

Strategic analysis brief

Use of business express deposit boxes to avoid reporting requirements



Australian Government

AUSTRAC



Strategic analysis briefs

AUSTRAC strategic analysis briefs provide insights for government and industry on money laundering and terrorism financing (ML/TF) risks, trends and methods.

These briefs aim to assist Australian businesses by providing information that may be helpful in identifying and mitigating the risk of their business being misused by criminals. This information can

- » be relevant to their AML/CTF programs, policies and procedures
- » help to inform their management and mitigation of ML/TF risk
- » enhance the quality of reporting to AUSTRAC.



This work is licensed under a Creative Commons Attribution 4.0 International License.

Attribution: Material obtained from this document is to be attributed to: © AUSTRAC for the Commonwealth of Australia 2015.

CONTENTS

Purpose	2
Source	2
Key points	2
Money laundering method	3
Business express deposit boxes and AML/CTF regulation	4
Indicators	4
Suspicious matter reporting	5
Where can I get more information?	5

PURPOSE

To inform reporting entities about the use of business express deposit (BED) boxes and internet banking facilities by serious organised crime groups (SOCGs) to avoid know your customer and ongoing customer due diligence requirements.

SOURCE

The information in this typologies brief has been drawn primarily from information provided by the Australian Crime Commission. The brief also contains information sourced from AUSTRAC and some financial institutions.

KEY POINTS

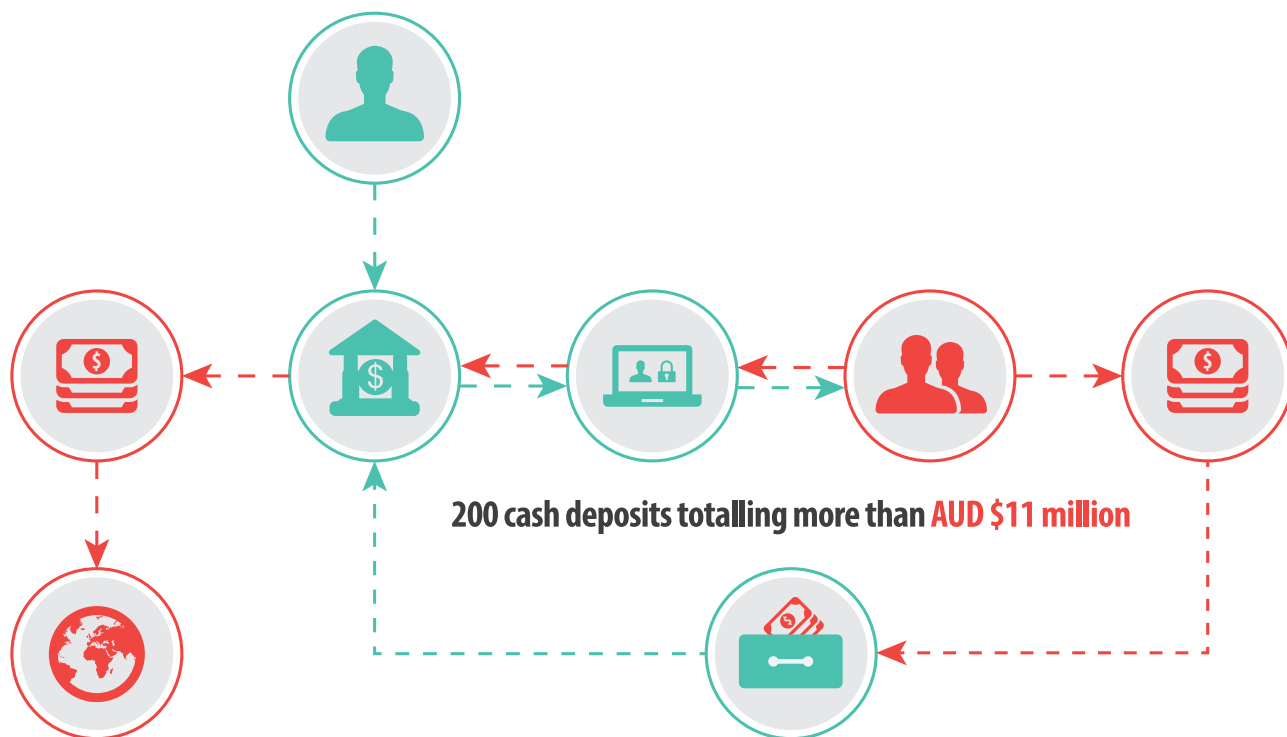
- » SOCGs are using BED boxes to circumvent the AML/CTF compliance programs of banks.
- » SOCGs are using third parties with little or no criminal history, such as foreign students, to incorporate companies and open bank accounts with internet banking facilities.
- » Illicit funds are deposited into the bank accounts by making bulk cash deposits through BED boxes, meaning that the individuals depositing the funds are not being identified.
- » The SOCG, rather than the account holder, sends the funds offshore using internet banking.
- » Banks have reported the activity in suspicious matter reports (SMRs).

