Anti-Money Laundering & Counter Terrorism Financing Program

Entity:	Integrity Financial Planners Pty Ltd (IFP)
ABN:	71 069 537 855
AFSL:	2250051

Contents

Intellectual Property and disclaimer

Version 1.1 – August 2021

References:

- AUSTRALIA'S FINANCIAL PLANNING SECTOR > MONEY LAUNDERING AND TERRORISM FINANCING RISK ASSESSMENT (published by AUSTRAC in 2016)
- FSC/FPA Industry Guidance (FSC Guidance Note No. 24) Managing AML/CTF, FATCA and CRS Customer Identification Obligations 19 May 2017
- http://www.austrac.gov.au/part-b-amlctf-program-customer-due-diligence-procedures

1 Background and purpose of document

1.1 Background

(a) The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (**AML/CTF Act**) imposes a range of compliance and reporting obligations on reporting entities. In general, if an entity is a reporting entity, they are required to prepare an AML/CTF Program which consists of two parts:

(i) General (Part A); and

(ii) Customer due diligence procedures (Part B).

(b) The AML/CTF Act is administered by the Australian Transaction Reports and Analysis Centre (**AUSTRAC**).

(c) Integrity Financial Planners Pty Ltd (**Licensee**) is a reporting entity for the purposes of the AML/CTF Act. The Licensee registered with AUSTRAC as a reporting entity on 23/05/2001. As a representative of the Licensee, financial advisers are required to comply with the obligations that apply to the Licensee as a reporting entity.

(d) The Licensee is exempt from the requirement to prepare a full AML/CTF Program because it merely arranges for a person to receive a 'designated service' (ie. acquiring a financial product under the Corporations Act from another reporting entity, the product issuer) (**item 54 service**).

(e) Instead, the Licensee is required to prepare a 'Special Program' which only consists of Part B. The primary purpose of Part B is to ensure that the Licensee (a reporting entity under AUSTRAC) knows its customers/clients and understands their clients' financial activities.

(f) As an 'item 54 service' reporting entity, the Licensee is exempt from lodging an annual AML/CTF compliance report with AUSTRAC.

1.2 Purpose of this document

The purpose of this document is to establish the Special Program so the Licensee has a documented framework that meets its client due diligence (**CDD**) obligations under the AML/CTF Act.

1.3 Responsibility

(a) A Responsible Manager (or a delegate with appropriate experience and seniority) will be responsible for ensuring that the Licensee and its authorised representatives meet the requirements of this Program.

(b) A Responsible Manager (or a delegate with appropriate experience and seniority) will assess the accuracy of this Program by reviewing the Program on an annual basis (unless more immediate updates are required due to legislative or regulatory change).

(c) A Responsible Manager (or a delegate with appropriate experience and seniority) will be the appointed AUSTRAC compliance officer for the purposes of this Program.

(d) Enrolment and registration procedures are set out in http://www.austrac.gov.au/businesses/enrolment-and-registration/enrolment-and-registration.

2 Money laundering

2.1 What is money laundering

Money laundering involves processing illicit profits in ways which mask ownership and make the funds appear to have come from legitimate sources. This enables criminals to hide and accumulate wealth, avoid prosecution, evade taxes, increase profits through reinvestment, and fund further criminal activity, including terrorism.

2.2 How is money laundered?

Money laundering occurs in areas ranging from banking to gaming, luxury goods to international trade, and alternative remittance to cash intensive businesses. It can involve:

(a) moving money or other property across borders (for example, international funds transfers, remittances, bulk cash smuggling and cross-border movement of bullion and jewellery);

(b) concealing money or other property domestically (for example, purchasing high-value goods and real estate, gambling and putting money into legitimate businesses).

2.3 What is the money laundering cycle?

The money laundering cycle describes the typical three-stage process criminals may use to conceal the source of illicit funds and make funds appear legitimate:

(a) **Placement:** Introducing illegal funds into the formal financial system (for example, making 'structured*' cash transactions into bank accounts).

(b) **Layering:** Moving, dispersing or disguising illegal funds or assets to conceal their true origin (for example, using a maze of complex transactions involving multiple banks and accounts, or corporations and trusts).

(c) **Integration:** Investing these now distanced funds or assets in further criminal activity or legitimate business, or purchasing high-value assets and luxury goods. At this stage the funds or assets appear to have been legitimately acquired.

