a gaming place and the entity's requirement to pay a levy, which changed from time to time (Table-1). The present levy applicable from January 1, 2023, is Rs. 500 million, increased from Rs. 200 million imposed on April 1, 2015.

In 1991, all casino and slot machines were banned in Sri Lanka by a presidential decree of President R. Premadasa. However, several illicit gaming activities remained and according to media reports, numerous raids carried out from time to time identified illicit gambling 'dens' that were unauthorized and illegal. In 2002, casinos were permitted to recommence with limited operations, with five land-based casinos operational between

2 Source: https://coins.lakdiva.org/casino/w_bros_casino_lk.html (accessed Sep. 22, 2022)

3 The Betting and Gaming Levy Act, No. 40 of 1988

Table – 1: Changes to the Betting and Gaming Levy (since 1988) Applicable to Gaming Institution carrying out Casino and Rujino[4]

Year	Levy (in Rupees)
April 1, 1988	1 million
April 1, 2001	25 million
April 1, 2002	12 million
April 1, 2005	50 million
April 1, 2013	100 million
April 1, 2015	200 million
January 1, 2023*	500 million

* Based on the proposed amendments to the B&GL Act (As per Appropriation Bill 2022)

Source: Ministry of Finance (numerous annual reports), Inland Revenue Department

Kollupitiya and Dehiwala. These were Stardust, Marina, Bellagio, Bally's, and MGM. It appears that many Sri Lankan casinos carry the names of more popular counterparts in the USA to create a sense of familiarity among the casino participants who frequently travel around the casino and gaming circuits. However, the Sri Lankan casinos do not have any formal business or franchise links to its namesake US casinos.

At present, although many websites in relation to gaming activities refer to five operational casinos in Colombo area, operationally, Sri Lanka's casino sector is reduced to three land-based casinos (LCB Network PLC, 2006; Howe & Newton, 2015). The reduction was cited as business viability concerns by the owners, while several cited reasons such as burdensome levies, and operational limitations due to unlicensed operations.

Although operationally active, Sri Lanka's casinos did not have a sector regulator. Until the end of August 2022, the sector did not have a designated authority to grant licenses or issue and monitor the entry and exit requirements of a casino operative institution. Much of this policy uncertainty was owed to the sociological, cultural, and religious pressure surrounding the concept of gambling trumping over the political will to have a regulatory environment for casinos. However, from time to time, attempts to reignite the gaming sector as a viable tourist attraction for Sri Lanka resulted in the legislature passing a law to license the Casino Sector, the Casino Business (Regulation) Act, No. 17 of 2010 that speaks of a licensing regime that is carried out by the Secretary to the Ministry of the Minister in charge of the subject of casino business[5]. The Casino Business Act is a Minister-centric piece of legislation, where licensing powers are set out as per Ministerial regulation and does not refer to appointment of any regulatory authority. Furthermore, the act speaks of the Minister having the power to make regulations, and terms and conditions of the license issued to any casino business, the fees charges,

Table-2: Land-based Casinos in Colombo, Sri Lanka (as of Oct. 01, 2022)

Location	Number	Table Games	Slot Machines	Poker Tables	Total Casino-sq./Ft
Colombo	5	178	134	40	32,000

[4] A casino game which is identified within the definition of a 'gaming' place

[5] Section 2(1) and 2(2) of the Casino Business (Regulation) Act, No. 17 of 2010

procedure for cancellation etc. Prior to August 31, 2022, successive governments had purposefully or unwittingly, designed to overlook appointing the law as a subject coming within the purview of any cabinet minister, thereby enabling such Minister to oversee the subject of the casino business. This lacuna led to the casino regulation law to remain redundant.

However, on August 31, 2022, the casino regulation was signed by the President Ranil Wickramasinghe in his capacity as the Minister of Finance. The Regulation, titled Casino Business Licensing Regulation, No. 1 of 2022, identifies the licensing requirements, renewal, licensing fee, cancellation and grounds for inquiry, appointment of a compliance officer, conduct within the casino and such other related matters.

