



Section 8. Money Laundering & Terrorism Financing Sample Staff Awareness Training.

DRAFT - SUBJECT TO PROFESSIONAL STANDARDS REVIEW

Sydney
29 February, 2016

Deloitte.

Audit. Tax. Consulting. Financial Advisory.





Instructions

Suggested instructions for staff AML/CTF training program

- Alert staff involved in providing gambling and/or foreign currency exchange services to the AML/CTF program:
 - supply a copy of the program;
 - require staff member to acknowledge in writing that they have received, read and understood the program;
 - advise staff of identity of AML/CTF Compliance Officer; and
 - advise staff of new procedures under the AML/CTF program (eg. customer identification and verification).
- Specific AML/CTF training for staff is to cover:
 - the Hotel's obligations under the Act and AML/CTF Rules;
 - the consequence of the Hotel's non-compliance with the Act and AML/CTF Rules;
 - the type of ML/TF risk that the Hotel might face and the potential consequences of each risk; and
 - the Hotel's processes and procedures under its AML/CTF program that are relevant to the work carried out by each employee.
- Provide staff with ML/TF risk awareness training.
 - This can be provided as part of normal compliance training (eg. alongside responsible service of gambling (RSG) or responsible service of alcohol (RSA) training).
 - It should be provided to:
 - all existing staff;
 - all new staff; and
 - thereafter on a regular, refresher basis (similar to RSG and RSA).
- AUSTRAC provides e-learning courses which can be found at www.austrac.gov.au/courses.html.
- A draft awareness training pack is attached.
- ***The awareness training must be delivered to all employees. More detailed training will need to be delivered to those employees involved in the provision of gambling and/or foreign currency exchange services or those employees who may be exposed to ML/TF risks at the Hotel.***



Limitations and disclaimers

Limitations

This report should be read in its entirety.

This report does not constitute legal advice. Our review and comments are provided to you in our capacity as professional advisers based on our professional experience and expertise.

This engagement was performed in accordance with the scope of work agreed between AHA and Deloitte. In performing this service, we have complied with Australian Professional Standard (“APS”) 8, the Statement of Management Consulting Services^[1].

Where Deloitte has provided advice or recommendations to the AHA, we are not responsible for whether, or the manner in which, suggested improvements, recommendations, or opportunities are implemented. The management of the AHA, or their nominees, will need to consider carefully the full implications of each of these suggested improvements, recommendations or opportunities, including any adverse effects and any financing requirements. Based on their consideration, the management of AHA should make decisions as appropriate.

The work performed and detailed in this report does not constitute an assurance engagement in accordance with Australian Auditing Standards.

The matters detailed in our report are only those which came to our attention during the course of performing our procedures and do not necessarily constitute a comprehensive statement of all the weaknesses or issues that exist. Accordingly, management should not rely on our report to identify all weaknesses and issues that may exist in the systems and procedures discussed. The report should be read in the context of the scope of our work. Had we performed additional procedures or had we performed an assurance engagement in accordance with Australian Auditing Standards, other matters might have come to our attention that would have been reported to you.

This report should not be relied upon as a substitute for actions that the AHA should take to assure itself that the controls are operating efficiently.

This report and all deliverables have been prepared solely for the use of AHA, and should not be quoted in whole or in part without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose.

Liability limited is by a scheme approved under Professional Standards Legislation.

[1] APS 8 is issued by the National Councils of the Institute of Chartered Accountants in Australia and of the Australian Society of Accountants.

Disclaimers

Deloitte refers to the Australian partnership of Deloitte Touche Tohmatsu and its subsidiaries. Deloitte, one of Australia’s leading professional services firms, provides audit, tax, consulting, and financial advisory services through around 3000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit Deloitte’s web site at www.deloitte.com.au.

Deloitte is a member of Deloitte Touche Tohmatsu (a Swiss Verein). As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other’s acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names “Deloitte,” “Deloitte & Touche,” “Deloitte Touche Tohmatsu,” or other, related names. Services are provided by the member firms or their subsidiaries and affiliates and not by the Deloitte Touche Tohmatsu Verein.

Liability limited by a scheme approved under Professional Standards Legislation.

Confidential - this document and the information contained in it are confidential and should not be used or disclosed in any way without our prior consent.

© Dec, 2007. All rights reserved.



Glossary

Some AML/CTF terms are shown below.