*Structuring involves breaking down cash transactions into small amounts to avoid triggering mandatory reporting of cash transactions of AUD10,000 or more as required under the AML/CTF Act.

3 Special Program (Client due diligence only)

3.1 Client Due Diligence (CDD)

(a) Under this Program, the Licensee is required to be reasonably satisfied that:

(i) an individual client is who they claim to be;

(ii) for a non-individual client (eg. company or trust), the client exists and their beneficial ownership details are known.

(b) By knowing its client, the Licensee will be better able to identify and mitigate money laundering and terrorism financing risks in the conduct of their financial transactions, particularly where the activity or transactions are unusual or uncharacteristic.

(c) Under the Special Program, financial advisers are required to implement CDD procedures, including:

(i) collecting and verifying client identification information - for example, documents, data or other information obtained from a reliable and independent source;

(ii) identifying and verifying the beneficial owner(s) of a customer;

(iii) identifying whether a client is a PEP (or an associate of a PEP) and taking steps to establish the source of funds used during the business relationship or transaction;

(iv) obtaining information on the purpose and intended nature of the business relationship.

(d) When implementing the Special Program, the Licensee is also required to consider the money laundering/terrorism financing risks posed by various factors, including (but not limited to):

(i) client types

(ii) clients' sources of funds and wealth

(iii) delivery channel

(iv) any foreign jurisdictions the reporting entity deals with.

3.2 Meeting the CDD requirements

(a) In order to meet the CDD requirements, the Licensee requires its financial advisers to complete the following FSC and FPA identification forms as they apply to the client:

(i) Individual and sole traders;

(ii) Trusts (regulated & unregulated);

(iii) Companies (Australian & Foreign);

(iv) Associations;

(v) Registered Co-operatives;

(vi) Government bodies;

(vii) Partnerships;

(viii) Verifying officer.

(b) The CDD procedures outlined must be performed prior to the arranging for a person to receive a financial service from the Licensee. This requires that all the relevant customer identification information for the client be collected and verified prior to any product being provided to the client.

(c) Further information on the specific requirements of client due diligence for each respective entity can be found on the AUSTRAC 'Ready Reckoner' at http://www.austrac.gov.au/ready-reckoner.

3.3 Collection of information

(a) The person conducting the procedure must be reasonably satisfied that the client is the individual/entity he or she or it claims to be.

(b) Client identification information can be collected from sources other than the client. However, the client identification information that is to be verified must not be verified from the same source that it is collected.

(c) Tax information collected in an ID Form serves as a client's self-certification of their tax status. Contrary to other client identification information, tax information must be collected **FROM** the client or their authorised representative. Tax information must be collected prior to an account being opened for the client.

3.4 Verification of information

(a) Verification is the process the reporting entity uses to confirm that the client information provided by, or about, a client is accurate.

(b) Where the source of verification is a document, the Licensee will verify client information using an original or certified copy of a primary photographic, or primary non-photographic, or secondary document. For example, the financial adviser (as a representative of the Licensee) could verify the client's name by referring to their driver's licence that shows the client's first name, middle initial, and family name.

(c) If a client provides identification documents in a language other than English, AUSTRAC requires the Licensee to obtain a translation of the document into the English language by an accredited translator (except in circumstances where the identification documents are in another language that personnel of the reporting entity understands).

(d) Where the source of verification is via an electronic database, the Licensee (or the financial adviser) will use reliable and independent electronic data from at least one or two separate data sources, depending on the type of information needing to be verified.

(e) If the above CDD procedure has been carried out but the person carrying out the procedure cannot be reasonably satisfied that the client is the individual/entity he or she claims to be (and the person is unable to conduct a further client identification procedure to address this doubt), then the financial adviser should not arrange for the provision of the financial service or product .

(f) In addition, the financial adviser will need to consider whether this gives rise to a 'suspicious matter' which would require reporting to AUSTRAC.

3.5 Beneficial ownership

(a) A beneficial owner of a client is defined as an individual (a natural person or persons) who ultimately owns or controls (directly or indirectly) the client. This may be the case where your client is a company that is a corporate trustee of a trust.

(b) Ownership for the purposes of determining a beneficial owner means owning 25 per cent or more of the client.

(c) The definition of 'control' includes whether the control is exerted by means of trusts, agreements, arrangements, understandings or practices and whether or not the individual has control based on legal or equitable rights. It includes where an individual can exercise control through making decisions about financial and operating policies.

