# Procedure: Unusual Matter - Gaming

## 1. Purpose

To assist Club on East (the Club) meet with suspicious matter reporting obligations under the *Anti-Money Laundering & Counter-Terrorism Financing Act 2006.*

## 2. Responsibilities

All Staff

## 3. What is an unusual matter

Club on East considers the following as red flags/unusual matters for transaction monitoring purposes:

Examples of red flags or unusual matters:

- Unusual transactions or circumstances are evident.
- The customer's known business background may be considered suspicious.
- Individuals or groups work together to gain the trust of gaming staff or collude with staff to avoid detection or provide identification when collecting winnings.
- The customer profile does not match the amount of funds they are gambling with—low income versus large amounts of gambled funds. For example, it is known that a customer receives Centrelink benefits or has a low-paying job, but they gamble significant sums of money. Ask yourself how they got access to that kind of money.
- Customers who gamble with large amounts of cash and do not use the ATM deliberately use multiple cashiers or only cash redemption terminals (CRTs) to avoid observation or monitoring by Club Team members.
- Production of unusual or false identification.
- The use of aliases and, or a variety of similar addresses.
- Customer sources of funds are suspected to be linked to criminal activity.
- The customer asks for cheques to be made out below $10,000.

- Customers in the gaming machine areas do not intend to play gaming machines. They insert large amounts of cash or credits into EGMs and engage in minimal or no gameplay to appear like a real player before cashing out.
- Customers who approach other customers to purchase payout vouchers. A legitimate player is offered cash (by the money launderer) for accrued credits or winning tickets. The money launderer then claims the legitimate credits as their own.
- Customers who cannot present identification when seeking to cash out or claim winnings.
- Customers presenting counterfeit note/s.
- Customer sources of funds are suspected to be linked to criminal activity – the patron is a known criminal, money launderer or terrorism financier, and the patron is involved in a suspicious matter.
- Customers may request a cheque to be written in the name of a third party.
- High redemptions over a short period.
- The sum of transactions adds up to significant amounts of money.
- A customer receiving a volume of cheques within a specific period beyond that of which would be considered a reasonable amount of winnings by one person.
- A customer receiving multiple cheque payments on a single day beyond that would be considered a reasonable amount of winnings by one person for one day.
- The customer involved in a transaction is considered a high risk politically exposed person.

## Avoiding Identification procedures

- The customer provides a false or altered identification document (ID)
- The customer is reluctant to give ID and asks staff to refer to information or ID previously provided/on file
- The customer repeatedly collects winnings just below the thresholds for mandatory ID collection
- The customer makes an unusual enquiry to venue staff about whether they report to government authorities or, more specifically, to AUSTRAC, the tax office or law enforcement agencies
- The customer advises they have no ID and request winnings be paid by cash to the threshold amount and never return to collect the balance by cheque (some states allow part payment up to cash limit and balance by cheque)

## CRT receipts

- The customer plays an EGM and then saves cash redemption terminal (CRT) receipts so they can later rely on them to justify the receipt of funds.
- The customer requests any redeemed or CRT receipts from venue staff.

## Payments

- The customer feeds an EGM with cash and requests a cheque or electronic funds transfer (EFT) payment after no or minimal play.
- After minimal or no play, the customer feeds an EGM with cash and requests a cheque or EFT payment for amounts under the non-cash threshold.
- The customer attempts to have funds directed to a third party, such as another person or a company.
- The customer supplies a third party's BSB and account number, along with their account name, to effect a payment to a third party without detection.
- The customer states they don't have a bank account and insists on receiving cash.
- The customer offers venue staff a small gift or bribe not to record any cheque or EFT payment details.
- The customer advises venue staff they have a 'cash business' and asks to exchange cash for cheques.

## Customer behaviour

- Individual note acceptors have large sums of cash inserted, but records indicate minimal or no play.
- A customer tries to circumvent note insertion limits by playing multiple EGMs at once, sometimes non-adjacent EGMs
- The customer attempts to influence a new staff member to ignore their suspicious activity by offering tips.
- The customer only deals with one venue staff member and avoids other staff
- Customers with no known relationship sharing funds
- The customer has large sums of cash, with indications they have recently been involved in a serious crime, e.g. they are wearing an electronic tracking device
- The customer abandons an EGM and fails to request a payout once credits are to a value greater than the cheque/EFT payment threshold amount

- The customer plays EGMs at a venue far from the home address listed on their ID or their known place of business
- A customer who regularly uses a loyalty card suddenly doesn't use it and appears to have significant winnings
- A law enforcement agency makes enquiries to a venue about a customer's gaming activity

- A venue staff member informs a customer that AUSTRAC or a law enforcement agency has or will be visiting the venue

### Fraud

- The customer sells a cheque issued by a venue to a broker and then returns to the venue, advising that they have lost the cheque and require a replacement.

- The customer alters the name of the payee of a cheque or changes the dollar amount to a higher value.

### Counterfeit notes

- Customer attempts to use counterfeit notes to credit an EGM
- An EGM or CRT rejects the customer's banknote as the note is identified as being counterfeit
- The customer asks the cashier to change banknote denominations instead of using a CRT with a counterfeit note scanner
- The customer asks to change banknote denominations for odd reasons, e.g. because they are a collector seeking a specific note serial number or series

### Know your customer information

- The customer is identified as a politically exposed person or linked to one.
- Customer is linked to adverse, crime-related media
- The customer is matched through screening against an Australian or international sanctions list or PEP list
- The customer is a member of, or linked to, a known terrorist organisation
- The customer's source of wealth or source of funds is unexplained and inconsistent with their profile
- The customer's source of wealth and funds indicates they are linked to a business in an industry known for being cash-intensive. Therefore, EGM play/cashing out for a cheque or EFT payment may indicate they are putting the business' gross takings through EGMs to avoid paying tax.

## 4. Procedure – Action to be taken

1) Where a staff member identifies a matter which may be considered unusual, they are required to report the issue, as soon as is reasonably practicable, to their immediate Duty Manager. Use the UNUSUAL MATTER REPORT.

2) The Duty Manager will record the details of the unusual matter that has been reported to them using the UNUSUA MATTER REPORT and notify the AML/CTF COMPLIANCE OFFICER. If the customer is not known to the Club – the Duty Manager will collect as much information as possible about the customer without tipping them off.

    a) If possible inform the customer that the Club needs to update its records and will request the patron to complete a new MEMBERSHIP APPLICATION FORM.

    b) If the customer is not already a member, encourage them to join.

    c) Check the SIGN-IN REGISTER for sign in details and verbally collect and confirm the customer's name, address and date of birth, verify against their ID.

    d) If the customer is an existing member, check the Membership Data base for details.

    e) If possible, inform the member that the Club needs to check its records and confirm membership details with them. Verbally collect their name, address and date of birth, verify against their ID.

3) Notify the AML/CTF COMPLIANCE OFFICER as soon as possible.

IMPORTANT:

Reports of unusual matters must not be completed in the presence of customers. Customers must not be informed that suspicion has been formed on a matter, or that a Suspicious Matter Report (SMR) is being, or has been completed.

## 5. Related Documents:

POLICY: SUSPICIOUS MATTER

PROCEDURE: UNUSUAL MATTER REPORT FORM

PROCEDURE: CUSTOMER IDENTIFICATION FORM

PROCEDURE: ENHANCED CUSTOMER DUE DILIGENCE

# MEMBERSHIP APPLICATION FORM