In addition to this law and regulation, another elaborate piece of law enables casinos to carry out payment of a gaming levy to the Inland Revenue Department, the taxation authority of the country. The Betting and Gaming Levy Act, No. 40 of 1988 and its amendments including the Act, No. 14 of 2015, imposes the levy upon the casinos. Furthermore, Part II of the Finance Act, No. 10 of 2015 also required a casino industry levy from 'persons who are engaged in the business of a casino' to pay a Casino Industry Levy of Rupees one billion per casino[5]. Payments were to be collected by the Commissioner General of Inland Revenue with summary collection powers due to any default in payment of levy was vested on the Magistrates' court within which jurisdiction, the defaulter's place of business, residence would come under[6].

Casino definition is also important in this aspect, especially in the absence of a sector regulator or a licensing authority in the past. The Betting and Gaming Levy Act of 1988, as amended, defines "gaming"[8];

> *'means the playing of any game for a stake, and includes the playing of Baccarat, Punto banco, big six, Blackjack, boule, Chemin–de-fer, Chuck – a – luck, Crown and anchor, Faro, Faro bank, Hazard, Poker dice, Pontoon, American for French roulette, Trente – et – Quarante, Vingt – et – um or Wheel of Fortune at any premises to which individuals have access– (a) with or without payment; (b) whether as of right or not'.*

This definition has proceeded to identify a casino by its games carried out within the premises.

Similar definition can be found in the Finance Act of 2015, which imposed a hefty levy against a 'person who is engaged in the business of a casino,' interpreting the term "casino" to refer to as:

> *'…any premises to which individuals have access— (a) with or without payment; (b) whether as of right or not, for the playing of any game for a stake and includes the playing of baccarat, punto banco, big six, black jack, boule, Chemins - de - fer, chuck - a - luck, crown and anchor, faro, faro bank, hazard, poker dice, pontoon, American French roulette, Trente - et - quarante, vingt - et - um, or wheel of fortune or any other game which the Minister may from time to time by Order published in the Gazette, specify.'*[9]

---

6 Section 6(1) and 6(2) of the Finance Act, No. 10 of 2015 – However, this provision was not carried out.

7 Section 7 and Section 8 of the Finance Act

8 Section 7 of the Betting and Gaming Levy Act of 1988

9 Sections 6 and 7 of the Finance Act, and Section 5 of the Casino Business (Regulation) Act

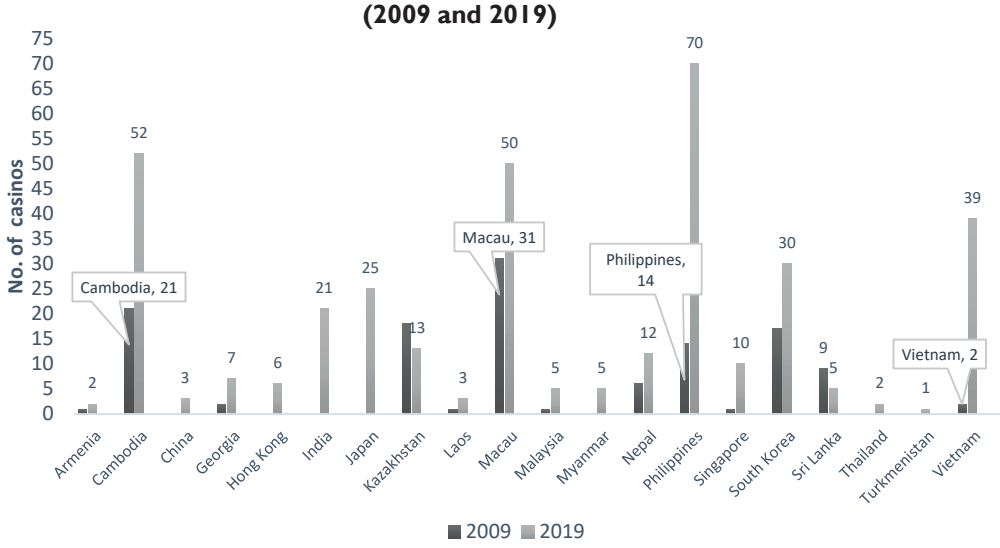
It appears that the Finance Act had borrowed the Casino definition from the Casino Business (Regulations) Act, No. 17 of 2010. Until August 2022, the legality surrounding Sri Lankan casino sector has been unclear. From 2002 to 2022 August, the land-based casinos operating in Colombo and Dehiwala have neither been declared as illegal nor legal as per the existing law. Furthermore, the government had raised levies and charged gaming levies from the casinos from time to time. The casinos designated were not licensed due to the absence of a licensing authority, until now. This was largely due to the absence of a Ministerial appointment to oversee the Casino Business (Regulations) Act.

