Australian Government
AUSTRAC

Proposed updated guidance on reporting multiple cash transactions - threshold transaction reporting (TTR) obligations

Page title	Reporting transactions of $10,000 and over: Threshold transaction reports (TTRs) Reporting multiple cash transactions
URL	https://www.austrac.gov.au/business/how-comply-guidance-and-resources/reporting/cash-transactions-over-10000-ttr

Reporting multiple cash transactions

When your customer makes multiple cash transactions, each individual transaction is considered to be a separate and distinct designated service. You don't need to combine the transactions and submit a TTR, even if the transactions occurred closely together. You must submit a TTR to AUSTRAC for each individual cash transaction of A$10,000 or more.

If you suspect your customer is structuring their transactions to avoid the TTR reporting threshold you must submit a suspicious matter report (SMR) to AUSTRAC.

Structuring

Customers may deliberately split a larger cash transaction into several smaller transactions to try to avoid a TTR being submitted. This is called structuring, a common money laundering technique used to launder illicit funds. Structuring transactions to avoid reporting is a criminal offence.

You must consider whether your customer has a reasonable explanation for conducting multiple transactions, or whether this activity is suspicious. If you reasonably suspect that transactions have been structured to try and prevent them from being reported in a TTR, you must submit an SMR to AUSTRAC.

Your transaction monitoring program must be able to detect possible structuring of cash transactions and include triggers for further investigation and reporting to AUSTRAC if required.

Examples

We have provided examples of when a TTR is required on this page. In each of the examples you must also consider if there are reasonable grounds for suspicion. If you believe the transactions could be linked to criminal activity, or that a customer is attempting to structure their transactions to avoid being reported, you must submit an SMR to AUSTRAC.

See also Structuring for more information and examples of structuring transactions.

Example 1: Splitting a transaction into two accounts – TTR not required

Jane holds several accounts with Bank A. She visits the bank with $14,000 in cash and asks to deposit $8,000 into one account and $6,000 into another account.

Each deposit is considered to be a separate designated service. Bank A does not need to submit a TTR for either deposit as neither of the deposits meets the $10,000 threshold.

Example 2: Splitting a transaction into two accounts – TTR required

Brian holds several accounts with Bank B. He visits the bank with $14,000 in cash and asks to deposit $11,000 into one account, and $3,000 into another account.

Bank B has provided two separate designated services to Brian. As the first transaction exceeds the $10,000 threshold, Bank B has an obligation to submit a TTR to AUSTRAC for that transaction.

The obligation to provide a TTR does not apply to the second transaction of $3,000, as this transaction does not meet the $10,000 threshold.

Example 3: Splitting transaction into two accounts – TTR required

Wei holds two accounts with Bank C. He visits the bank with $27,000 in cash and deposits $15,000 into his first account and $12,000 into his second account.

Bank C has provided two separate designated services to the customer. Both transaction amounts exceed the $10,000 threshold. Bank C has an obligation to submit two TTRs to AUSTRAC – one for the $15,000 transaction and one for the $12,000 transaction.

Example 4: Transaction limits – splitting transactions into the same account

On Monday, Pam visits a branch of Bank D to deposit $12,000 in cash into an account she holds. Pam says she operates a small business and would like to split the deposit into three transactions to align with her business turnover for Friday, Saturday and Sunday. Pam explains that this will make the reconciliation process with her accounting software easier and more accurate.

Pam deposits the following amounts of cash into her account:

1. 1.00pm: Friday's turnover: $4,500.
2. 1.04pm: Saturday's turnover: $4,500.
3. 1.09pm: Sunday's turnover: $3,000.

Although these transactions were conducted closely together, there is no obligation to submit a TTR because each deposit represents a separate designated service and none of the deposits involve a threshold transaction.

Example 5: Transaction limits – splitting transactions into the same account through an ATM

Scarlett attends an ATM of Bank E to deposit $15,000 in cash into an account she holds with the bank. Bank E has a cash deposit limit on its ATMs of $5,000.

Scarlett deposits the following amounts of cash into her account:

1. 1.00pm: $5,000
2. 1.05pm: $5,000
3. 1.10pm: $5,000.

Although these transactions were conducted closely together, there is no obligation to submit a TTR because each deposit represents a separate designated service and none of the deposits involve a threshold transaction.

