CYPRUS GAMING AND CASINO SUPERVISION COMMISSION

GUIDANCE FOR SUSPICIOUS ACTIVITY REPORTING

Version 1

02 April 2021

Table of Contents

DEFINITIONS

"AMLCO" means the Anti-Money Laundering Compliance Officer.

"AML/CFT" means Anti-Money Laundering and Combating the Financing of Terrorism.

"Direction/AML/CFT Direction" means the AML/CFT Direction, issued by the Commission in line with the provision of the Article 59(4) of the AML Law and Regulation 18 of the Casino Operations and Control (General) Regulations of 2016.

"Casino operator" or "Operator" means the holder of the integrated casino resort license in the Republic of Cyprus and licensed to operate the temporary and satellite casinos.

"The Commission" means the Cyprus Gaming and Casino Supervision Commission.

"The Law" or "AML Law" means the Prevention and Suppression of Money Laundering Activities Laws of 2007 (L.188 (I)/2007).

"MOKAS" or "Unit" means the Unit for Combating Money Laundering of the Republic of Cyprus.

INTRODUCTION

1. These Guidance are prepared by Cyprus Gaming and Casino Supervision Commission as a best practice document and may assist the operator in establishing adequate processes and procedures to recognize and report suspicious activity as required under the Prevention and Suppression of Money Laundering Activities Laws of 2007 (L.188 (I)/2007) (AML Law) and the Commission's AML/CFT Direction.

2. The Money Laundering and Terrorist Financing environment is constantly changing. Individuals involved in such activities are continually attempting to exploit new and different services and products offered by various sectors in an effort to disguise the true nature of their illicit activities and proceeds. These Guidance are a summary of non-exhaustive steps and best practices when dealing with the execution and/or review of clients' transactions and activities and the assessment of suspicion.

Money laundering in the casino sector

3. Using any amount of money in a casino, that is the proceeds of crime, can amount to money laundering when the person using or accepting the money knows or ought to have known that it is the proceeds of crime. Therefore, both the customers and employees of the operator may commit a money laundering offence depending on their level of knowledge.

4. The AML Law criminalizes any involvement with the proceeds of crime if a person knows or ought to have known that the property is criminal property. The offences relate to the concealing, disguising, converting, transferring, acquisition, use and possession of criminal property, as well as arrangements which facilitate the acquisition, retention, use or control of criminal property. For example, in the gambling sector, it may involve taking of cash, cheque, or card payments to form a wager in cases where those funds are the proceeds of crime, or holding money on account for a customer for the purposes of gambling.

5. Money laundering in the gambling sector takes two main forms:

- Exchanging money, assets, goods, and property that were acquired criminally for money or assets that appear to be legitimate or 'clean' (so called classic money laundering). This is frequently achieved by transferring or passing the funds through some form of legitimate business transaction or structure.
- The use of criminal proceeds to fund gambling as a leisure activity (so called criminal or 'lifestyle' spend).

6. Money laundering often involves a complex series of transactions that are usually difficult to separate. However, it is generally considered that money laundering is typically accomplished through a number of phases:

(i) Phase one: Placement — Placement is the first phase of money laundering circle. It includes physical disposal of cash or other assets derived from criminal activity. In this phase, the money is placed into the financial system or retail market or is smuggled to another country.

(ii) Phase two: Layering – Layering is the second phase of money laundering circle. It attempts to conceal or disguise the criminal origin of the proceeds. Typically, it is achieved by number of complex transactions that move money in and out through various accounts and/or countries with the purpose of separation of illicit proceeds from their source.

(iii) Phase three: Integration – Integration is the third and final phase of the money laundering circle. It involves integrating the criminal proceeds into the legitimate economic and financial system. This phase supplies apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appears to be normal business or personal transactions.

7. The operator needs to be mindful that the money laundering offence also includes simple criminal spend which might not include all typical stages of the money laundering process (placement, layering and integration) and not all three stages of money laundering circle need necessarily to take place for it to be considered money laundering.

Terrorist financing

8. The Combating of Terrorism Law of 2019 (75(I)/2019) establishes the terrorist financing offence and offences related to engagement in, or facilitating terrorism. It also establishes the lists of prescribed persons that are believed to be involved in terrorism.

