

Current and emerging threats

Criminals are adept at identifying vulnerabilities in financial products or sectors, and exploiting these vulnerabilities to facilitate financial crime and launder the proceeds of their illicit activities. In compiling this report, AUSTRAC reviewed both public and restricted material to identify current and emerging threats posed by financial crime and money laundering activities.

Criminals continue to misuse the legitimate financial system to perpetrate crimes such as card skimming, online scams, ponzi and illegal superannuation schemes. In addition, emerging, or in some cases re-emerging, criminal threats include trade-based money laundering, bulk cash smuggling, and the misuse of new payment methods, including prepaid debit cards and mobile payment services.

Trade-based money laundering

In order to transfer a large volume of money across international borders and integrate it into the formal economy, some criminals employ a method known as trade-based money laundering. This process involves disguising and moving the proceeds of crime using trade transactions in an attempt to legitimise the source of the funds. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports.

Trade-based money laundering has continued to evolve, and common methods include:

- over and under-invoicing of goods and services – misrepresentation of the price of the goods and/or services in order to transfer additional value between the importer and exporter
- over and under-shipment of goods and services – overstating or understating the quantity of goods being shipped or services provided. In some cases, no goods are shipped
- multiple invoicing of goods and services – issuing more than one invoice for the same trade transaction
- falsely describing goods and services – misrepresenting the quality or type of goods and services.

There are a number of general indicators that may prompt a suspicion that trade-based money laundering is being perpetrated. Financial institutions may notice irregular account activity among their clients: the client may have received significant amounts of money within a relatively short period of time, or been involved in large international funds transfers to or from an overseas company located in a country of interest to authorities (for example, a known tax haven country).



Bulk cash smuggling

Criminals continue to rely upon bulk cash smuggling to move the proceeds of illicit activity across international borders. Recent information from various Australian law enforcement agencies indicates that criminals have attempted to smuggle significant amounts of money out of the country to avoid cross-border reporting requirements. In addition, a number of recent cases have identified criminals stockpiling large amounts of cash, possibly in preparation for bulk cash smuggling operations.

For example, a recent investigation uncovered AUD3 million cash hidden in 13 suitcases at Sydney airport and a further AUD5 million was found in a storage facility. The money was allegedly destined for the Middle East².

In another case, a person was found to have AUD1.5 million cash stashed in cardboard boxes inside the boot of his Mercedes-Benz. A search of his home uncovered a further AUD250,000 cash³. In a third case, police seized AUD3 million cash hidden in the roof of a house⁴.

Mules and third parties

To avoid direct involvement in the money laundering process, criminals may use 'mules' (people unrelated to the initial criminal activity, who are used to unwittingly transfer funds to criminals overseas) or complicit third parties who have no criminal record to carry out the laundering on their behalf. In some instances, these people may be known to the criminal; for example, they may be family members or associates. Criminals may also recruit other parties such as unemployed persons or students looking for work to assist in their illegal activities.

The mules or third parties may be given instructions to:

- deposit funds into their own account and then transfer the funds to another entity
- deposit funds into another entity's account
- undertake international funds transfers to other entities.

The inclusion of third party or agent details in transaction reports assists law enforcement officers to identify criminal associations and follow the trail of illicit proceeds. Depending on the circumstances, reporting entities may also consider the involvement of a third party in a transaction as suspicious, and therefore the submission of an SMR to AUSTRAC is also warranted.

2 'Terror cash claims', *The Sunday Telegraph*, 2 August 2009, p.7.

3 'A Sydney driver, a flash car and the \$1.5m found in a Mercedes Benz in Cabramatta', *The Daily Telegraph*, 20 November 2009.

4 'Police seize millions in roof', *The Sydney Morning Herald*, 30 April 2009.

New payment methods

The use of new payment methods and 'e-money' has also emerged as a money laundering vulnerability.

Prepaid debit/credit card

Prepaid cards permit users to load money onto a card prior to its use. There are a wide variety of prepaid cards which can be used in many different ways; some allow limited use while others offer multiple uses. Some prepaid cards can be linked to an individual account, while others can be linked to a collective account. In addition, cards can be issued by financial institutions or non-traditional banking institutions.

Prepaid cards are particularly vulnerable to misuse for the purposes of money laundering. Customers purchasing multiple prepaid cards which can be accessed overseas and customers reloading significant amounts of cash onto cards are potential indicators of illicit activity to which institutions should be alert.

Online money transmitters

Online money transmitters are also gaining wide use. E-currencies (such as e-gold) offer an electronic means of exchange which is backed by precious metals or bullion, and which can be converted into a globally accepted currency⁵.

Web-based operators who offer financial services across borders and do not authenticate the identities of their customers before transactions are conducted are particularly at risk of being misused for money laundering.

Mobile payment services

Mobile payment services offer a new mechanism for the transfer of funds. For example, mobile devices can be used to access bank accounts and conduct transactions. Similarly, where mobile payment services are not linked to bank accounts, the mobile service provider can act as a payment intermediary⁶. Mobile payment options can potentially be misused for money laundering and the financing of terrorism, or used as a cash substitute for other forms of criminal activity; for example, drug sales. Several features of mobile payment services render them particularly vulnerable to exploitation by money launderers:

- funds can be transferred or withdrawn anywhere, anytime
- funds can be transferred or withdrawn anonymously due to the difficulty in identifying those undertaking mobile payments carried out using prepaid mobile accounts
- multiple accounts can be used to facilitate the structuring of multiple transfers. By employing several different SIM cards, users can use multiple mobile payment accounts to structure these transfers
- funds can be transferred in small values, so the transfers will appear random, inconsequential and unrelated to criminal activity
- funds (for example, charitable donations) can be transferred, knowingly or unknowingly, to criminal groups or terrorist organisations through apparently legitimate charities.

Appendix B of this report lists a number of other publications developed by Australian and international organisations that provide more information about money laundering and terrorism financing typologies.

⁵ See Glossary for an explanation of **e-currencies**.

⁶ Financial Action Task Force, 2006, *Report on New Payment Methods*, <www.fatf-gafi.org>