(d) To identify the beneficial owner of a client, the financial adviser should establish and understand the ownership or control structure of the client. In most cases, the financial adviser should request information from the client. Examples of information that may assist a reporting entity in identifying a beneficial owner of a client include:

(i) a certificate of incorporation of a company with ASIC and/or an annual statement including the amendments submitted to ASIC

(ii) a trust deed

(iii) a partnership agreement

(iv) the constitution and/or certificate of incorporation for an incorporated association

(v) the constitution of a registered co-operative.

(e) Once a financial adviser has established who is a beneficial owner or owners of a client, they must collect at least the following information in relation to each individual beneficial owner:

(i) full name; and

(ii) date of birth or full residential address.

4 Politically Exposed Persons (PEPs)

4.1 Who are politically exposed persons (PEPs)?

(a) PEPs are individuals who occupy a prominent public position or function in a government body or international organisation, both within and outside Australia. This definition also extends to their immediate family members and close associates.

(b) There are 3 categories of PEPs:

(i) Domestic PEPs are individuals who hold a prominent public position or function in an Australian government body;

(ii) Foreign PEPs are individuals who hold a prominent public position or function in a government body of a foreign country;

(iii) International organisation PEPs are individuals who hold a prominent public position or function in an international organisation.

(c) Due to their position and influence, many PEPs are in positions that potentially can be abused for money laundering and related predicated offences, including corruption and bribery, as well as activity related to terrorism financing.

(d) A person's status as a PEP would cease when that person no longer holds the position that qualifies them as a PEP. However, you should continue to apply a risk-based approach to determine whether an existing client who is no longer a PEP should continue to be treated as a high-risk client. For example, if a person no longer holds a 'high risk' position but maintains close ties with their political network, you may need to continue to be alert to the client's activities.

4.2 Risks associated with PEPs

(a) A financial planner must automatically treat all foreign PEPs as high-risk clients.

(b) On some occasions, Domestic PEPs and 'international organisation' PEPs may also be considered to be high risk depending on the circumstances. You will need to conduct a risk assessment on domestic and international organisation PEPs before deciding whether to apply the enhanced customer due diligence requirements to these clients (see 4.4(b)).

(c) Not all PEPs present the same AML/CTF risk. If a PEP undertakes transactions of the type that would normally be undertaken by non-PEP clients, and there is no evidence to suggest the funds came from an unusual source, the normal procedures may be

sufficient to mitigate the money laundering/terrorism financing (**ML/TF**) risk (eg. simply asking the client general questions about the transaction and documenting the responses as normal).

(d) In some circumstances financial advisers should consider obtaining further information from a PEP and seek more documentary evidence to verify the information provided.

4.3 What to do when a PEP may become a client?

(a) The Licensee is required to have:

(i) procedures to identify whether any individual client or beneficial owner is a PEP, or an associate of a PEP (See ID Forms). The Licensee requires the financial adviser to undertake this identification process before they provide the client with the financial service, or as soon as practicable afterwards.

(ii) risk-based procedures to determine whether a client is a PEP. These procedures may include:

(A) checking the client's background through an internet search;

(B) consulting reports and databases released by various organisations that specialise in analysing corruption risks;

(C) subscribe to a specialist PEP database, if more thorough checks need to be conducted.

(b) Generally, domestic or international organisation PEPs may be considered to be of lower ML/TF risk, but this cannot be assumed – the financial adviser needs to carry out their risk-based procedures to decide whether a PEP is of higher ML/TF risk. For domestic PEPs or international organisation PEPs that are beneficial owners of a client, a financial adviser must carry out the client identification and verification procedures which apply to individuals.

4.4 Foreign PEPs and high risk domestic or international organisation PEPs

(a) For foreign PEPs or high ML/TF risk domestic PEPs who are beneficial owners, the Licensee must carry out the client identification and verification procedures which apply to individuals. The Licensee (or the financial adviser) is also required to:

(i) obtain senior management approval before establishing or continuing a business relationship with the client and before providing, or continuing to provide, a designated service to the client;

(ii) take reasonable measures to establish the client's source of wealth and source of funds;

(iii) comply with enhanced client due diligence requirements.

