TMS behaviours

Terminology

Term	Definition
Month	30 days.
6-month average	180 days divided by 6.
Account	A Currencycloud account identified by a string identifier (UUID) within account's `source_id` field. It is the account the funding was sent to or the account the payment was sent from - as denoted by the transaction's `account_source_id` field.
Parent account	If account A has a `parent_source_id` field containing the `source_id` value of account B, then account B is the parent of account A. It is the parent account of the account the funding was sent to or the account the payment was sent from - as denoted by the transaction's `parent_account_source_id` field.
Child account	If account A has a `parent_source_id` field containing the `source_id` value of account B, then account A is the child of account B.
Account family	A set of Currencycloud accounts that are all related (child, parent, sibling).
Funding	Transaction with the `transaction_type` field set to "fund".
Payment	Transaction with the `transaction_type` field set to "payment".
Sender	The sender of the transaction. If a transaction is a funding, the sender is identified by the the `sender_bank_account_digest` field of the transaction. If a transaction is a payment, the sender is identified by the `sender_id` field of the transaction. Payment's `sender_id` is an arbitrary identifier assigned by the payment service, and it is separate from the `account_source_id`.
Recipient	The recipient of the transaction. If a transaction is a funding, the recipient is identified by the the `recipient_id` field of the transaction. Fund's `recipient_id` is an identifier assigned by the funds service, and it is the same as the `account_source_id`. If a transaction is a payment, the recipient is identified by the `recipient_bank_account_digest` field of the transaction.
Threshold	Each behaviour has a defined threshold. In order for a behaviour to score, the `Actual` value must be higher or equal than both the `Expected` and the `Threshold` value. For any other scenarios, the behaviour will not score. Example here →
Bank account digest	A synthetic field of a transaction that calculates a single value for each individual set of bank account details provided within the transaction. Think of it as a single value identifier for otherwise compound identifier like a tuple of `sort_code` and `account_number`.
Upper bound of a set	A value that is calculated as 2 standard deviations higher than the mean of the set.

Mutable / Non-mutable behaviour	After an alert has been reviewed and closed by an Analyst, the specific behaviour breaches that led to the alert being generated are automatically muted for the same number of days as the look-back window for each behaviour (`muting period` = `actual time window`). All behaviours are mutable apart from the following five: - Structuring: Fund account structuring, Payment account structuring, Payment sender structuring - High risk customer - Politically Exposed Person
Business Risk Alignment	**Business Risk Alignment** is the strategic process of aligning each rule with our organisation's objectives and regulatory requirements, ensuring all risks are systematically addressed to support goals, optimise resources, and minimise negative impacts. Our business risks are: - **Fraud Risk:** Identifying and preventing fraudulent transactions. - **Money Laundering Risk:** Detecting patterns indicative of money laundering activities. - **Compliance Risk:** Ensuring adherence to regulatory and legal requirements. - **Operational Risk:** Maintaining system integrity and preventing operational issues. - **Reputational Risk:** Protecting the organisation's reputation by preventing association with illicit activities.

Change Log

The log was created in Aug '24. Any changes prior to this date can be found in TRUM Jira tickets (R.ai threshold optimisation, different muting periods, etc.)

#	Implementation Date	Change Overview	Rule impacted	Rationale	Implemented by
1	27 Aug 2024	Reduce the behaviour score	- Payment Sender Average Value - Reduce score from 25 to 10 - Payment Sender Structuring - Reduce score from 25 to 15	@Joseph Carrasco **Problem to solve:** At the time, TMS generated a high volume of alerts (≈150 daily), many of which resulted in no action being taken (<10%). This created unnecessary noise and operational strain. **Actions:** Reduce TMS alert volume by reducing the partial score of certain behaviours. The focus is on Sender behaviours, specifically Payment Sender Average Value (from 25 to 10) and Payment Sender Structuring (from 25 to 15). Notably, the three House Accounts with the highest alert volumes - Revolut, Covercy, and Centtrip - will be targeted for these adjustments. **Impact:** By implementing these changes, we anticipate a significant reduction in the daily alert volume, from ≈150 to ≈90, while producing minimal adverse impact (approximately 89% of Entity Relationship Ended alerts would still be triggered). This will prevent a new backlog within	@Joseph Carrasco