Glossary of AML/CTF Terms

AML/CTF – Anti-Money Laundering and Counter-Terrorism Financing

AUSTRAC – Australian Transaction

Reports and Analysis Centre

CDD – Customer Due Diligence

DFAT – Department of Foreign Affairs and Trade (Australia)

EDD – Employee Due Diligence

FATF – Financial Action Task Force

FTRA – Financial Transaction Reports Act 1988 (Cth)

HR – Human Resources

KYC – Know Your Customer

PEP – Politically Exposed Person

ML/TF – Money laundering and Terrorism Financing

SOFTA – Suppression of Financing of Terrorism Act 2002 (Cth)

SLAs – Service Level Agreements

SUSTRs – Suspicious Transaction Reports

The AML/CTF Act – Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)

The Rules – AUSTRAC consolidated AML/CTF Rules registered at project commencement.



How can you make your team aware of the new requirements?

AML/CTF training should be undertaken on the basis of risk presented by each position

Initial awareness sessions should be conducted with staff to assist them to apply the AML/CTF program provided in the Kit

Key focuses should be on:

- What is money laundering and terrorism financing?
- What to look for?
- How to manage an incident?
- What are the obligations of staff and management?
- Where to get help?
- *Staff need to be trained differently according to responsibilities and risks they manage*
- Ongoing training
- Currently this is envisaged to be part of the existing training framework
 - Licensing training
 - Responsible gaming accreditation.



Money laundering and gaming machines

Gaming/Poker machines and foreign currency exchange have been regulated for some time under the existing FTRA and SOFTA legislation. The new AML/CTF Act enhances obligations

The new law includes

- Enhanced laws and rules related to gaming industry
- Customer identification and due diligence for \$10,000 or more
- Suspicious activity reporting remains a focus
 - It is an offence to 'tip off' or tell a client a suspicious report is being filed
- AML/CTF compliance programs
- Common rules for casinos, pubs and clubs
- Terrorism financing
 - It is an offence to deal with terrorists
 - Terrorists can be both domestic and foreign
 - You have obligations to check names for large payouts and suspicious matters against government terrorist lists. Your state AHA office can guide you in respect of these lists.

What are money laundering and terrorism financing?

Money laundering (ML) is the process of taking money from illegal activity (predicate crimes) and making it appear to be legally obtained. Terrorism financing (TF) includes the financing of terrorist acts, terrorists and terrorist organisations, using processes similar to money laundering.

Placement

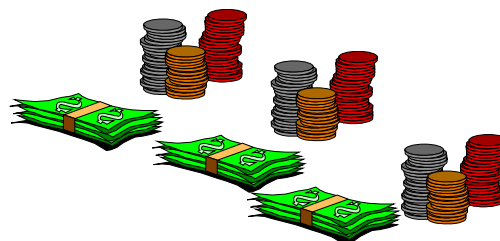


This is the first step in the process. Cash is placed into financial system.

Examples: Deposit Cash into gaming machines, "smurfing" (distribution of cash in small amounts), cash converted into monetary instruments, asset purchase to disguise cash



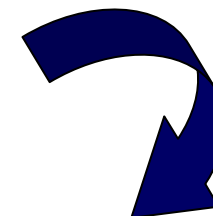
Layering



After the money is placed, it is moved around to break the investigative trail.

Obtaining cheques from hotels to explain the funds as winnings would be an obvious example of how to do this

Examples: Assets sold, movements of assets/funds/instruments designed to distance money from the crime



Integration



After the money has been disguised, it is removed by the criminal organization.

Examples: Property/asset purchases, successful mingling of crime proceeds with legitimate business income, elaborate use of corporate vehicles and listed companies



Legislative obligations

Each venue is obliged to conduct staff awareness

The Hotel's AML/CTF risk awareness training program will be delivered to all relevant employees. In summary, the program should be designed to enable employees to understand:

- the obligations of the Hotel under the Act and AML/CTF Rules
- the consequences of non-compliance
- the type of ML/TF risks the Hotel might face and the potential consequences of such risk
- the processes and procedures set out in the Hotel's AML/CTF program that are relevant to the work carried out by the employee.



Key obligations for your hotel

Customer identification and reporting are key obligations

The Act requires those involved in the providing designated services to:

- identify their customers before providing certain services
- report certain transactions above a monetary threshold
- report suspicious matters.



Key obligations for your hotel's AML Program

Your AML/CTF Program needs to include these components

	Gaming & Foreign Currency Exchange Programs
Risk identification and mitigation	√
Record keeping	√
Independent review	√
'Board' / management oversight	√
Training and awareness	√
Suspicious and significant transaction/matter reporting	√
Staff identification and due diligence	√
Customer identification, KYC, additional KYC/enhanced due diligence	√
Program reports to AUSTRAC	√



Obligation changes from the introduction of risk-based law

AHA members are impacted by Australia's adoption of an expansive application of a risk-based anti-money laundering and counter terrorism financing regime, but many obligations are not new

Prescriptive / Reporting Approach Specified Businesses (Narrow Application)

Financial Transaction Reports Act 1988 (FTRA)

- Applicable to Cash Dealers which includes pubs, clubs and casinos
- Reporting regime, requiring strict compliance with specific measures (e.g. 100pts check)

Suppression of the Financing of Terrorism Act 2002 (SOFTA)

- All businesses in Australia prohibited from dealing with terrorists

State gaming machine legislation

- Generally prescriptive in nature

12 December 2006

Risk-Based Approach Activity-Based (Broad Application)

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

(Expanded coverage, did not repeal FTRA 1988 or SOFTA 2002)

Applies to specified activities ('designated services') rather than business types – what you do is the most important thing

Risk-based approach, with providers of designated services required to develop and implement individualised AML programs

There is no "right answer" – principles guide what you should do



Why should you care?