(b) The enhanced CDD requirements include:

(i) seeking additional information from the client (or from third party sources) in order to:

(A) clarify or update the “know your client information” already collected from the client;

(B) clarify or update beneficial owner information already collected from the client in regards to the beneficial owners of the client;

(C) obtain any further know your client information or beneficial owner information, including, where appropriate, taking reasonable measures to identify and verify:

(1) the source of the client's and each beneficial owner's wealth; and
(2) the source of the client's and each beneficial owner's funds;
(3) the nature of the client's ongoing business with the reporting entity;

(ii) undertake more detailed analysis of the client's information and beneficial owner information, including, where appropriate, taking reasonable measures to identify:

(A) the source of the client's and each beneficial owner's wealth; and

(B) the source of the client's and each beneficial owner's funds;

(c) For all foreign PEPs and high risk domestic or international organisation PEPs, financial advisers should closely scrutinise the investment transactions conducted by that client.

5 Risk based assessment

5.1 Risk based assessment

The Licensee is required to have a risk-based CDD procedure and have regard to the considerations set out below:

(a) client types, including beneficial owners of customers and PEPs

(b) client' sources of funds and wealth (for example, by enquiring into the expected source and origin of the funds to be used in the provision of the designated service)

(c) nature and purpose of the business relationship (for example, the client's business or employment)

(d) control structure of non-individual clients (for example, complex corporate structures and the underlying beneficial owners)

(e) types of designated services the reporting entity provides

(f) how the Licensee (or the financial adviser) provides its designated services (for example, over-the-counter or online)

(g) foreign jurisdictions in which the Licensee (or the financial adviser) deals (for example, clients that live or are incorporated in a foreign country).

5.2 Assessment: Low Risk

In general, the Licensee considers that its client base is likely to be 'low risk' for the following reasons:

(a) the client base generally comprises of retail investors who require financial advice in relation to investments, superannuation and insurance.

(b) the source of funds from these clients are mainly derived from salary, inheritance, domestic investments, and funds in superannuation.

(c) other than corporate trustees of family trusts and self-managed superannuation funds, the clients in general are individuals who are Australian residents (i.e. no beneficial ownership for individuals).

(d) financial services are delivered in person to the individual.

(e) financial services are generally only provided after representatives have conducted a thorough investigation into the client's circumstances as part of meeting the best interest's duty requirements under the Corporations Act.

(f) financial products are generally issued by companies regulated under Australian laws.

(g) In general, financial products are acquired in the client's own name or in the name of a self-managed superannuation fund in which the client is the trustee and beneficiary or the name of the family trust/corporate trustee of the family trust having confirmed who the beneficial owners are.

6 Record keeping

6.1 Record keeping

The Licensee requires the financial adviser to retain the relevant ID Form and documents used to verify the client for a minimum of seven years after the relationship with the client ends.

7 Cyber enabled fraud

7.1 Background

(a) Financial advisers are particularly vulnerable to cyber-enabled fraud attacks when acting as a gateway between clients and financial institutions or product issuers. There are instances in which a third party hacked a client's email and used it to instruct the financial adviser to make a withdrawal or transfer of funds, often into intermediary, or 'mule' bank accounts. The purpose of mule bank accounts is to allow the hacker to temporarily store the funds which have been acquired illegally until it is transferred.

(b) There were also cases in which a financial adviser's email was hacked and used to email the product issuer to request a funds transfer, purportedly at the request of the client.

(c) Cyber enabled fraud is the most frequently reported suspected crime type in the financial planning sector (51 per cent as reported by AUSTRAC in 2016). The risks of cyber enabled fraud in the financial planning industry has been rated as 'medium' by AUSTRAC.

7.2 Examples of cyber enabled fraud

Some examples of cyber enabled fraud include the following:

(a) diverting a client's phone number, in an attempt to circumvent call-back controls;

(b) accessing a client's email history (including attachments, drafts and sent items) to more accurately impersonate the client (for example, by referencing personal situations such as home renovations);

(c) using social media (either by hacking the account or relying on publicly available information) to gather information about the client; and

(d) creating a new email account using the client's name in order to impersonate the client.

7.3 Key indicators of cyber enabled fraud

AUSTRAC described some key indicators of cyber-enabled fraud as including:

(a) client's email has different tone/language to customer's usual communications;

(b) client's email has poor grammar, spelling mistakes or uncommon terminology;

(c) client usually contacts the financial adviser by telephone, then suddenly makes contact by email;

(d) client changes bank details soon after changing other details such as contact address or phone number;

(e) client emails express urgency – for example, claiming the client is travelling overseas, attending a funeral, or purchasing a property requests for the financial adviser to transfer funds to an account or complete application forms on the client's behalf, then to send back to the client for signing;

(f) client email requests to send funds overseas – for example, claiming the client is distressed and has become stranded overseas with their bank cards stolen.