With the introduction of the licensing requirements by way of Regulation, the casinos are now well placed to apply for licensing, and to be governed with regulatory mandates on their operations as set out by the Regulation. Furthermore, the Casino Business Act does not provide player protection. The Regulation also prohibits minors from entering or taking part in the games run within the premises.

There are no online casino operators based in Sri Lanka. The prevailing law does not place any bar on citizens or residents from playing online casino gaming. Due to the absence of legal protection and lack of regulation over player protection in the country, any ramifications would be borne by the player and would not get noticed by the AML/CFT regulator. However, with the Annual Appropriation Act for 2023 passed in the parliament, the registration of online gambling has also been introduced. The mechanism to carry this out is yet to be determined.

Apart from these provisions of law, Sri Lanka does not permit any foreign investor or an overseas company to engage in any commercial, trading, and industrial activities relating to lotteries within the Sri Lankan legal jurisdiction[10].

Figure 1: Land-based Casinos - Central and Eastern Asia (2009 and 2019)



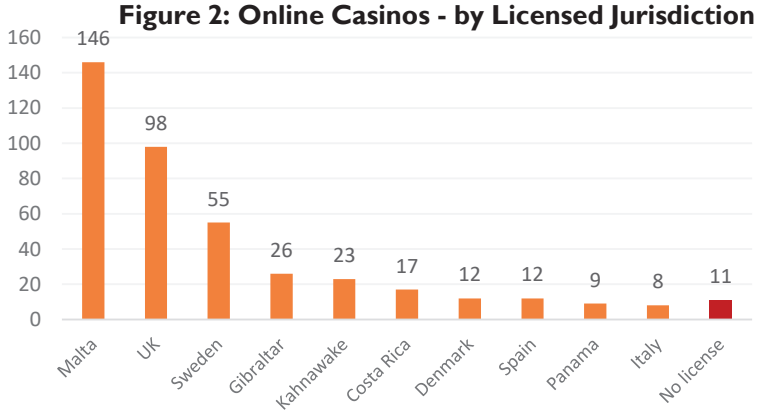
Source: Author's compilation based on data sourced from www.worldcasinodirectory.com

[10] The Foreign Exchange Act, No. 12 of 2017 – Regulation 2(b) Part II Clause A- 4(2) and of B 2 of the Schedule to the Foreign Exchange (Classes of Capital Transactions in Foreign Exchange Carried on by Authorized Dealers) Regulations, No. 1 of 2017, dated 17.11.2017.

Although deemed as high-risk sector for any jurisdiction, it is noteworthy that the number of casino institutions has increased in the Eastern and Central Asian region jurisdictions. This may be a result of governments recognizing the casinos' increased contribution for the national economy by way of gaming revenue tariffs and duties. Therefore, effective management, licensing, and supervision of this highly controversial and challenging sector would provide much needed short to medium term foreign exchange revenue.

Irrespective of being faced with a deadly pandemic, AML/CFT supervisor for the casino sector is required to follow the FATF's 40 Recommendations, of which, Recommendations 22, 23, and 28 set out the specific conduct expected from the DNFBPs category (FATF, 2020) and within it, the casino sector supervision. The following FATF Recommendations directly and indirectly apply to the casino sector.

Figure 2: Online Casinos - by Licensed Jurisdiction[1]



Source: Author's compilation based on data sourced from www.worldcasinodirectory.com

[1] No. of online casinos were less than 5 for US-New Jersey, Antigua and Barbuda, Philippines, Anjouan, Portugal, Ireland, Estonia; while BVI, St. Kitts and Nevis, Belgium, Serbia, Jersey, Germany, and Cyprus had only one registered online casino.

