You must make sure your transaction monitoring systems alert you to unusual, large or complex transactions or patterns of transactions. What defines a transaction as large or unusual will depend on the size of your business or organisation and the services you offer. It also depends on the types of customers and transaction activities you normally deal with. Indicators of criminal activity There are many customer transactions that may indicate your business or organisation is being exploited for money laundering, terrorism financing or other serious crime. Examples of these indicators include: gambling proceeds being deposited into foreign bank accounts buying casino chips and cashing them out with no gaming activity associations having multiple accounts under multiple names transactions that donâ€™t match the customer profile high volumes of transactions being made in a short period of time depositing large amounts of cash into company accounts depositing multiple cheques into one bank account purchasing expensive assets, such as property, cars, precious stones and metals, jewellery and bullion using third parties to make wire transfers using an accountant or lawyer to make transactions using cash to buy large amounts of gold regularly selling large amounts of jewellery, gold or precious metals storing large amounts of cash in a safety deposit box cashing bank drafts for foreign currency exchanging large amounts of currency for travellerâ€™s cheques withdrawing large amounts of cash making multiple transactions on the same day from different locations using false or stolen identities to open bank accounts repaying loan balances early or in cash describing frequent transfers of funds as loans from relatives moving funds through different accounts closing insurance policies and requesting payment to a third party sending investment funds to high-risk countries reducing (structuring) the amount of cash deposits or withdrawals to avoid triggeringÂ transaction reporting rules. Read ourÂ case studiesÂ for more examples of indicators of criminal activity that businesses have recognised and reported to AUSTRAC. If you are suspicious about a transaction If your monitoring program identifies suspicious customer transactions or behaviour, you must apply your enhanced customer due diligence and submit aÂ suspicious matter report (SMR)Â to AUSTRAC. Identifying a higher ML/TF risk does not necessarily mean that a customer relationship must be terminated, but if you decide to terminate a customer relationship,Â continue to apply ECDD and OCDD until the termination takes effect. You can consider placing restrictions on the account to prevent further transactions. You should continue to monitor for new accounts that could be related to the closed accounts.