



ANTI MONEY LAUNDERING & COUNTER TERRORISM FINANCING

PART A

OBJECTIVE

To comply with the Federal Government Anti-Money Laundering /Counter Terrorism Financing legislation (AML/CTF Act).

Gaming transactions (“payouts”) for amounts of \$10,000 or more are subject to special identification requirements using “reliable information”. “Suspicious activity” will need to be recorded and reported to AUSTRAC as will “threshold transactions”. There are also requirements relating to:

- employee training and due diligence;
- privacy, secrecy and storage of information collected and reports supplied to AUSTRAC; The AML/CTF Act and rules require a club to have appropriate “programs” (processes) in place that address these requirements and the following sections expand on details of these requirements.

SCOPE

All gaming/cashier staff (including managers & Club Directors) are to receive a copy of this program at the time of induction/training, updated versions and as directed with refresher training. Each employee is to have a signed copy of this document maintained in Club records. Existing employees (as at time of AUSTRAC review) and future employees will be required to attend an in-house training program to receive updated training on this reviewed Part A document and the Part B document.

RISK ASSESSMENTS

The risk assessment process used in the following Part A program is a modified version of the risk matrix used in Occupational Health & Safety Risk Management and as described in the Austrac E-Learning documents.

AML/CTF PART A PROGRAM

1 (a) Identify the customer types including any politically exposed persons at South Tweed Sports

The customer demographics of the Club reflect the shire generally with an ageing population, particularly those of 65 years and over and a lower average (than national or NSW) of Overseas born persons and speakers of languages other than English. The majority of the population is Australian born (84.7%) with only 15.3% born overseas. In addition, the majority of the overseas born are from the UK, New Zealand or South Africa and are English speaking.¹

¹ Tweed Shire Community Profile, community profile communities working together Tweed Shire Council May 2008



Religious affiliation is shifting as the population becomes more dynamic and broader social changes occur in Australia. Mainstream Christian church affiliation has declined for the Anglican and Roman Catholic denominations while the small numbers of Buddhist, Hindu, Muslim and Jewish adherents have all increased. In addition, the number of people professing no religious affiliation has also increased.²

STS Club membership is regulated by state legislation and membership is attained through a process which involves identification and recording. Members are usually known to staff, management and other members through relationships built over a long period of time.

Non-members are also admitted to STS, however this involves a process of identification and recording and is also regulated by state legislation governing clubs.

The designated services for AML/CTF purposes provided by clubs involve prize payouts on gaming machines and wagering. In a club environment these services are generally regarded as low risk and are considered low risk at STS. When coupled with the nature of STS patronage it is likely that the majority of customers can be regarded as posing a low risk in terms of money laundering/terrorism financing considerations.

Politically Exposed Persons

Identifying the type of customer is a factor in assessing risk. For example, if a significant proportion of customers are foreign nationals and the services provided are that of a “boutique” bank with significant overseas transactions as opposed to say a local credit union, then the risk posed from Politically Exposed Persons (PEPs) is likely to be a consideration when developing an AML/CTF program.

PEPs are defined as³:

“ .. individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government ,judicial or military officials, senior executives of state owned corporations, important political party officials. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories. “

STS is a community based organisations with a majority of patrons being regular and typically residing in the local area. Over 75% of members residing in the existing postcode of 2486 or one either side, 2485 or 2487. Additionally, the designated services provided by clubs like STS, in the context of AML/CTF considerations, are straightforward, transparent and relatively low risk.

Unless there are reasons to suggest otherwise, it is highly unlikely that PEPs would be a consideration for STS in assessing their AML/CTF related risk exposure.

1 (b) Identify the AML/CTF risks associated with customer types including any politically exposed persons at South Tweed Sports.

The risk assessment rated this a low-medium risk (see Risk Assessment Customer Types). The action required is consistent with existing legislative requirements as it applies to membership and bona fide visitation.

From a control perspective, the risk (customers/PEPs) cannot be eliminated, substituted, or isolated. Engineering controls may include zero tolerance on the production of appropriate identification for new memberships or visitation while Administrative controls of staff training, performance appraisals and refresher training aid in maintaining the current risk status.

