



Money Laundering Terrorist & Proliferation Financing Associated with the Gaming Sector **RISKS**

The Gaming Sector has generally unique characteristics that carry inherently high financial crime risks. These include risks affiliated with an inconsistent regulatory environment, the cross border nature of the activities and the offering of quasi-financial services such as currency exchange and money transfers. Additional inherent risks are the variety, frequency and volume of transactions. Further increasing the inherent risks is the rapid growth of online gaming services with the popular feature of non-face-to-face customer onboarding and interactions.

Inherent Risks in the Gaming Sector

Both land-based and online gaming are inherently vulnerable to certain financial crime risks. They are exposed to criminal activities such as organized crime, loan sharking, prostituting and drug and human trafficking. It is therefore important to have the necessary identification and reporting frameworks in place to detect any incidences of illicit activity.

Customer Type Risks and Red Flags

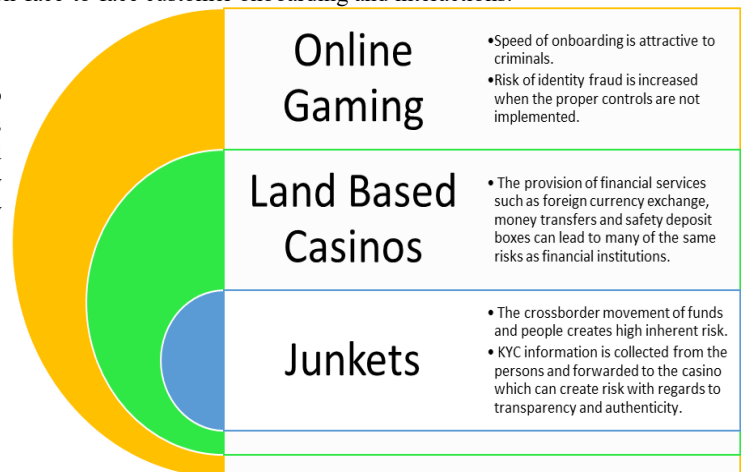
Whether the gaming entity is a physical location or an online platform, the identification of customer risk revolves around three (3) basic components:

- ⇒ Customer Identity/Know Your Customer (KYC)
- ⇒ Source of Funds (SOF)
- ⇒ Source of Wealth (SOW)

Properly identifying potential customers prior to opening a gaming account or allowing the customer to exceed reporting thresholds is a critical component of an effective Anti-Money Laundering/Counter Terrorist Financing/Counter Proliferation Financing (AML/CFT/CPF) program. The risk of obtaining fraudulent or counterfeit identification documents (IDs) is increased especially if foreign IDs are accepted during the customer due diligence process.

Once a customer's identification has been established, it is important to determine the SOF and SOW. Depending on the internal policies of the entity as well as local legislation, customer due diligence may be conducted for either all customers or those whose gaming activity exceed reporting thresholds and those whose activity is deemed suspicious.

Even if the SOF appears to be legitimate, gaming operators should evaluate whether the customer's level of gaming is proportionate to the SOF and SOW. This is critically important for those customers labeled as "High Rollers" or "VIPs" because their high level of gaming activities may increase the risk of large amounts of criminal proceeds being laundered over fewer transactions.



Beware of individuals conducting proxy bets. Proxy bets occur when third parties place wagers on behalf of anonymous individuals.

Beware of individuals who refuse to provide IDs or alter the spelling of their names when placing wagers or opening accounts.

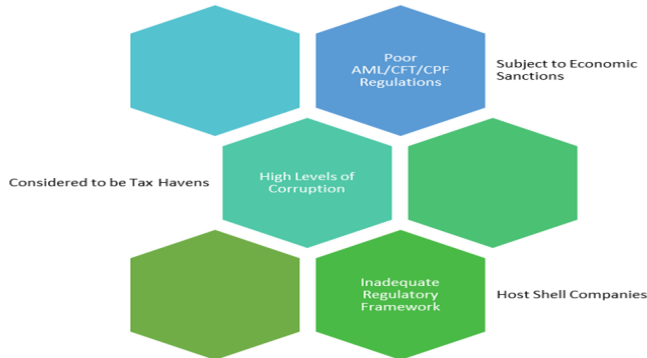
Beware of attempts to obscure the audit trail of transactions such as the opening of multiple accounts.

In this Newsletter...