COVID-19 pandemic led to the industry pivoting towards non-physical online gambling, which rose in popularity (FATF-GAFI, 2020). This trend also saw an increase in unlicensed gambling sites as shown in Figure 2.

1.3 FATF Responsibilities Cast on the Casino and Gaming Sector

The COVID-19 pandemic was identified by the FATF as impacting the abilities of the government and private sectors to implement AML/CFT obligations for supervision, regulation, and policy reforms, to suspicious transaction reporting, and international cooperation (FATF-GAFI, 2020).

○ The European Union 4th and 5th Directives

The European Union (EU) 4th Directive on ML identifies casinos within the gambling services definition. Under the EU AML framework, gambling services are defined as services which involve wagering a stake with monetary value in games of chance, including those with an element of skill such as lotteries, casino games, poker games and betting transactions that are provided at a physical location, or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services. When carrying out a wagering activity (or betting) above EUR

Table-3: FATF Recommendations Relevant for the Casino Sector

Main FATF Recommendations	Main Rec. Focus (Sri Lanka's current rating)	Complimentary Recommendations
22	Customer Due Diligence: (Largely Compliant)	R. 10 (Customer Due Diligence) R. 11 (Record Keeping) R. 12 (Politically Exposed Persons) R. 15 (New Technologies) R. 17 (Reliance on Third Parties)
23	Reporting Suspicious Transactions: (Compliant)	R. 18 (Internal Controls, Foreign Branches and Subsidiaries) R. 19 (High Risk Countries) R. 20 (Reporting of Suspicious Transaction) R. 21 (Tipping-off and Confidentiality)
28	Supervision and Monitoring (Partially Compliant)	R. 35 (Sanctions)

Source: Compiled by author based on FATF (2021-July)

2,000 the customer due diligence is applied by the institution. All member states of the EU are required to apply to these mandates, and the only exception is where a member state is identifying the sector as a low risk for ML/TF concerns. Even so, the member state is required to inform the EU Commission.

The EU report also identifies this sector as a fast-growing sector, with the use of high technological input. Therefore, member states are required to carry out supervisory activities to supervise the institutions via designated authorities that are charged with setting out the anti-money laundering guidance to these institutions they supervise.

1.4 COVID-19 and its Impact on the Gaming Sector Supervision

Casinos have interactive games and "at-the-institution" based close contact playing arrangements, and gaming tables arranged with at least 4-8 people participating per table. Due to this factor, casinos are high-risk environments in terms of COVID related guidelines. Further, the fact that most of the customers are visitors to the country, who may have had a greater exposure to the Corona virus in their own jurisdictions, casino environments could be termed as a hotbed for the pandemic to spread and an environment open to easy contamination (Ghaharian & Bernhard, 2020). In such an environment, the on-site the regulators have an unenviable job to balance in terms of the AML/CFT supervisory needs while safeguarding their health by preventing exposure to COVID carriers.

Under normal circumstances, the supervisory activities relating to the gaming sector would be as shown in Figure-3. However, with the advent of the COVID-19 pandemic related departure from normalcy, the situation is envisaged as changed to Figure-4 formalities.

1.5 Sri Lanka's Efforts at Risk based Supervision of Casinos

AML/CFT risk based supervision of the casino sector involves understanding the sector's ML/TF risks, and undertaking risk assessments from time to time, and developing adequate mitigation methods and control strategies to address these risks. Every year, during the months of November - December, information is collected from the casino institutions via a detailed risk assessment questionnaire. Based on the survey responses received from the compliance officers of the casinos, the FIU evaluates the ML/TF risk of the casino for the upcoming year. The questionnaire is prepared based on the FATF recommendations (listed out in Table 3), and also focus on the operational structure of the casino businesses. The questionnaire's central focus is on three areas from which magnitude of ML/TF risks is expected to emanate from, namely, ownership – stakeholders' risk, casino employees' risk, and customer risk.