² *Ibid.*

³ AUSTRAC Guidance Note – “Risk management and AML/CTF programs – September 2007”, clause 6.6 in ClubsNSW Anti Money Laundering and Counter Terrorism Financing GUIDELINES FOR CLUBS (2007) [15].



2. Identify the designated services STS provides and assess the risks posed by such designated services.

GAMBLING SERVICES

These services are related to prize payments resulting from wins or accumulated credits on gaming machines or wagering (ClubTab).

3. Identify the AML/CTF risk area/behaviour associated with the designated services STS provides.

The designated services are gambling services (poker machines and TAB [wagering]). A basic set of risk considerations are:

a. Third party purchase of significant prize or payout entitlements.

The most common reported money laundering related activity likely to present itself in clubs involves a person ("third party"), different from the person, who placed the bet(s) and won the prize(s), i.e. the actual prize-winner, offering to purchase the prize for cash. The prizes are usually larger prizes with a value of more than a few hundred dollars and can involve linked jackpot or standalone machine prizes. The risk is considered low due to the staff supervision (both machine attendants and supervisory) on the machine floor and the regularity and familiarity of the customer base.

With the gradual proliferation of ticket in ticket out technology [TITO], purchase and redemption of higher value tickets is also likely to provide an opportunity for money laundering activity. Any indication of this activity should be treated as suspicious and should be further investigated. Also considered a low risk, TITO is not in place at STS as of July 2018.

Such activity is likely to take place without any knowledge of the club management or its staff and the club may only be alerted if outside information is received. Staff that happen to witness an event or if it is identified by examination of video surveillance records where these are available should be further investigated.

Another scenario might involve collusion between staff and the money launderers to facilitate such activity. This could take the form of staff alerting the money launderer to significant payout situations and facilitating the introduction of the money launderer to the prize winner or simply not reporting suspicious activity to management. It is likely that such occurrences are infrequent and with the majority of staff at STS with ten (10) years or more of service the trust factor is high and so the risk deemed low.

Risk Assessment - The risk assessment rated this a medium risk (see Risk Assessment 3rd Party).

From a control perspective, the risk cannot be eliminated, substituted, isolated or engineered. Administrative controls that inform customers (signage), staff training and risk assessment of any new technology aid in maintaining the current risk status.

b. Abnormal play and credit redemption i.e. cancelled credit/ticket out.

A typical scenario involves a player(s) inserting significant amounts of cash and after minimal or no play redeeming the playing credit and in the process acquiring a club cheque or cash and establishing a record of the transaction. Unless more sophisticated electronic monitoring techniques are available this type of behaviour is difficult to detect and requires more detailed investigation to substantiate. It is also likely that this type of activity is infrequent as indicated by the media article below.

Victorian Commission for Gambling Regulation Chief Peter Cohen said: "Suspicious transactions" -- those where large sums are won after little gameplay -- are recorded on every machine in Victoria. Mr Cohen said investigations into such transactions had found no evidence of money laundering. " (The Herald Sun - September 17, 2006, "Crims cash in on pokies").



Where a player inserts cash and redeems the credit with minimal or no play suspicion would be aroused if an unusually high number of redemptions over a relatively short period of time had taken place and when taken together amounted to a significant amount of money. Where a player inserts large amounts of cash and turns over (bets) the money or a bets a significant portion of the money by playing the gaming machine then unless there is other independent intelligence/information available it is difficult to conclude that the activity is suspicious.

If there are reasons to suspect that money laundering is occurring, STS has electronic player tracking systems and individual player activity can be identified and so there is some ability to analyse the data collected to support or dismiss any suspicions. For example it may be possible to review the history of time spent playing in relation to turnover, wins and cancelled credit/money-out records to support or dismiss suspected abnormal behaviour.

Furthermore, the staff are trained and alert to unusual numbers of machine cancel credit docket and will advise their Supervisor where occasions arise that raise suspicion. This combined with the existing technology assists in determining the risk at a low level.

Risk Assessment - The risk assessment rated this a medium risk (see Risk Assessment Abnormal Play-Credit Redemption).

From a control perspective, the risk cannot be eliminated, substituted, isolated or engineered. Engineering controls are unable to stop the playing of gaming machines where high volumes of cash are inserted with little or no play occurring before any collection.