9. Disrupting and preventing these terrorism-related financial flows and transactions is one of the most effective ways to fight terrorism. Terrorist financing is the process by which terrorists fund terrorist acts or terrorist organizations. Terrorists need financial support in order to perform their activities. Terrorists need money and other assets, for weapons but also training, travel and accommodation to plan and execute their attacks and develop as an organisation.

10. There is little difference between terrorists and other criminals who will seek to

exploit the vulnerabilities in the operator's controls to bypass or misuse the operator's AML/CTF controls. The techniques used to launder money and to finance terrorism are very similar and, in many instances, identical. An effective AML/CFT program must address both risks.

11. Despite similarities in both money laundering and the financing of terrorism, there are subtle differences between them. For example, whilst the motivation behind money laundering is profit seeking, the motivation behind terrorist financing is usually ideological.

12. An important difference to be aware of is that the money laundering schemes are primarily designed to hide the "source" of the funds, terrorist financing activities are primarily designed to hide the "purpose" for which these funds are used. Furthermore, whilst funds used in money laundering always derive from criminal activity, in case of terrorist financing funds can stem from both legal and illicit sources. This combined with the fact that the amounts involved in terrorist financing are usually relatively small makes terrorist financing more difficult to detect and requires vigilance and the knowledge of staff.

SUSPICIOUS ACTIVITY REPORTING

Reporting Requirements

13. Suspicious activity should be identified both during the on-boarding, the ongoing due diligence of customers as well as during the transaction monitoring process and could be identified and raised by any employee of the casino operator. The reporting requirement for suspicion arises from Articles 27 and 69(d) of the AML Law and relates to Suspicious Activity Reports (SARs) and Suspicious Transaction Reports (STRs).

14. Suspicious Activity Reports (SAR) arise from the reporting of suspicion relating to the behaviour of a person which creates the knowledge or belief that he or she may be involved in illegal activities out of which revenue might be generated.

15. A Suspicious Transaction Reports (STR) arise from the suspicion related to specific transaction(s), which create the knowledge or belief that the transaction(s) may be an attempt to profit from the legitimisation of proceeds from illegal activities or hide the "purpose" for which these funds are to be used.

16. Article 27 of the AML Law states that "A person who knows or reasonably suspects that another person is engaged in laundering or financing of terrorism offences, and the information on which that knowledge or reasonable suspicion is based, comes to his

attention in the course of his trade, profession, business or employment, shall commit an offence if he does not disclose the said information to the Unit as soon as is reasonably practicable after it comes to his attention. An offence under this section shall be punishable by imprisonment not exceeding two years or by a pecuniary penalty not exceeding five thousand euro or by both of these penalties".

17. In addition, based on Article 69 (d) of the AML Law, it is required that when the casino operator knows or has 'reasonable suspicion that monetary sums, irrespective of the amount thereof, constitute proceeds from illegal activities or relate to terrorist financing, to ensure the Unit is immediately notified, on their own initiative, by submitting a relevant report and providing supplementary information after a relevant request by the Unit'. The obligation to report to the Unit also includes the attempt to execute such suspicious transactions.

Knowledge and suspicion

18. If a person employed by the casino operator thinks a transaction is suspicious, it is not necessary for them to know the exact nature of the criminal offence or that particular funds are definitely those arising from crime. The employee could have noticed something unusual or unexpected and, after making enquiries, the facts do not seem normal or make commercial sense. It is not necessary to have evidence that money laundering is taking place to have suspicion.

19. A transaction that appears to be unusual is not necessarily suspicious. Many customers will, for perfectly legitimate reasons, have an erratic pattern of gambling transactions or activity. Even customers with a steady and predictable gambling profile will have periodic transactions that are unusual for them. Therefore, an unusual transaction could be the basis for further enquiry, which may in turn require judgement as to whether the transaction or activity is suspicious. A transaction or activity not considered suspicious at the time, could if suspicions are raised later, result in an obligation to report the activity. Likewise, if concern escalates following further enquiries, it is reasonable to conclude that the transaction is suspicious and will need to be reported to MOKAS.

20. Unusual patterns of gambling, including the spending of large amounts of money in relation to the casino customer's profile (e.g. age, occupation, personal circumstances, previous patterns of gambling, associations etc.), should receive attention, but unusual behaviour should not automatically lead to grounds for knowledge or suspicion of money laundering/terrorist financing, or the submission of a report to MOKAS. The casino operator should also consider whether suspicious or irregular patterns of play or behaviours if not an

indication of money laundering activity, could be considered indicative of a customer having problematic or even pathological gambling problems and referred to person having responsibility for this area of regulatory risk.