- ⇒ **Inherent Risks in the Gaming Sector**
- ⇒ **Customer Type Risks and Red Flags**
- ⇒ **Jurisdiction Risk and Red Flags**
- ⇒ **Product Risk and Red Flags**
- ⇒ **Channel Risk and Red Flags**
- ⇒ **Three Lines of Defense for Gaming Institutions**

Jurisdiction Risk and Red Flags

Certain countries are known for high levels of corruption, money laundering, drug trafficking and cartel activities. It is important for entities to consider the inherent risk in the jurisdictions where they conduct business. Jurisdictions with higher risk are known to have the following characteristics:



Gaming entities operating in countries with lenient or weak AML/CFT/CPF regimes can fall under the control of criminal syndicates. These syndicates can be known to bribe corrupt government officials to obtain licences to operate establishments such as casinos. Gaming entities (physical or online) are also vulnerable to being used as front companies to facilitate the flow of criminal proceeds.



Product Risk and Red Flags

Gaming products comprise games and quasi-financial products.

Gaming products include blackjack, bingo, horse racing and sports betting. Different products have different risks. Products such as poker, mahjong and baccarat have **chip dumping risk**. Chip Dumping occurs when a group of players intentionally loses to a designated winner who is paid in laundered funds that appear to be legitimate winnings. Sports Betting carries a risk of match-fixing and other fraudulent behaviour.

Quasi-financial products are offered by gaming entities to facilitate the flow of funds for gaming activities. These include credit accounts, pre-paid cards, mobile wallets and other digital wagering applications. Criminals take advantage of a common payment method by using illicit proceeds to repay outstanding balances on a credit account. Criminals also combine illicit proceeds with game winnings within a mobile wallet or deposit account. At a physical casino, criminals may request to combine illegally gained cash with chips and slot machine winnings in a casino-issued cheque.



Channel Risk and Red Flags

Channel risk involves the method by which an entity's products are delivered. It increases with non face to face business relationships and transactions where payments are sent to or received from unknown or unassociated third parties.

The Gaming Sector is constantly evolving and gaming operators develop and offer new products and platforms to appeal to a diverse customer base and to increase accessibility. Anonymous deposit methods such as pre-paid cards, cryptocurrency and cash are red flags for gambling operators.

It is important for gaming entities to conduct Gaming Risk Assessments which focus on third party and remote transactions which could be exploited. A Technology Risk Assessment should also be completed for new products and channels and should specifically address all emerging risks.

Three Lines of Defense for Gaming Entities

The success of any AML/CFT/CPF Program in Gaming is highly dependent on the effectiveness of the **Three Lines of Defense**. The lines of defense ensure compliance with the gaming entity's AML/CFT/CPF Program and establish clear roles, responsibilities and oversight. This approach is crucial in the Gaming Sector where entities are normally open 24/7. This means that criminals have the opportunity to commit financial crimes at any time of the day.

The Three Lines of Defense therefore mitigate financial crime risks by ensuring the timely filing of regulatory reports, the maintenance of proper records of financial transactions and the conducting of customer due diligence and risk assessments.

FIRST LINE: FRONT LINE STAFF

The First Line of Defense includes personnel who interact directly with patrons. These include cashiers, table games dealers and slot attendants. These individuals have a wide range of responsibilities such as collecting and verifying customer identification. This first line is critical in observing suspicious activity and escalating incidents for further investigation.

SECOND LINE: COMPLIANCE

The Second Line of Defense involves Compliance personnel. Their duties would include conducting risk assessments, establishing policies and procedures, maintaining internal controls and ensuring adequate training. The Second Line of Defense must be fully independent from the operations and have the authority to act. This means that they must be empowered to investigate real or potential breaches of laws or regulations and have access to Senior Management and the Board of Directors, as necessary.

THIRD LINE: INTERNAL AUDIT

The Third Line of Defense is the Audit Function. It involves Internal Audit personnel who conduct independent testing of the AML/CFT/CPF Program and associated processes and procedures. The testing and reviewing of the program are done to ensure that the AML/CFT/CPF Program is working effectively to identify and mitigate risks.

Every entity has its own appetite for risk. This determines the type of customers it will accept, the type of products it will offer and the jurisdictions in which it will operate. Using a RISK BASED APPROACH will allow the entity to focus its effort where it is most needed and has the most impact.

References

AML Foundations for Gaming: ACAMS.org , 2021

REMEMBER

FOR MORE NEWSLETTERS:

[Financial Services Regulatory Commission - Newsletters \(www.fsrc.kn\)](http://www.fsrc.kn)