7.4 What to do when you suspect you have encountered a cyber fraud

If the Licensee or a financial adviser authorised by the Licensee suspects that cyber fraud is being carried out, the Licensee expects the financial adviser to do the following:

(a) Verify the transaction with the instructing client personally over the telephone. Do not verify over email (as email may have been hacked).

(b) Do not execute any transactions until the instruction has been verified personally with the client over the phone - irrespective of the urgency that has been placed on the transaction.

(c) If the client confirms the instruction, file note the discussion with the client and execute the transaction.

(d) If the client denies the instruction, warn the client their details may have been subject to potential cyber fraud;

(e) Lodge a suspicious matter report with AUSTRAC via your AUSTRAC Portal.

8 Suspicious matter reporting

8.1 Obligation to report

(a) As a reporting entity, the Licensee must submit a suspicious matter report (SMR) if they form a reasonable suspicion of money laundering, terrorism financing or other offences such as fraud or tax evasion, operating under a false identity, or of a matter relating to the proceeds of crime.

(b) Examples of suspicious matters may include:

(i) The client is not who they claim to be;

(ii) The client is not forthcoming about, or there are inconsistencies with, the client's source of funds;

(iii) Short period of time between investing the funds and withdrawing the funds;

(iv) Significant funds appearing in the client's account;

(v) Overseas transactions are frequent without plausible explanation;

(vi) The funds are inconsistent with the client's income;

(vii) The client becomes angry or refuses to provide information or the information they provide is inconsistent;

(viii) The client wants to minimise paperwork;

(ix) The client expresses preference to transact in cash.

8.2 What information must be reported in a suspicious matter report?

When lodging a suspicious matter report, the Licensee must provide details about their business and all details known about:

(a) the suspicious matter

(b) the person/organisation(s) to which the matter relates

(c) any transactions related to the matter.

8.3 What are the timeframes for reporting a suspicious matter?

(a) As a reporting entity, the Licensee must submit an SMR to AUSTRAC within 24 hours after forming the relevant suspicion if the suspicion relates to terrorism financing or three business days after forming the suspicion in all other cases.

(b) The time period for reporting a suspicious matter starts when the Licensee forms a 'suspicion on reasonable grounds'. This may occur at any time during the enquiry, request, proposal, or commencement stages of providing a designated service to the client.

8.4 Tipping off

(a) The Licensee must not disclose to any person (other than AUSTRAC) that it formed a suspicion about a client or that it submitted an SMR to AUSTRAC. Doing so would constitute 'tipping off', which is an offence under the AML/CTF Act.