Example 6: Transaction limits – splitting transaction into the same account

Leo visits a post office to deposit $11,000 in cash into his account with Bank F. The post office acts as an agent for Entity F and applies a cash deposit limit of $7,000. Due to the limit, Leo deposits the following amounts of cash into his account:

1. 1.00pm: $7,000
2. 1.05pm: $4,000.

Although these transactions were conducted closely together, there is no obligation to submit a TTR because each deposit represents a separate designated service and none of the deposits involve a threshold transaction.

Example 7: Purchase of a bank cheque

Vijay visits a branch of Bank G to purchase a bank cheque for $10,000 and make a deposit of $5,000 into an account he holds with the bank. Vijay also pays a $10 fee for the bank cheque.

To complete the deposit and purchase of the cheque, Vijay hands over a total of $15,010 in cash to the teller.

Bank G is required to submit a TTR. Two designated services are provided by Bank G – the $5,000 deposit and the purchase of the $10,000 cheque. Bank G has an obligation to submit a TTR for the purchase of the $10,000 cheque.

Under Chapter 19 of the AML/CTF Rules the bank is required to include additional information in the TTR about the bank cheque including the physical currency used to purchase it.

Example 8: Purchase of two or more foreign currencies

Sophia attends a currency exchange business to purchase foreign currency ahead of an overseas holiday. Sophia uses Australian cash to make the following foreign exchange transactions:

1. Purchase A$7,000 worth of Euros.
2. Purchase A$7,000 worth of Pounds Sterling.

There is no obligation to submit a TTR because each currency exchange is a separate designated service, even though they were conducted within a short timeframe. Neither of the exchanges involve a threshold transaction.

Example 9: Purchase of gaming chips – TTR not required

Allan attends Casino H and exchanges $7,000 in cash for gaming chips at the casino cage. He then goes to a blackjack table and purchases another $5,000 in gaming chips using cash.

There is no obligation to submit a TTR because each purchase of the gaming chips is a separate designated service, despite the short timeframe between transactions. Neither of the transactions involve a threshold transaction.

Example 10: Sending money overseas – TTR required

Margaret goes to a remittance service provider to send money to her family and contribute to the development of a community centre in a foreign country. Using physical cash totalling $12,000, she sends $2,000 to her family in one transaction and sends $10,000 for the development of the community centre in a second transaction.

The remittance service provider has provided two designated services to Margaret.

No TTR is required for the first transaction of $2,000, as this transaction does not meet the $10,000 threshold. There is an obligation to submit a TTR for the second transaction because it meets the threshold of $10,000 or more in physical cash.

Related pages

- Transaction monitoring
- Suspicious matter reports (SMRs)

Related legislation

- Sections 41 and 43 of the AML/CTF Act
- Chapter 19 of the AML/CTF Rules

Proposed updated web content on structuring

Page title	Reporting transactions of $10,000 and over: Threshold transaction reports (TTRs)
URL	https://www.austrac.gov.au/business/how-comply-guidance-and-resources/reporting/cash-transactions-over-10000-ttr#accordion-360

Structuring

Structuring is a money laundering technique which involves transactions being deliberately split into smaller amounts to avoid threshold transaction reporting.

Structuring is a criminal offence. If you suspect that a customer is structuring or attempting to structure their transactions to avoid reporting, you must submit a suspicious matter report (SMR) to AUSTRAC. An SMR is only reportable in circumstances where you reasonably believe that the 'sole or dominant purpose' of splitting of the transactions is to avoid reporting requirements.

Examples

Example 1: Multiple bank deposits – SMR required

Cerise visits Cedar Bank and deposits $4000 cash into her account. Later that day she returns to the bank and deposits a further $7,000 cash. The next day, she returns to Cedar Bank and purchases a bank cheque with $6500 cash and deposits another $9000 cash into her account. A review of Cerise's previous transactions and her known sources of income reveals that it is derived primarily from social security payments. Cedar Bank applies enhanced customer due diligence measures that involves collecting additional information and undertaking additional verification.

Cedar Bank suspects Cerise is structuring her transactions to avoid the TTR requirements, so submits an SMR to AUSTRAC.

Example 2: Casino gaming – SMR required

Ivan attends the Universal Casino where he is a loyalty club member, and uses cash to purchase $8,000 in gaming chips at the casino cage. He then goes to a blackjack table and exchanges another $8,000 cash for gaming chips.