Administrative controls that trigger staff investigation of potentially suspicious activity aid (high cash volume/little or no turnover) and docket analysis (multiple dockets on one machine or multiple dockets to one player) in maintaining the current risk status.

c. Multiplayer games (MTGMs).

Not applicable to STS as there are no MTGM's. This section will be added if/when MTGM's are purchased for the gaming room.

Risk Assessment – There has been no risk assessment conducted as there are no MTGMs currently. Before any installation of such machines occurs, a risk assessment will be conducted.

d. Stolen or counterfeit money.

In these cases the motivation is to exchange the stolen or counterfeit money for legal currency with or without a transaction record. Depending on the circumstances, note acceptors may not be able to discriminate between stolen or counterfeit notes and unless there are other reasons to suspect abnormal behaviour e.g. a large amount of money deposited in the gaming machine and redeemed with minimal or no play or other reasons to suspect the players intentions such as unusual behaviour, then this activity is unlikely to be detected until the cash held in the machine is cleared and counted.

An example of this activity in NSW involves the discovery of stolen notes in gaming machines. The notes were marked with dye but the extent of the marking did not allow the note acceptor to reject the notes.

A MAN has been charged after dye-stained banknotes, allegedly stolen from an ATM, were used to play poker machines at a hotel in Sydney's west. Staff at a hotel at Regents Park tipped off police on Thursday after noticing that dye-stained money had been fed into machines at the hotel. Police went to the hotel and arrested a man a short distance away.....Police allege the money came from an ATM stolen from Bondi Junction in late March.

(The Daily Telegraph, 21 April 2007, "Arrest after stolen cash used in pokies")



Risk Assessment - The risk assessment rated this a medium risk (see Risk Assessment Abnormal Play-Credit Redemption).

From a control perspective, the risk cannot be eliminated, substituted, isolated or engineered. Engineering controls are unable (currently) of detecting counterfeit or stolen (dyed) money.

Administrative controls that trigger staff investigation of potentially suspicious activity aid in maintaining the current risk status.

e. Wagering.

TAB operations under the AML/CTF have designated services with risks associated with;

Helping customers to open a TAB account

Risk Assessment - The risk assessment rated this a medium risk (see Risk Assessment Wagering New Accounts).

From a control perspective, the risk cannot be eliminated, substituted, isolated or engineered. Administrative controls minimise the risk via zero tolerance on the production of appropriate ID documentation.

Dealing with cash amounts of \$10,000 or more (Threshold Transaction Reports)

From a control perspective, the risk cannot be eliminated but the system put in place by TAB/SSC has made the risk even lower. Administrative controls minimise the risk via completing the appropriate TTR/SMR documentation and speaking with the SSC staff. Staff safety is paramount and so an occasion may arise that staff may need to complete the transaction where the customer information is insufficient; in that case it will be likely a suspicious activity requiring more information and reporting.

Reporting on something that is suspicious (Suspicious Matter Reports)

This might include situations where:

- ☐ A customer asks not to be reported
- ☐ A customer asks how to avoid being reported
- ☐ A customer splits or attempts to split transactions to get below the \$10,000.00 cash total
- ☐ A customer refuses to show ID or give details for a threshold transaction report

In these cases staff are required to complete a suspicious transaction report.

Further information on TAB and AML/CTF is available in the TAB AML/CTF section of the Operators Manual.

4. Identify the methods of delivery the services STS provides and assess the risks posed

The delivery of club designated services is strictly regulated. The summary of clauses under the *Gaming Machine Regulation 2002* (NSW) illustrates the legislative environment applying to clubs in New South Wales and other states. The method of delivery is highly controlled with significant regulatory requirements for identification and records. It is reasonable to agree with the Industry body ClubsNSW conclusion that in the case of clubs the method of service delivery poses very low risk.