21. The operator's AMLCO (and their staff) should have an enquiring and critical mindset with the ability to assess the circumstances of each case, consider all available and relevant information and come to an evidence-based decision. In some cases, it will be necessary to gain more information about a customer (or others) through further direct questions and/or by utilising wider sources of information to corroborate information already provided by the customer, or identify and resolve inconsistencies, to assist in arriving at a reasoned and recorded decision.

22. The AMLCO should keep themselves (and their staff) up to date with new data sources, collection, reporting and analysis methods and engage with the operator's information technology specialists to identify opportunities to increase the efficiency and accuracy of the operators AML/CTF information management capability.

23. It is important that the information used and the rationale for the decision is recorded. Where concerns are raised, it is good practice to corroborate information provided by the customer and collected from other sources and not to accept the absence of corroborating information as a positive indicator.

24. It should be stressed within internal training and guidance that in order for either an internal or external report to be made it is not necessary to have knowledge of or to establish the exact nature of any underlying criminal offence, or that the particular funds or property were definitely those arising from a crime. Furthermore, it is not necessary to await conviction of a customer for money laundering or other criminal offences in order to have suspicion that money laundering has taken place.

Money laundering typologies

25. It is important that the operator's AMLCO maintains their awareness of the ML/TF typologies as well as of red flags (see section Red flags/Indicators of suspicious activity) for recognizing potentially suspicious transactions and activity. This knowledge will assist in interpreting what is being seen or reported and should be included within the training provided to staff.

26. Publications by national and international agencies, professional associations, and credible media are good source of information and will assist in ensuring that the understanding of ML/TF typologies are current.

Criminal spend – spending ill-gotten gains

27. The most common form of money laundering in a casino happens by customers using money derived from criminal activity to place wagers. One indication of criminal spend could be a significant increase in a customer's spend suddenly or over a period of time. However, it is also not unusual for legitimate players to have spikes in play. Identifying criminal spend and differentiating spikes in play from that of legitimate customers is dependent upon adequate implementation of customer due diligence measures, monitoring play over time and especially ascertaining the customer's source of funds. The staff should also be properly trained to spot red flags and report them accordingly.

Avoiding detection – structuring or "smurfing"

28. This includes all the situations where there is an indication that a customer is trying to avoid regulatory thresholds for customer due diligence and/or reporting. For example, a customer could have more than €2,000 in chips in his possession but could choose to cash out less. A process where a customer leaves the casino with a large amount of chips or stores them onsite in a safety deposit box for extended period is known as "chip walking". Even though there may be legitimate reasons for a customer to do this, it could also be a sign that the customer is trying to hide funds or structure transactions below the reportable threshold or use the chips as a form of currency for illegal transactions such as drug deals. In order to mitigate the risk, it is necessary to monitor and review situations where a customer seems to have held back a significant amount of chips from redemption. Each circumstance must be assessed to determine if the transaction raises suspicion or not and relevant reasons should be properly documented. To monitor the ongoing risk, the casino operator's monitoring of the levels at each casino of unredeemed chips and the amount of chip redemptions from irregular or new customers is an important indicator.

Avoiding detection – concealing identity

29. The operator should have adequate controls in place to identify persons trying to use false identification (forged, altered or another person's) documents to meet threshold requirements, sign up for loyalty programs, satisfy the operator's enquiries, retrieve, transfer or deposit money. To mitigate risk associated with loyalty programs membership, the operator needs to be satisfied as the validity of ID provided. Additionally, the customers should be required to provide a valid ID in order to conduct transactions over €2,000 threshold even when using the loyalty card in order to mitigate the risk. The attempted use of false or conflicting identification or the avoidance of responding to requests to confirm identity should be considered a high-risk matter.

Converting 'dirty money'

30. The operator should have adequate controls in place to detect situations where a customer is trying to convert small denomination bills into larger bills (e.g. €100) especially when there is minimal gaming activity. This method is also known as "bill stuffing" and it could also apply to situations when a customer is trying to exchange the bills for new bills by converting e.g. 'old' €100 notes to new €100 notes. New notes may be sought if a criminal wishes to unload currency loaded with drug residue or suspects that the notes are marked. The customer could put the money in the slot machines and then request a cash out voucher. Kiosk machines can be used to redeem the voucher for €100 notes. Criminals can sometimes also attempt to use cash-out vouchers to transfer funds from one associate to another. However, controls needs to be in place in order to help identify the instances of possible bill stuffing.