After a short period of playing blackjack, his total balance of gaming chips has increased to $17,500. Ivan decides to redeem a portion of these chips. He cashes in $8,500 of gaming chips at the table and then proceeds to the casino cage where he cashes the remaining $9,000 of his gaming chips.

Universal Casino's transaction monitoring program identifies a change in Ivan's gambling activity. A closer review of Ivan's gambling activity indicates that he has engaged in structuring. Universal Casino submits an SMR to AUSTRAC with the relevant description of Ivan's behaviour and their grounds for suspicion.

Related legislation

- Sections 41 and 142 of the AML/CTF Act

Proposed updated web content on transaction monitoring

Page title	Transaction monitoring
URL	https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/amlctf-programs/transaction-monitoring

Transaction monitoring

Your business must have an appropriate risk-based transaction monitoring program in place to help your employees identify suspicious behaviours and transactions and to take steps to protect your business and customers.

A transaction monitoring program helps your business to:

- Identify, mitigate and manage money laundering and terrorism financing (ML/TF) risks.
- Identify and report suspicious matters to AUSTRAC.
- meet your ongoing customer due diligence (OCDD) and enhanced customer due diligence (ECDD) obligations. Read more about your obligation to have an ECDD program in place that documents the actions you will take when the money laundering or terrorism financing risk is high.

You must document how you monitor customer transactions in Part A of your AML/CTF program. Your transaction monitoring program must be based on your risk assessment of your business or organisation and define the processes you follow to identify suspicious customer transactions, including:

- unusually large transactions
- complex transactions
- the splitting of transactions to avoid TTR reporting obligations, known as 'structuring'

- unexpected patterns of transactions that don't seem to have a legitimate purpose.

How you monitor transactions and develop your program depends on the size of your business or organisation and your level of assessed ML/TF risk. Depending on the type, size and complexity of your business or organisation, your transaction monitoring program can be manual or automated. You should allocate appropriate resources and give priority to analysing and actioning alerts raised by transaction monitoring.

Your transaction monitoring program

Your transaction monitoring program should:

- define the processes you follow to identify suspicious customer transactions
- document the systems, controls and procedures that mitigate and manage your ML/TF risks
- capture all sources of customer and transaction data or information
- set out systems and controls that trigger alerts for further review such as:
    - size, frequency or patterns of transactions that may indicate unusual or suspicious activity, including suspected fraud or identity theft
    - transactions that are sent to or received from a high-risk country or region
    - structuring of transactions to avoid TTR reporting obligations
    - payments that are sent to or received from a person or organisation on a sanctions list
    - activities that may be inconsistent with a customer's risk profile or history
    - increased monitoring of higher risk customers previously suspected of or investigated for potentially suspicious activity
    - other unexpected account activity from a customer which may indicate money laundering or terrorism financing

- implement processes to consistently review and manage the internal escalation and investigation of alerts
- prioritise alerts according to the level of risk

- document processes to consistently manage the reporting of potentially suspicious matters
- detail sufficient assurance processes to review the management of alerts
- continually monitor transactions across all levels of your business, not just, for example by branch or venue level
- document processes with enough detail to be consistently applied
- document and audit any automated transaction monitoring processes.

How your processes work together to understand your customer's AML/CTF risk profile

You must use your information sources and processes to monitor the services you are providing to customers to identify, mitigate and manage ML/TF risks.

Applicable customer identification procedures (ACIP), transaction monitoring, ECDD, reporting and other information all contribute to a better understanding of your customers. Your processes and information sources must contribute to a **single understanding of the customer and their risk profile**, rather than operate or exist independently.

Transaction monitoring alerts must be considered against the customer's history, including any information from law enforcement. You must ensure there is a central or accessible customer history for customer due diligence purposes.

For example, different teams in your business might hold information about a customer's suspected connections to terrorism, transaction monitoring alerts, suspicious activity on the customer's account and information from law enforcement about this customer.

You must have systems and controls in place so your business is able to easily and quickly combine this information, to give a comprehensive view of the customer's ML/TF risks.