There are many reasons why this is important for staff and licensees

- Community obligations
 - AHA members are committed to being good citizens
- The new legislation carries a series of penalties which can be levied against individuals (staff and officers, including companies), Penalties include:
 - Custodial sentences for serious offences
 - Fines of up to \$11 million per offence for corporate and \$2.2 million for individuals
 - Loss of license – violations are material considerations for state gaming authorities
- Customers who violate the law are also subject to penalties
- AUSTRAC has other enforcement powers including the power to appoint an auditor to review your program.



‘Predicate’ crimes that produce dirty money

Commonly observed crimes

- theft from employer
- participation in an organised criminal group and racketeering
- terrorism, including terrorist financing
- trafficking in human beings and migrant smuggling
- sexual exploitation
 - obtaining benefits from prostitution
 - including sexual exploitation of children
- trafficking in drugs and psychotropic substances
- illicit arms trafficking;
- illicit trafficking in stolen and other goods;
- counterfeiting currency
- counterfeiting and piracy of products
- tax evasion and avoidance
- fraud – including social security fraud
- corruption and bribery
- murder, grievous bodily injury
- kidnapping, illegal restraint and hostage-taking
- robbery or theft
- smuggling
- extortion
- forgery
- piracy
- environmental crime
- insider trading and market manipulation.



When is a customer high risk?

Customer risk needs to be assessed continuously, understanding profiles and red flags is helpful in identification of risk

The customer behaviour is suspicious where they act or do something that is or is like a Red Flag (see following slides)

'Red flags' are provided in the next few slides. The purposes are to:

- Raise staff awareness
- Trigger questions
- Determine if a customer needs to be identified for a matter of less than \$10,000
- Indicate to the venue's staff the common types of practical situations where a risk of ML/TF may exist
- Determine whether a *Suspicious Transaction/Matter Report* should be filed
- Help staff recognise possible money laundering and terrorist financing schemes, lists are not all-inclusive, but indicators based on real examples

Known customer attributes may also indicate higher risk

- They are from overseas and are hard to identify
- They are a politically exposed person (PEP) (they are from overseas and are an important person that may have obtained funds from corruption)
- They are from a high risk jurisdiction (see tool in the Kit)

Customer AML/CTF red flags (high risk and suspicious matter indicators)



What is suspicious behaviour and when is a customer high risk?

- Customers who provide insufficient or suspicious information
 - Reluctant to provide complete information on identity or occupation if asked
 - Uses unusual or suspicious identification documents that cannot be readily verified
 - Background differs from that which would be expected based on information provided and activities
 - Home/Business telephone is disconnected or wrong
 - Makes frequent or large transactions with no record of past patronage of the venue.
- Efforts to avoid reporting or record keeping requirement
 - A customer or group
 - Tries to persuade an employee to not file required reports or to not maintain required records.
 - Is reluctant to provide information needed to file a mandatory report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed
 - Is reluctant to furnish identification when obtaining a cheque payout (includes <\$10,000)
 - Asks to be exempted from reporting or record-keeping requirements
 - Asks for several cheques to be made below the \$10,000 / specified threshold
 - Uses multiple loyalty scheme cards with no apparent purpose other than to manipulate records of play.
- Changes in transactions
 - A rapid increase in the size and frequency of sessions with no corresponding explanation
 - Inability to track the true owner of funds being played
 - Significant turnover in large denomination bills that would appear uncharacteristic given players “story”/ (employment etc).

Customer AML/CTF red flags (high risk and suspicious matter indicators)



What is suspicious behaviour and when is a customer high risk?

Activity inconsistent with the customer's business / occupation and previous history

- The transaction patterns show a sudden change inconsistent with normal activities
- A large volume cash deposited into EGMs, when the nature of the customers business or occupation would not appear to justify such activity
 - E.g. salary and wage earner depositing funds from bundles of cash
 - Sources of funds are important to understand
- Customers patronising the gaming room area and then play less than expected/normal
- Customers who approach or communicate with other patrons with the objective of participation or co-opting patrons assistance in obtaining credits or winnings cheques
- Requests for transfer of funds by cheque or machine credits to other patrons.