Using chips to facilitate illegal activity

31. Criminals are known to use casino chips as an alternative form of currency. The chips can be used to store funds, transfer to associates or facilitate illegal transactions. A control should be in place to reduce the risk of chips being used for illegal purposes by validating if the customer at the time of chips redemption had gambling winnings or prior chip buy-ins. Similar procedures should be applied when requesting redemptions of cash-out vouchers at the cashier.

Paying the expenses of others

32. Paying the expenses or debts of other person is a well-known money laundering method that is used to transfer illicit funds without creating a money trail of payments between the associates. The operator should be especially alert to risk related to third party payments. The risk significantly increases if a third-party payment originates from an entity or unrelated individual, and especially if it involves cross border transfers of funds.

Cleaning

33. Offset betting is the process of placing equal bets on both outcomes of a casino game and is known as a method used in attempt by criminals to clean the funds. To reduce suspicion, the criminals often use their associates to place the other side of the bets. However, surveillance should be able to assist in detecting such behaviour. Furthermore, often those who attempt to "clean" their money request a pay-out in the form of a cheque.

34. The operator should bear in mind that the above examples are not exhaustive.

Terrorist financing – sources and methods

35. The funding of terrorist organisations could be undertaken through using the proceeds from both illegal and apparently legal activities. Criminal activities generating such proceeds include kidnappings (demanding ransom), extortion (demanding money for "protection"), smuggling, thefts, robbery, and drug trafficking. Legal fund-raising methods used by terrorist groups may include:

- Collection of membership subscriptions
- Sale of books and other publications
- Cultural and social events
- Donations
- Community solicitations and fund-raising appeals from society

36. Funds originating from criminal activity can be laundered by terrorist groups using the same methods used by criminal groups motivated by profit. The operator should be alert not only to the manipulation of gambling activity to clean money or to attempts by customers to conceal identities, but be vigilant as to how the financial facilities offered to customers may be exploited e.g. structured deposits to or withdrawals from accounts, the use of monetary instruments (bankers draft, traveller cheques), use of credit and debit cards, wire funds transfers using "straw men", false identities or companies without physical presence or proxies (nominees) from the close family environment, friends and associates.

37. Non-profit and charitable organisations are also used by terrorist groups as a means of raising funds and/or serving as cover for transferring funds in support of terrorist acts.

Responsibilities regarding suspicious activity reporting

38. The Operator's system for identifying, monitoring, and reporting suspicious activity should be risk-based by directing sufficient resources at those areas the operator has identified as higher risk. The operator should have sufficient controls and monitoring systems for the timely detection and reporting of potentially suspicious activity.

39. The operator should perform effective due diligence actions and should have in place systems and processes to detect and monitor high risk behaviour or transactions or activity that may be inconsistent with a customer's source of income, regular activities, or other expected factors.

40. The AMLCO is the primary contact point for considering all AML/CTF issues whether

arising from the business and for enquiries by external authorities and has the responsibility for receiving internal reports and reporting suspicious activities or suspicious transactions to MOKAS.

41. Once an employee has reported their suspicion in an appropriate manner to the AMLCO or to an individual to whom the AMLCO has delegated the responsibility to receive such internal reports, he has fully satisfied his obligation under the Law.

42. The casino operator must notify MOKAS[1] of the names and positions of person whom they appoint as AMLCO and Deputy AMLCO. The AMLCO must ensure that they are registered with MOKAS and assigned access credentials for MOKAS' online 'goAML' web-based reporting tool. The AMLCO is responsible for compliance with the MOKAS 'goAML' user guide and reporting instructions.

43. The AMLCO should develop an effective suspicious activity monitoring process comprising the following policies and procedures:

(a) Procedures to identify and as necessary, monitor suspicious transactions and customers activity through various channels, including but not limited to employee identification, inquiries from law enforcement and alerts generated by adequate transaction monitoring systems.

(b) A formal documented evaluation of each suspicious transaction or activity by the AMLCO.

(c) Documenting by the AMLCO the decision whether suspicious transaction/activity should be reported to the Unit or not.

(d) Decisions to cease a business relationship or prevent further occasional transactions.