For Sri Lanka, customer risk is deemed as the most prevalent risk. Criminals who frequent casinos as gaming participants would be intermingling their criminal proceeds with regular customers gaming proceeds. Criminal proceeds can be used in both low-risk casino products- such as slot machines, and with those with high likelihood games of risk. Typologies speak of frequency of the latter type of games being used at the layering stage is high, especially games such as roulette, baccarat, multiple batch placement with different outcomes – could be used primarily in a long-term layering stage of ML the way to mitigate this is through customer due diligence (CDD).

Casinos in Sri Lanka are required to conduct CDD on customers when they are engaging in inward and outward financial transactions that aggregate in either direction to the equivalent of USD 3,000 or more, regardless of the actual currency of the transaction(s) in a single business day.

Furthermore, the ML/TF risk is also envisaged as high for the following categories of customers who participate in the gaming environment of the casino.

Figure-3

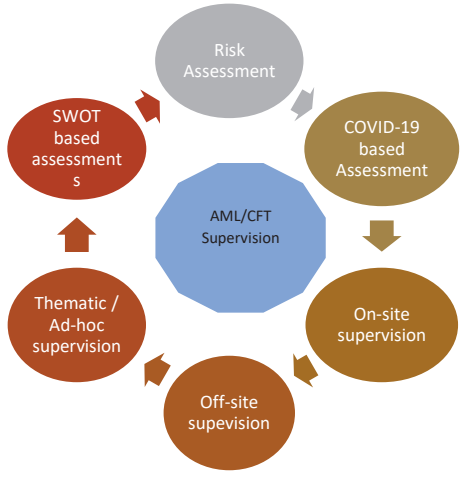


Figure-4

Source: Author Developed

1. High risk foreign jurisdiction customers

2. Customers who had been travelling just to play – as an organized group (junkets) or as a conglomeration of professional players.

Furthermore, customer risk could emanate from the modes of payment utilized by the customer. Usually, modes of payment are abused by would-be money launderers to launder illegal proceeds via casino structures. Several such high-risk modes refer to;

1. Structuring /smurfing – using different entities to infiltrate the gaming practices although beneficiary is a single person carrying out the laundering ring;

2. Dividing large amounts into smaller amounts – allowing easy infiltration, with no / minimum attention to the players;

3. Refining – converting low denominations to large denominations – this is also for chips – nominal fee to use as a carry and to be converted by a third party;

4. Customers/ players taking advantage of the shift changes of casino personnel– the new person coming on to the gaming floor may not identify the table change or the game change much – 1,600 casinos in USA – small amounts get structured and smurfed;

5. Transactions just below threshold of the USD 3000 – then the player is structuring using third parties to not draw attention to himself;

6. Excessive abuse of ATM/debit and credit cards – to use loading/ unloading below or at threshold levels;

7. Loan sharking – the practice of offering loans and money exchange services to playing customers;

8. Illegal and abusive use of Casino accounts – to deposit the money earned through gaming to carry out hawala type of remittances or to instruct Casino to draw wire transfers hiding the information relating to the player;

9. Abusive use of safety deposit boxes maintained at the casinos with the option of transferring of funds from one jurisdiction to another

E.g.: Cash being held by the casino in location A and the customer goes to location B in country X and asks to use the monies in the box as collateral for his play money in Casino at country X. The rest he would withdraw from the Casino in X and move the money from location to location; and

10. Using Money Mules: drug money laundering via money mules who recruits third parties that are using casinos to process/launder proceeds of crime.[11]

1.6 Conclusion

In conclusion, the casino sector needs to be vigilant when onboarding a new customer as a player. Furthermore, supervisors need to be

[11] Case study : Grosvenor casino in the UK – serious deficiency in the internal controls – convicted in the UK – regular visitor to the Grosvenor branch – when he first started to go to the casino, the staff has asked for CDD where he got the cash he responded as restaurant business – there have been instances where 150,000 pounds being played – but no red flag was raised – the investigations revealed 15,000 Irish currency notes – and still the casino staff did not ask anything – nothing was reported to FIU-UK. Casino was fined to pay Stirling pounds 950,000 as a penalty for charity services -

aware of practices adopted by casinos in customer onboarding, sources of wealth affirmations obtained by casinos, screening of Politically Exposed Persons (PEPs) and designated persons, and transaction monitoring. Most of these processes are easily carried out via automation and digitization. Previously, the sector had more to complain owing to lack of licensing preventing the institutions from gaining access to reputable merchants, high-quality merchandise, and licensed software. Now with the licensing regimes in place, such issues are expected to be history.