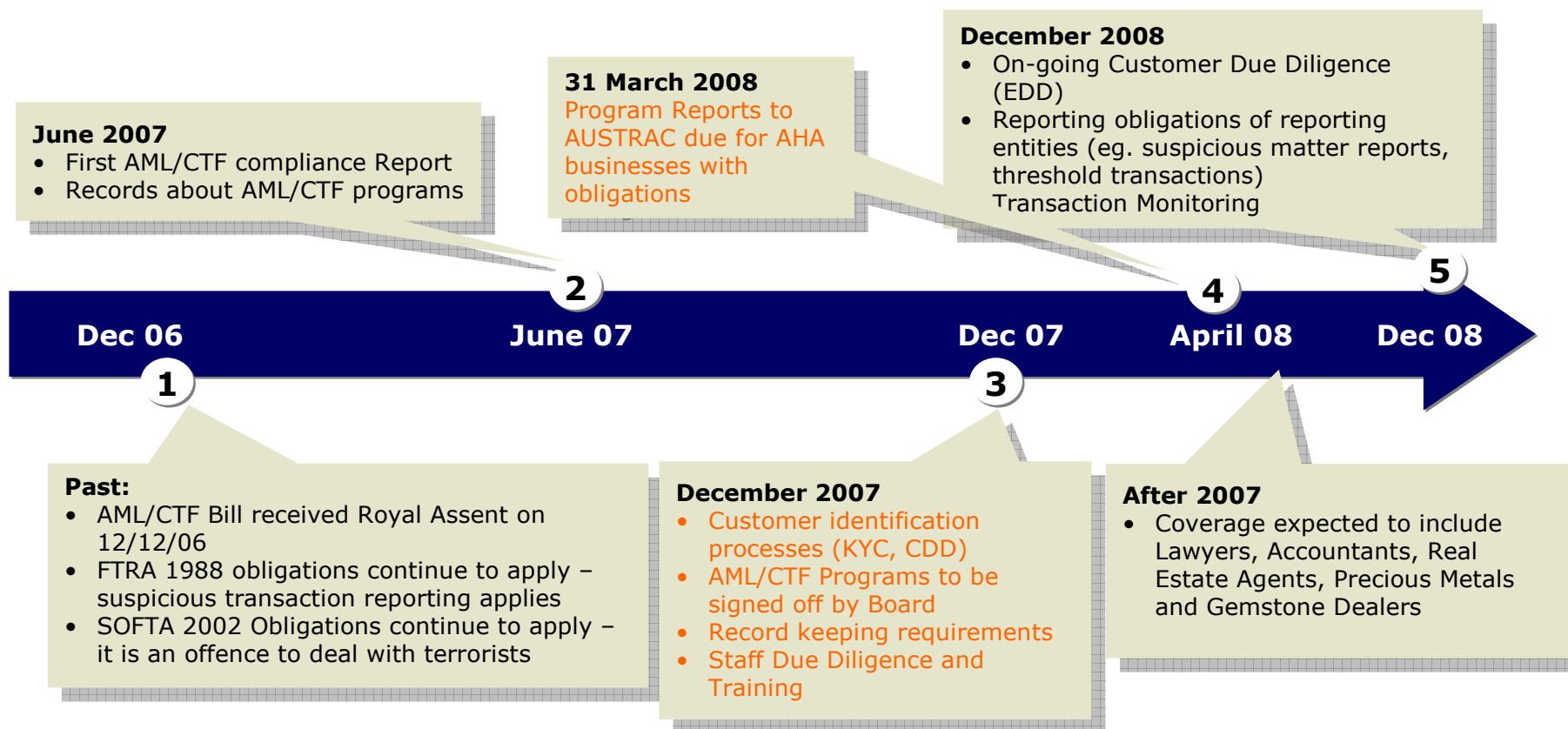
Other suspicious customer activity

- Frequent exchanges of small dollar denomination for large dollar denominations
- Frequent deposits of currency wrapped in currency straps or currency wrapped in rubber bands that are disorganized and do not balance when counted
- Purchases credits for amounts under a specified threshold
- Purchases credits from other patrons
- Customer who consistently purchases or tries to purchase large credits on machines or wins with the objective to 'double up'
- Customer who frequently asks for cheques for unplayed funds
- Putting money into slot machines and claiming the accumulated credits as a jackpot win.



What do you need to do – by when?

AHA members are currently subject to FTR Act obligations. Some existing obligations will be replaced over 2007 and 2008 by the new AML/CTF Act





Who can you call for help?

AML/CTF Program support can come via the AHA or AUSTRAC

Support

- Your state AHA office
- AUSTRAC Helpline
 - 1300 021 037
 - Help_desk@austrac.gov.au
 - Options are via seminars, on-line or phone