In the overall context of designated services i.e. AML/CTF Act, Section 6, those services provided by clubs can be considered relatively low risk. This arises both because of the simple nature of these services i.e. an uncontrolled random win on a gaming machine or sporting/wagering event triggers the service and the highly regulated/controlled environment in which the triggering event and service is offered.⁴

Gaming Machines Regulation 2002 (NSW)

Clause 15 Records relating to prizes to be kept by clubs

Clause 18 Meters

Clause 19 Additional records by clubs

Clause 20 Clearance and refilling of gaming machines in clubs

Clause 43 Requirement to keep record or copy of player activity statement

Clause 77 Authorised progressive gaming machines—reading and recording of meters and jackpot reconciliations

Clause 78 Authorised progressive systems—reading and recording of meters and jackpot reconciliations

Clause 87A Requirement to keep record or copy of player activity statement under this Part

Clause 95 Records of gaming machine tickets issued

Clause 98 Records to be made on redemption

Clause 99 Separate records of certain gaming machine tickets

Clause 100 Unclaimed gaming machine tickets

Clause 102 Records and other material

Clause 137 General requirement for records to be kept for 3 years

Dealings with foreign jurisdictions

In terms of the provision of gambling services by clubs this risk consideration can be regarded as not applicable unless a club assesses otherwise. STS has no presence or business links with foreign jurisdictions.

Size of gaming machine operation

Relative to the risk posed by other designated services such as bullion dealers or financial services involved with the transfer of money, the overall risk posed by gaming machines is generally acknowledged as low⁵. This view is partly reflected by the AML/CTF Act and Rules which have set a transaction reporting threshold level of \$10,000.

Despite AML/CTF Rules setting a reporting threshold of \$10,000 money can be laundered through a large number of smaller transactions and STS should be vigilant to indications of this type of activity. Clubs fall into a relatively broad range when categorised in terms of gaming machine revenue and turnover. For guidance in assessing average gaming machine operation size and activity Table 1 (next page) lists clubs in terms of revenue bands together with the average revenue and turnover per gaming machine.

⁴ See above n 3 [16].

⁵ *Ibid.*



Table 1 - Summary NSW club gaming machine statistics

Club Annual Gaming Machine Revenue Band	Average number of gaming machines	Average annual revenue per gaming machine*	Average annual turnover per gaming machine	Average annual player win per gaming machine	Average return to player
\$0 to \$200,000	9	\$8,678	\$78,322	\$69,644	88.9%
\$200,000 to \$ 500,000	17	\$19,097	\$176,076	\$156,979	89.2%
\$500,000 to \$1 million	27	\$26,145	\$250,450	\$224,305	89.6%
\$1 million to \$2 million	44	\$33,049	\$331,215	\$298,166	90.0%
\$2 million to \$5 million	78	\$40,206	\$422,423	\$382,217	90.5%
\$5 million to \$10 million	141	\$48,440	\$561,535	\$513,095	91.4%
\$10 million to \$20 million	237	\$56,865	\$683,859	\$626,994	91.7%
\$20 million plus	431	\$79,368	\$1,151,955	\$1,072,587	93.1%
State wide	55	\$47,510	\$579,061	\$531,551	91.8%

- MTGMs are included in these averages
- Source: NSW Office of Liquor Gaming and Racing for year end May 2007.

Attempts at money laundering are more likely to occur in an environment where there is high gaming machine turnover and revenue and where there is access to multi terminal gaming machines (MTGMs) as opposed to those with low turnover and revenue and without MTGMs. It is suggested that for purposes of classification in terms of money laundering activity those clubs with annual gaming machine revenue less than \$2 million can be classed as very low risk, those with gaming machine revenue in the range \$2 million to \$10 million as low risk and those above \$10 million as potentially low to medium risk.⁶ South Tweed Sports revenue is between \$5M-\$6M.

However clubs falling within these broad categories may need to re-assess their risk exposure if the gaming machines are operating at levels that are significantly above the per machine averages shown. For example, if a club has 20 gaming machines and an annual gaming machine revenue of \$1.6 million, that is, \$80,000 per machine per annum, then the risk level would arguably be higher than that suggested by considering the \$1.6 million revenue only as the average revenue per machine in this band is around \$33,000. South Tweed Sports average revenue per machine as at July 2018 is just over \$43,000.

Despite this Industry basis of a low risk rating, each factor within the gaming operation that may be used for money laundering has been separately assessed and rated for risk with appropriate actions noted (see earlier and individual risk assessments).