From the points of view of the casinos and from the online gaming sector, the regulator needs to be on its toes to identify and mitigate potential threats. With the new licensing requirements in place, close dialogue would need to be maintained with the issuer of licenses, the Ministry of Finance, with the FIU and the sector participants. Awareness and typologies would assist both the industry and the policymakers to form policies to support all stakeholders and mitigate future ML/TF threats providing a safe environment for legitimate entertainment and gaming sector in which all parties could perform amicably to their full potential.

References

Adam Rose and Associates, 1987. *THE REGIONAL ECONOMIC IMPACTS OF CASINO GAMBLING: ASSESSMENT OF THE LITERATURE AND ESTABLISHMENT OF A RESEARCH AGENDA,* Washington, DC: National Gambling Impact Study Commission.

Becker, G., 1968. Crime and punishment: an economic approach. *Journal of Political Economy,* 76(2), pp. 169-217.

Becker, G. & Murphy, K., 1988. A theory of rational addiction. *Journal of Political Economy,* 96(3), pp. 675-700.

Carvalho, N., Rodrigues, H. & Brochado, A., 2022. *Double or nothing: push and pull factors of casinos in Europe*. [Online] Available at: https://link.springer.com/article/10.1007/s10708-022-10749-7#citeas [Accessed 13 March 2023].

Centers for Disease Control and Prevention, 2020. *Coronavirus Disease 2019 (COVID-19)*. [Online] Available at: https://www.cdc.gov/coronavirus/2019-ncov/community/organizations/business-employers/casinos-gaming-operations.html [Accessed 28 October 2020].

Falls, G. & Thompson, P. B., 2013. Casinos, casino size, and crime: A panel data analysis of Michigan counties. *The Quarterly Review of Economics and Finance,* 54(1).

Falls, G. & Thompson, P. B., 2014. Do Casinos Contribute to Violent Crime? A Panel Data Analysis of Michigan Counties. *The Journal of Gambling Business and Economics* , 8(2), pp. 35-55.

FATF, 2009. Vulnerabilities of Casinos and Gaming Sector, Paris, France: FATF.

FATF, 2020. Financial Action Task Force Publications: The FATF Recommendations. [Online] Available at: http://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate) [Accessed 29 October 2020].

FATF-GAFI, 2020. COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses, Paris, France: FATF.

FinanceMonthly, 2019. Heres how casinos make money. [Online] Available at: https://www.finance-monthly.com/2019/03/heres-how-casinos-make-money/ [Accessed 13 March 2022].

Financial Intellgence Unit, 2014. National Risk Assessment -2014, Colombo: Financial Intelligence Unit of the Central Bank of Sri Lanka.

Ghaharian, K. & Bernhard, B., 2020. Sweden's Casino Cosmopol StayedOpen During the Pandemic: What Can We Learn?. UNLV Gaming Research & Review Journal, 24(2(1)), pp. 1-5.

Howe, A. & Newton, H., 2015. bestcasinosites.net. [Online] Available at: https://www.bestcasinosites.net/ [Accessed 30 October 2020].

LCB Network PLC, 2006. World Casino Directory. [Online] Available at: https://www.worldcasinodirectory.com [Accessed 30 October 2020].

Mallach, A., 2010. Economic and Social impact of introducing casino gambling: A review and assessment of literature. Federal Reserve Bank of Philadelphia: Community Affairs Discussion Papers, 10(01), pp. 1-28.

Niño Fidance, L., 2009. The mob never ran Vegas. Gaming Law Review and Economics, 13(1), pp. 27-40.