MONEY LAUNDERING METHOD

The following method involving BED boxes is being used by a SOCG:

1. Company accounts are established by foreign nationals, typically individuals aged in their late twenties to early thirties, on student visas.
2. Once the account has been established, the foreign national provides the internet banking details (username and password) to the SOCG.
3. SOCG members use BED boxes to make bulk cash deposits of illicit funds into the company accounts.
4. Over a 10-month period, the SOCG members made over 200 cash deposits totalling more than AUD11 million.
5. Numerous cash deposits were made each day at multiple bank branches, typically in values ranging between AUD40,000 to AUD60,000.
6. Conducting deposits in this manner means the identification details of the individual making the deposit are not reported to AUSTRAC.
7. The majority of deposits occurred in Western Australia, whereas the accounts are held in New South Wales.
8. The funds are pooled, either in the depositing account or a third-party account.
9. The SOCG then moves the deposited funds in large values (i.e. AUD100,000) to an offshore account using internet banking.
10. The foreign nationals are not responsible for conducting any of the financial transaction activity.

Banks have submitted suspicious matters reports regarding this activity to AUSTRAC.



BUSINESS EXPRESS DEPOSIT BOXES AND AML/CTF REGULATION

Under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), all entities which provide certain 'designated services' are 'reporting entities' under the Act and therefore subject to regulation by AUSTRAC. The AML/CTF Act requires reporting entities to submit, among other things, threshold transaction reports (TTRs) and SMRs.

Under section 43 of the AML/CTF Act, if a reporting entity provides a designated service to a customer and that service involves a threshold transaction (that is, a transaction of physical currency or e-currency of AUD10,000 or more), then the reporting entity must submit a TTR to AUSTRAC.

Reporting requirements for TTRs were strengthened on 1 October 2011 to require reporting entities to include details of the individual conducting a threshold transaction where that individual is not the customer of the designated service. This additional TTR reporting requirement means that reporting entities must report details of any third parties depositing currency of AUD10,000 or more into an account, a requirement that assists AUSTRAC to identify the use of third parties to launder illicit cash.¹

However subparagraph 19.3 (17)(a)(i) of the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* (AML/CTF Rules) allows for an exemption for reporting entities in gathering 'agent' details when 'the transaction involves a deposit service carried out in non-face-to-face circumstances by the individual'.² In these instances the reporting entity is only required to report the customer details in the Threshold Transaction Report and not those of the third party making the non-face to face deposit, as stated in 19.3 (17)(b).

INDICATORS

The following indicators highlight potentially suspicious customer behaviour associated with BED boxes. In isolation, the indicators are not necessarily synonymous with money laundering or other illicit activities. However the appearance of multiple indicators may be indicative of laundering the proceeds of crime.

- » Accounts opened in company names with foreign nationals on student visas as signatories.
- » Business receiving very large volumes of cash compared to businesses of a similar type, size or location
- » Frequent bulk cash deposits using BED boxes followed by multiple international funds transfers.
- » Identities of individuals making cash deposits are not established.
- » Account activity inconsistent with customer profile.
- » The customer does not have a legitimate business reason to use BED boxes.
- » Numerous deposits occurring each day at a number of different bank branches.
- » Deposits occurring in a different state to where the accounts are held.
- » There is no building located at the business or residential address provided by the customer (for example, as checked on Google Maps).
- » International funds transfers from business account are not related to the actual payment of goods or services for the business.

1 Further information on threshold transaction reporting is available on the AUSTRAC website: <www.austrac.gov.au/threshold-transaction-reports-ttrs>

2 The AML/CTF Rules can be viewed on the Comlaw website <www.comlaw.gov.au/Series/F2007L01000>.

SUSPICIOUS MATTER REPORTING

Reporting entities, including financial institutions, must submit SMRs to AUSTRAC detailing any financial activity which they consider to be suspicious.³ Presented above is a non-exhaustive list of possible indicators which may help identify potential money laundering and other serious and organised criminal activity.

AUSTRAC assesses and disseminates relevant SMRs to law enforcement agencies and other authorities for their consideration. AUSTRAC also assists reporting entities to detect and deter money laundering by increasing their understanding of the vulnerabilities within their industry. By strengthening internal AML/CTF controls and programs, reporting entities can better undertake enhanced and ongoing customer due diligence, and develop policies and strategies to protect their services from being misused by criminals.

WHERE CAN I GET MORE INFO?

Please contact the AUSTRAC Contact Centre:

- » Telephone: 1300 021 037
- » Email: help_desk@austrac.gov.au

Information is also available on the AUSTRAC website at www.austrac.gov.au.

³ If a reporting entity forms a suspicion at any time while dealing with a customer (from the enquiry stage to the actual provision of a designated service or later) on a matter that may be related to an offence, tax evasion, or proceeds of crime, they must submit an SMR to AUSTRAC. Offences include money laundering, terrorism financing, operating under a false identity or any other offence under a Commonwealth, state or territory law < <http://www.austrac.gov.au/suspicious-matter-reports-smrs>>.

www.austrac.gov.au