5. Implement programs/procedures to mitigate the risk

Existing operational practices and procedures

Club gaming services operate in a highly structured and regulated environment. State legislation places a significant number of requirements on clubs which when taken as a whole ensure that the gambling environment in clubs is not only subject to high levels of security and integrity but is also a low risk environment in relation to money laundering.

Attachment (ClubsNSW 4) identifies the significant operational practices that apply to gaming machines in NSW clubs.

Employee/Staff Training

In the first instance staff training will be face to face, either one on one or in small groups. Staff will have a simple workbook to read and participate along with and at times will record information as part of the learning process. It is expected that the combined training time of Part A and Part B will be one (1) hour. The staff involved in the training will

⁶ See above n 3 [17]



be all gaming, cashier and TAB staff. Front Reception staff will receive a varied program designed to link the responsibilities of correct membership and visitation procedures and how such procedures link with the AML-CTF program.⁷

All new staff deployed (or existing staff to be trained) in relevant areas/activities will receive the training as part of their induction.

Initial training and refresher training will focus on;

- Procedures applying under state legislation regarding entry requirements i.e. identification and sign in procedures and the risk analysis process;
- Procedures under state legislation regarding prize payment procedures i.e. identification and records to be kept and the risk analysis process;
- Specific AML/CTF requirements for identification applying to payouts over \$10,000 (see “safe harbour” identification requirements)
- Awareness and reporting of “suspicious” activity to the compliance officer or designated management persons. This includes awareness of requirements related to privacy and secrecy.
- Awareness that a maximum penalty¹⁶ of 100,000 units (\$11 million) for a company and 20,000 units (\$2.2 million) for a person can be incurred if the CEO of AUSTRAC undertakes proceedings in the Federal Court and a civil penalty order is issued.

Refresher training will occur within six months of staff receiving the updated (to be approved by AUSTRAC) training material.

Employee Due Diligence

The very low to medium AML/CTF risk posed by clubs, the nature of the regulatory framework in which clubs operate, particularly processes in place that deal specifically with identification and recording practices related to prize payouts and entry requirements, indicate that for STS their existing human resources/industrial relations employment and staff policies/programs should be sufficient to meet the employee risk posed in relation to money laundering and terrorism financing.

Risk Assessment - The risk assessment rated this a medium risk (see Risk Assessment Employee Due Diligence).

From a control perspective, the risk cannot be eliminated, substituted, isolated or engineered. Administrative controls minimise the risk through screening of all new employees, consideration of screening of transferred or promoted employees and making staff aware of the consequences of breaching AML-CTF obligations.

6. Ensure oversight of the program by the club Board and senior management and implement an independent review process.

Compliance Officer

Chief Financial Officer Alex Gilks is the appointed Compliance Officer in relation to this AML/CTF policy. Brendan Walsh (Gaming & IT Manager) will be trained to the level of Compliance Officer who then may cover any absences of Alex Gilks.

⁷ The AML/CTF Act does not impose a requirement on clubs to identify customers at entry; however state legislation does impose such a requirement. Information obtained at entry can be of assistance in preparing suspicious activity reports and is part of a framework that clubs already have in place and which can be used to mitigate the effects of money laundering and terrorism financing in *ClubsNSW* see above n 3 [20].



Board and senior management oversight

Compliance Officer Alex Gilks will report monthly (within his Finance/Gaming report) to the Board and itemise any suspicious activity reports generated and discuss any changes to procedures/processes or the program. In his absence, Brendan Walsh will fulfill this reporting function.

Independent Review

The Board's Internal Audit committee will review this policy and program as part of its annual compliance audit. The checklist (refer attachment ClubsNSW 3) in the ClubsNSW AML/CTF guidelines is an appropriate audit document for a venue of low-medium risk like STS.⁸

AUSTRAC Feedback

AUSTRAC may provide STS with feedback on the entity's AML/CTF program or any other industry-wide AML/CTF matters. STS has an obligation to address any shortcomings to comply with the AML/CTF Act and Rules, even if AUSTRAC does not provide feedback directly.

Feedback may be reported in the Compliance Officer's monthly report or the Internal Audit (Board) review. Once received, STS must take action within 30 days (or earlier if a requirement).