Review and assurance of your transaction monitoring program

Your transaction monitoring must be applied to all designated services at all times. It must be supported by appropriate accountability and be regularly reviewed, to confirm that:

- processes are in place to make certain no disruptions to downstream AML/CTF processes occur when any changes are made to systems
- all systems changes that may potentially affect AML/CTF compliance require AML/CTF sign off
- all assurance processes are in place and AML/CTF processes are fully documented and mapped.

Transaction monitoring must be periodically reviewed to ensure it is operating as intended. Reviews must confirm that transaction monitoring is based on complete data, and that transaction monitoring rules remain appropriate and current. Automated transaction monitoring systems and program alerts need to incorporate any new methodologies, typologies or crime types.

Resolving any system issues must also receive adequate resourcing and priority. This should also be addressed from the time the failure or breakdown was identified to cover all past transactions.

Any problems identified must be addressed promptly. Failure to monitor transactions can have serious flow-on effects to other AML/CTF processes such as SMR reporting, conducting ECDD and the ongoing identification of ML/TF risks.

Example 1: Identifying high-risk transactions across a network

SavingsBank provides financial services products to a large portfolio of customers.

SavingsBank has a transaction monitoring program that monitors all customers to flag various behaviours. The customer behaviours link to risks that were identified when SavingsBank recently updated their ML/TF risk assessment.

A criminal network uses the bank to facilitate their activities

Unbeknown to SavingsBank, a network of 12 criminals open new accounts with them. The criminals plan to receive a transfer of funds into their accounts, wait several days, and then transfer the funds to multiple overseas accounts.

SavingsBank's risk assessment identified the overseas jurisdiction as high risk. As a result, they created alerts in their transaction monitoring program to flag individual customers transferring greater than $5,000 in a single transaction, or greater than $20,000 over a 28 day period, to that jurisdiction.

In an attempt to avoid detection, the criminals move no more than a total of $15,000 per month in small batches to the high risk jurisdiction. After several weeks, two members of the criminal network became more brazen and each transfer the full amount of $15,000 in one transaction.

Alerts are triggered in SavingsBank's transaction monitoring program

This triggers an alert on SavingsBank's transaction monitoring program, and following a further review, two SMRs were provided to AUSTRAC. However, the transaction monitoring program failed to identify patterns across the full criminal network's activity.

Law enforcement had an interest in the network and after receiving the two SMRs, serves a notice on SavingsBank for further information. On examining the additional customers, SavingsBank were able to see the full activity of the network. As a result, SavingsBank provided a series of SMRs to AUSTRAC.

Addressing the limitations of SavingsBank's transaction monitoring program

In this case, SavingsBank's transaction monitoring program was limited to the risks posed by the individual customers transferring funds to the high risk jurisdiction and was not adequately identifying multiple customers sending to the same beneficiary or increasing frequency of transactions to the jurisdiction. It was unable to identify patterns across the network, which could have been revealed, for example, if the transaction monitoring program had been set up to appropriately deal with the risk that the jurisdiction presented.

As a result, SavingsBank reviewed the capabilities of their transaction monitoring program and made changes to ensure it was identifying patterns of behaviour not just at the individual level, but also at a business level.

Example 2: Identifying structuring using transaction monitoring

SavingsBank provides a range of products and services to a large customer base. Their transaction monitoring program monitors all customers to flag various behaviours, including structuring. The behaviours link to risks identified in their ML/TF risk assessment.

A customer attends a branch to make a series of cash deposits into their personal account over two days:

- Monday – deposited cash of $7500.
- Tuesday – deposited cash of $5,400 at 10:15 AM and returned later that day at 3 PM to make a further cash deposit of $6000.

These transactions trigger a monitoring alert, which is reviewed to establish further information about the customer, including their transaction history. SavingsBank deems that these transactions could indicate structuring. SavingsBank undertakes enhanced customer due diligence, and submits a suspicious matter report to AUSTRAC.

The review also identifies a series of business accounts where the customer is a signatory. SavingsBank flags both the personal and business accounts for increased monitoring.

The following Wednesday, the customer returns to the same branch and makes a further two cash deposits of $8,000 and $4,000 into two of these business accounts.

SavingsBank's transaction monitoring systems triggers an alert for these two transactions and a further review is conducted, which includes linking the previous week's deposits by the customer. SavingsBank deems that these transactions are also suspected of involving structuring to avoid TTR reporting, and undertakes enhanced customer due diligence on these accounts. SavingsBank submits a further suspicious matter report to AUSTRAC.