(e) Employee training on detecting suspicious transactions or activity.

Documenting Reporting Decisions

44. The AMLCO must keep adequate records of suspicious activity and suspicious transaction reports. All internal enquiries made in relation to the report should be documented or recorded electronically. This information may be required to supplement the initial report or as evidence of good practice and best endeavours if, at some future date,

[1] Notification should be completed following approval from the Commission for AMLCO appointment as described in section Appointment of Anti-Money Laundering Compliance Officer ("AMLCO") of Commission's AML/CFT Direction.

there is an investigation and the suspicions are confirmed or disproved. The records management arrangements should include:

(a) All internal suspicion reports;

(b) Evaluation by the AMLCO of all internal suspicion reports through Internal Evaluation Reports containing the following information as a minimum:

- How the AMLCO managed the enquiries, including the sources of information used, their credibility, including requests for further information from the customer or staff, and the assurance or otherwise that the sources provide2;
- Assessment of the information collected and any other information about the customer/transaction that has been analysed as part of internal evaluation (e.g. customer's CDD information, customer's reputation, customer's transactional history with the operator, reasons for suspicion), along with any subsequent decisions about whether or not to await developments or seek additional information;
- The decision and rationale for deciding whether or not to proceed with an external SAR/STR;
- Any decisions to monitor the customer(s) concerned. Any advice given to operational teams about continuing the business relationship and any relevant internal approvals granted in this respect3;
- Decisions to cease a business relationship or prevent further occasional transactions.

---

[2] When requesting further information from the customer, the operator needs to be mindful of "tipping off" offence. A "tipping off" offence occurs when any person discloses, either to the person who is the subject of a suspicion or any third party, that:

a) information or documentation on ML/TF has been transmitted to MOKAS;
b) a SAR/STR has been submitted internally or to MOKAS;
c) authorities are carrying out an investigation/search into allegations of ML/TF;

and such disclosures may likely prejudice the subsequent investigations.

Tipping-off may also occur in those cases when an employee approaches the client to collect information about the internal on-going investigation, and through the intense questioning, the client becomes aware of the investigation.

[3] The operator should determine the actual risk presented by a customer subject to suspicious report and take appropriate measures to mitigate the risk. If a report has been submitted to MOKAS, the operator needs to consider if the relationship with the customer needs to be terminated or not. Decisions must be properly documented and retained.

(c) All external suspicion reports.

45. These records should always be supported by the relevant working papers and decision records. The maintenance and retention of such records is important as they justify and defend the actions taken by the AMLCO or other members of staff and must be made available to the Commission and MOKAS upon request. A report index should be kept and each SAR/STR be given a unique reference number.

46. Records should be maintained for at least six years from the date when the operator's relationship with the client was terminated or a transaction was completed. If an ongoing investigation is occurring, relevant CDD records should not be destroyed merely because the record retention period has expired.

Protection

47. Under the AML Law, protection exists for persons submitting suspicious reports.

48. As per article 69A of the Law, disclosure of information in good faith by an obliged entity or by an employee or director of such an obliged entity shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the obliged entity or its directors or employees in liability of any kind even in circumstances where they were not precisely aware of the underlying criminal activity and regardless of whether the illegal activity actually occurred.

49. Additional provision is stipulated in article 69B of the Law where a person is protected from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions once that person has submitted an internal or external report to MOKAS.

Penalties

a) Failing to report

50. Under article 27 of the AML Law, an offence is committed if a person does not disclose the information of suspicion to MOKAS. Failing to report is punishable by imprisonment not exceeding 2 years or by a financial penalty not exceeding €5.000 or both penalties.

b) Assisting a person involved in the commission of a predicate offence

51. As per Article 4 of the AML Law, assisting in any way a person involved in the commission of a predicate offence, is an offence punishable by 14 years imprisonment or by

a financial penalty up to €500.000 or by both.

c) Tipping-off

52. According to article 48(3) of the Law, "Tipping Off" is a criminal offence and is punishable on conviction by a maximum of two years imprisonment or a fine not exceeding €50.000 or both penalties.

Red flags of suspicious activity

53. There are numerous things that can make someone either know or suspect that they are dealing with the proceeds of crime. Some examples of how suspicions may be raised are listed below, although this is not an exhaustive list and there may well be other circumstances which raise suspicion.