Implement a Suspicious Activity Program/Process

Examples of suspicious activities associated with club designated services are identified earlier in section 2. Staff who observe suspicious activity associated with the gaming services are required to communicate their observations and details to their immediate supervisor. The supervisor then passes on such details to the compliance officer (Alex Gilks or in his absence Brendan Walsh) who would generate a suspicious activity report if in their opinion there are reasonable grounds to do so.

Staff should consider their role to be pro-active. STS would rather staff err on the side of caution and report concerns even if such occurrences prove to be above board. A SMR (Suspicious Matter Report) must be submitted within 24 hours of forming the suspicion.

Implement procedures to ensure that information and records accumulated as a result of the AML/CTF programs comply with privacy, secrecy and storage requirements.

In relation to secrecy it is important to note that a person must not be "tipped off" about any suspicious activity report. Records i.e. AML/CTF records which consist of the AML/CTF program, threshold transaction reports and suspicious activity reports (if any) require to be kept for seven (7) years.

9. Threshold Transaction reporting program/process.

Any wagering or gaming machine payout of \$10,000 or more that is paid in "physical currency", i.e. cash or "e-currency" is subject to reporting within 10 business days and in a form approved by AUSTRAC. For most clubs state legislation restricts gaming machine cash payouts to values of less than \$10,000. Threshold transaction reports form part of the AML/CTF compliance officer's responsibility.

⁸ Given this has not occurred to date, the Board will be asked to complete the first independent review within six months of AUSTRAC ratifying the submitted updated documents



10. Ongoing Customer Due Diligence (OCDD)

Know your customer information (KYC)

Your AML/CTF program will need to address whether and in what circumstances further KYC information about your customers should be updated or existing KYC information verified.

Trigger points could include:

- a significant transaction or series of transactions taking place or a significant change in the way an account has been operated by a customer (e.g. known patron gambling beyond traditional patterns)
- doubts arising about the identity of a new customer conducting significant transactions

Risk Assessment - The assessment rated this an acceptable risk (see Risk Assessment KYC-Identification).

From a control perspective, the risk cannot be eliminated, substituted, isolated or engineered. Administrative controls minimise the risk with staff vigilance and investigation as detailed in the risk assessment.

Transaction monitoring program

Examples of suspicious transactions include:

- significant transactions (in terms of amount or volume) for that customer
- transactions that exceed transaction or amount limits
- very high account turnover inconsistent with the size of the balance
- transactions outside the regular pattern of an account's activity.

The monitoring program of STS includes CCTV, player tracking (members), observations, member or visitor identification documents.

Enhanced customer due diligence

This program must be applied where STS assess ML/TF risk is high, or when a suspicious matter reporting obligation arises. In applying enhanced customer due diligence we may consider:

- seeking further information from the customer or third-party sources to clarify, update or obtain the customer's KYC information; consider any suspicion that may be reportable to AUSTRAC
- undertaking more detailed analysis of their KYC information
- verifying or re-verifying KYC information
- analysing the customer's past transactions and possibly monitoring future transactions
- whether a suspicious matter report ought to be lodged with AUSTRAC.

If we lodge a suspicious matter report in relation to a pre-commencement customer, we are required to verify that customer's identity under section 29 of the AML/CTF Act.

Trigger points could include:

- a significant transaction or series of transactions taking place or a significant change in the way an account has been operated by a customer (e.g. known patron gambling beyond traditional patterns)
- doubts arising about the identity of a new customer conducting significant transactions



FURTHER INFORMATION

For further information refer to Background Material - ClubsNSW 2007 – Part 1/2 - AML/CTF for Clubs or AUSTRAC
www.austrac.gov.au

IMPLEMENTATION

This policy/program document will be presented for Board approval at the August 2010 meeting.⁹

BREACH OF POLICY

The club has an obligation to consistently enforce this policy. Likewise, staff must also enforce this policy through compliance. Any staff member (including management) that breaches this policy shall be subject to counselling and/or disciplinary action which *may* include termination of employment.

NOTES – CHANGES/AMENDMENTS TO POLICY

DATE	CHANGE (& reason for)	RATIFIED (Board)

⁹ Or the next available Board meeting following AUSTRAC ratification