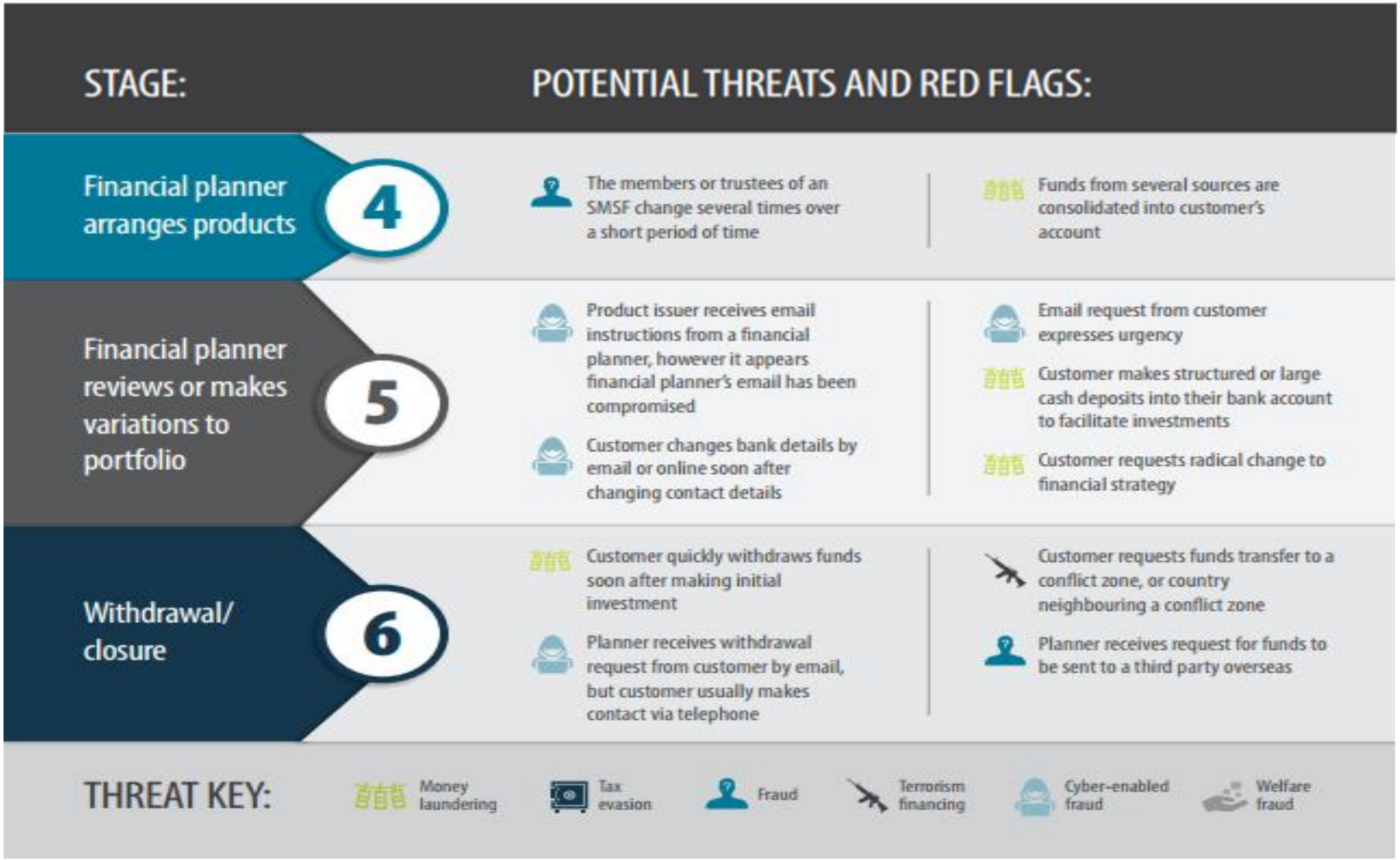
(b) The Licensee must not disclose any information that might reasonably lead a person to conclude that the Licensee formed a suspicion about a client, or that the Licensee communicated that suspicion to AUSTRAC.

(c) In addition, the Licensee must not disclose any requests from AUSTRAC for further information about a SMR report.

8.5 Examples

Examples of suspicious matters are set out below.


STAGE:
POTENTIAL THREATS AND RED FLAGS:
Client/planner relationship established
1
Customer enquires whether planner accepts large cash deposits
Customer requests advice on overly complex company/trust structures that go beyond their financial needs
Customer is reluctant to provide identification or behaves nervously
Customer requests advice on how to evade tax
Client information is collected, analysed and evaluated
2
Customer documents inconsistent with expected formats, appear altered or have inconsistencies (e.g. date of birth)
Customer has unexplained wealth inconsistent with economic situation
Customer requests unusual/ uneconomic investments
Customer uses company/trust structures with unclear beneficial owners
Customer reveals they are misleading Centrelink for welfare benefits
Customer has suspicious property ownership arrangements
Customer has money in, or corporate entities based in, tax havens
Customer's name appears on a terrorism watch list
Financial planner provides advice
3
Customer asks how to make an insurance claim before an insurable event takes place
Customer receives advice but chooses to implement the advice without the planner
Customer asks to establish an SMSF without being able to show source of funds/ownership for the initial transfer


STAGE:
POTENTIAL THREATS AND RED FLAGS:
Financial planner arranges products
4
The members or trustees of an SMSF change several times over a short period of time
Funds from several sources are consolidated into customer's account
Financial planner reviews or makes variations to portfolio
5
Product issuer receives email instructions from a financial planner, however it appears financial planner's email has been compromised
Customer changes bank details by email or online soon after changing contact details
Email request from customer expresses urgency
Customer makes structured or large cash deposits into their bank account to facilitate investments
Customer requests radical change to financial strategy
Withdrawal/ closure
6
Customer quickly withdraws funds soon after making initial investment
Planner receives withdrawal request from customer by email, but customer usually makes contact via telephone
Customer requests funds transfer to a conflict zone, or country neighbouring a conflict zone
Planner receives request for funds to be sent to a third party overseas
THREAT KEY:
Money laundering
Tax evasion
Fraud
Terrorism financing
Cyber-enabled fraud
Welfare fraud