Red flags/Indicators of suspicious activity

A. A person convicted of dealing in drugs is released from prison and immediately starts gambling large amounts of money. He/she is known to be out of work and other customers inform employees that he/she is supplying drugs again.

B. Stakes wagered by a customer become unusually high, not in accordance with their previous patterns of behaviour and the customer is believed to be spending beyond his or her known means, all of which requires some knowledge of the customer. For example, a customer is known to live in a modest accommodation with no known source of income, but nonetheless is spending money well above his or her apparent means. There is no set amount which dictates when a report to MOKAS should be made and much will depend on what is known, or suspected, about the customer.

C. A customer exhibits unusual gambling patterns with an almost guaranteed return or very little financial risk (sometimes across multiple premises). It is accepted that some customers prefer to gamble in this way but, in some instances, the actions may raise suspicion because they are different from the customer's normal gambling practices.

D. Money is deposited by a customer or held over a period and withdrawn by the customer without being used for gambling. For instance, suspicions should be raised by any large amounts deposited in gaming machines or gambling accounts that are then cashed or withdrawn after very little game play or gambling.

E. A customer regularly gambles large amounts of money and appears to find a level of losses acceptable. In this instance, the customer may be spending the proceeds of

crime and sees the losses as an acceptable consequence of the process of laundering those proceeds.

F. A customer's spend increases over a period of time, thereby masking high spend and potential money laundering.

G. A customer spends little, but often, and his annual aggregate spend is high and out of balance with his expected spend.

H. Noticeable changes in the gaming patterns of a customer. These changes might include e.g. customers who carry out transactions that are significantly larger in volume when compared to the transactions they normally carry out; customers who usually place small bets enquire about the opening of an account with the casino and the possibility of moving funds between accounts belonging to the same group of casinos; customers that carry out transactions which seem to be disproportionate to their wealth, known income or financial situation.

I. Customers in collusion who consistently appear to bet against each other on even money games (for example in roulette games). Such a technique offers the possibility of laundering the proceeds of crime without the risk of losing the monies subject to gaming.

J. A customer seeks to cash out chips or tickets in excess of €2.000 but when asked for identification reduces the amount of chips or tickets to be cashed out to less than €2.000.

K. Difficulties in conducting the necessary customer due diligence, such as those situations where:

    i. A customer refuses to provide personal identification documents.

    ii. A customer presents conflicting identification information in different gaming days such as different address, different ID number etc.

    iii. A customer presents suspicious or false identification documents, misleading or inaccurate information, or insists on identifying himself with a name or nickname that does not appear on his identification document.

    iv. A customer acts to exceed the €2000 identity verification threshold by using a number of casinos.

L. A customer attempts to influence, bribe or conspire with an employee of the

operator in order to avoid identification or making unusual efforts to befriend casino staff members.

M. A customer attempts to convince casino staff not to record transaction information including the instances where a customer refuses to use his loyalty card in order not to record transaction information.

N. A customer wires funds through a bank or other financial institution located in a country that is not his/her residence or place of business.

O. A customer purchases a large amount of chips at a table, engages in minimal gaming and then redeems or requests to redeem the chips for a casino cheque.

P. Customer requests the issuance of a winner's cheque/certificate in the name of a third party.

Q. A customer makes a large deposit using numerous small denomination bills (e.g. €10, €20) and withdraws it in chips at a table game, engages in minimal gaming and exchanges remaining chips at a cage for large denomination bills (e.g. €100), a casino cheque or money transfer.

R. A customer inserts €1.990 or similar amount below the threshold of paper money into a bill acceptor on a slot machine (e.g. contemporaneously inserting €5s, €10s, €20s), accumulating credits with minimal or no gaming activity, presses the "cash out" button to obtain a ticket. The customer goes to other machines and conducts the same activity at each machine. Then the customer redeems the tickets for large denomination bills or casino checks with different cage cashiers at different times in a gaming day.

S. A customer transfers funds to a casino for a deposit into a front money account and withdraws it in chips, engages in minimal or no gaming activity and exchanges/attempts to exchange remaining chips for a casino cheque.

T. Customer requests the issuance of a winner's cheque/certificate in exchange of money that has not derived from winnings at the casino.

U. Customer attempts to redeem a winner's cheque that does not correspond with the recorded winnings of the person.

V. Customer requests the transfer of winnings to the bank account of someone else.

W. Customer buys chips and leaves the casino without cashing out.