Sanction Scanner, 2020. Anti-Money Laundering Guidance for Gaming and Gambling. [Online] Available at: https://sanctionscanner.com/blog/anti-money-laundering-guidance-for-gaming-and-gambling-170 [Accessed 31 October 2020].

Shereen, M. A. et al., 2020. COVID-19 infection: Origin, transmission, and characteristics of human coronaviruses. Journal of Advanced Research, Volume 24(1), pp. 91-98.

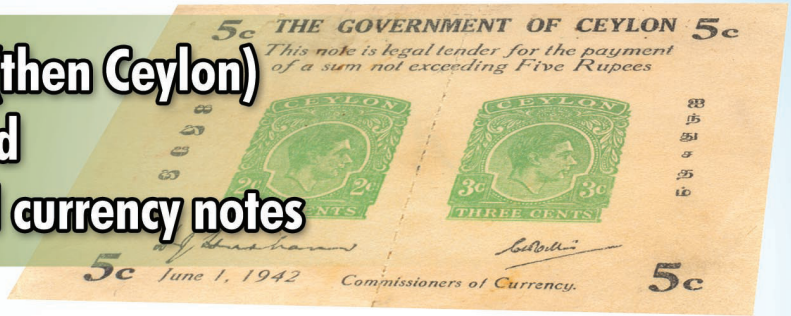
Walker, D. M., 2010. Casino and crime in the USA. In: B. L. Benson & P. R. Zimmerman, eds. Handbook on the Economics of Crime, Chapter 19. Northampton, MA: Edward Elgar Publishing, pp. 488-517.

Walker, D. M., 2013. Casinos and Crime: A Review of the Literature. 1st ed. New York: Springer Science and Business Media.

World Casino Directory, 2019. Wolrd Casino Directory Global Gaming Sumary 2019. [Online] Available at: https://www.worldcasinodirectory.com/statistics [Accessed 31 October 2020].

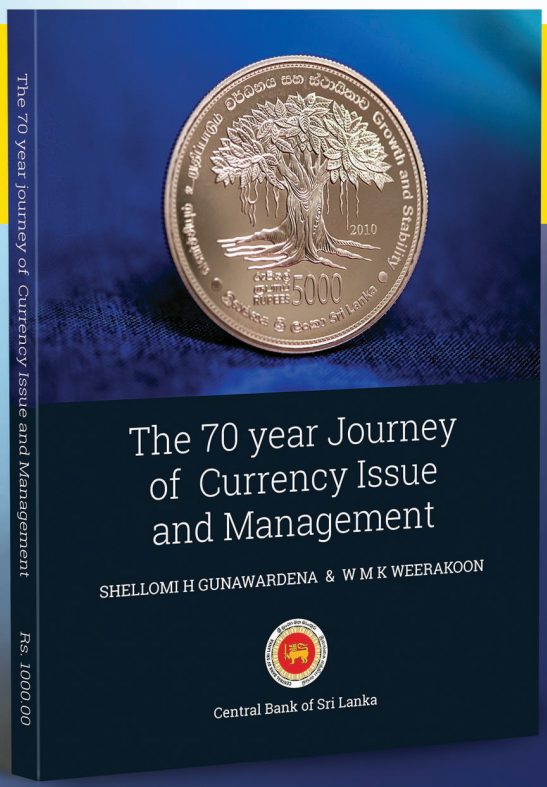
Did you know...

Sri Lanka (then Ceylon) once issued perforated currency notes



Ceylon also issued a Rs. 10,000 currency note!

Find out more interesting facts about our currency notes and coins from the publication



"The 70 Year Journey of Currency Issue and Management"

The publication, in English, is available for purchase by individuals and bookshops at Rs. 1,000 per copy, at the flowing locations:

Publication Sales Counter of the Economic History Museum (EHM), located at the Central Point Building, Chatham Street, Colombo 01 – 0112444502

All Regional Offices of CBSL at:

Anuradhapura – 025 222 2047
Kilinochchi – 021 228 5912
Matale – 066 222 2167
Matara – 041 222 2269
Nuwara Eliya – 052 305 9002
Trincomalee – 026 222 6967