				TMS and, over time, provide the capacity to explore strategies for increasing the alert volume for known higher-risk House Accounts. This change aims to optimise where Analysts spend their time and reduce system noise without adding additional operational strain.	
2	16 Jan 2025	Increase by 100% (2x) the “Expected” value	• Average value ◦ Fund account average value ◦ Payment account average value ◦ Payment sender average value • Average volume ◦ Fund account average volume ◦ Payment account average volume ◦ Payment sender average volume	@Joseph Carrasco **Problem to Solve:** The previous Transaction Monitoring System (TMS) relied on fixed thresholds for alerting, causing noise and missed risk signals due to stagnant and inflexible thresholds. ***Actions***: Percentage-based Increase Thresholds: • Retained existing static thresholds. • Introduced dynamic alerts based on percentage increases over historical averages (the “expected” value). ***Expected Impact:*** • Reduce Noise: Decrease false positives, improving alert quality. • Optimise Resources: Focus on actual risks, enhancing resource allocation. • Per this report - we expect alert volume to decrease by 9.63%, while ‘missing’ true positive 7 alerts **Impact Assessment:** High Level • Successful launch - behaviour changes working as expected • Alert volume decreased by 13.6% • Impact on FAT% TBC Details • Pre Launch ◦ Total alerts from period 06/01 - 10/01: 294 (Daily average: 58.9) ◦ Example alert with old behaviour logic: Here • Post Launch ◦ Total alerts from period 06/01 - 10/01: 254 (Daily average: 50.8) ◦ Example alert with new behaviour logic: Here (note the behaviours prior to 16/01 score using old logic) • Next steps ◦ Analyse alert volumes for the next 3 weeks to gather 1 month of data, then compare to previous month's FAT% and volume	TRUM Core

					W/C 27/01, Analysts to review alerts created post 16/01 for initial FAT% impact assessment	

List of Behaviours

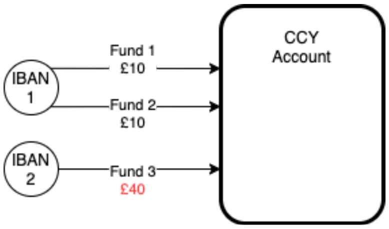
- Average value
  - Fund account average value
  - Payment account average value
  - Payment sender average value
- Average volume
  - Fund account average volume
  - Payment account average volume
  - Payment sender average volume
- Unique bank account digests
  - Fund account unique senders
  - Payment account unique recipients
- Bank account digest outlier
  - Fund account senders outlier
  - Payment account recipients outlier
  - Payment sender recipients outlier
- Common bank account digest
  - Fund account common sender
  - Payment account common recipient
  - Payment sender common recipient
- Value outlier
  - Fund account value outlier
  - Payment account value outlier
  - Payment sender value outlier
- Volume outlier
  - Fund account volume outlier
  - Payment account volume outlier
  - Payment sender volume outlier
- Transaction outlier
  - Fund account transaction outlier
  - Payment account transaction outlier
  - Payment sender transaction outlier
- Extended transaction outlier
  - Fund account extended transaction outlier
  - Payment account extended transaction outlier
- Structuring
  - Fund account structuring
  - Payment account structuring
  - Payment sender structuring
- Circular transaction
  - Fund account circular transaction
  - Payment account circular transaction
- Customer risk and PEP
  - Customer risk
  - PEP

Average value

Fund account average value

Description: The total value of funds received by an account over the last 20 days is compared against that account's 20-day average from the preceding 160 days (if the account is older than 6 months) or the expected value declared at onboarding (if the account is not older than 6 months).

Investigation tip: Conduct overall review as normal, while critically assessing who has funded the account.



<table>
<tr><td><b>Actual</b></td><td>

```
SELECT SUM(t.monitored_amount)
FROM transactions t
WHERE t.type = 'fund'
  AND (t.account_source_id = :context_source_id
    OR t.parent_account_source_id = :context_source_id)
  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 20 DAY)
```

</td></tr>
<tr><td><b>Expected</b></td><td>

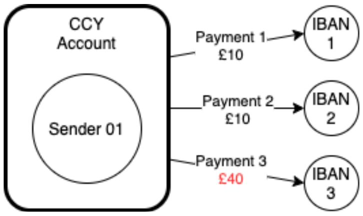
```
SELECT SUM(t.monitored_amount) / 8
FROM transactions t
WHERE t.type = 'fund'
  AND (t.account_source_id = :context_source_id
    OR t.parent_account_source_id = :context_source_id)
  AND t.effective_date < DATE_SUB(CURDATE(), INTERVAL 20 DAY)
  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 180 DAY)
```

</td></tr>
<tr><td><b>Score</b></td><td><code>5</code></td></tr>
<tr><td><b>Threshold</b></td><td><code>25_000</code></td></tr>
<tr><td><b>Business Risk Alignment</b></td><td>Money Laundering Risk</td></tr>
<tr><td><b>Notes</b></td><td>As of <code>16 Jan 2025</code> - The “Expected” value is doubled and then compared against the “Actual” value (see Change log for more details)</td></tr>
</table>

Payment account average value

Description: The total value of payments sent by an account over the last 35 days is compared against that account's 35-day average from the preceding 145 days (if the account is older than 6 months) or the expected value declared at onboarding (if the account is not older than 6 months).

Investigation tip: Conduct overall review as normal, while critically assessing who has funded the account and the beneficiaries of payments.

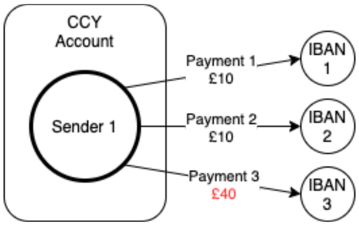


<table>
<tr><td><b>Actual</b></td><td><pre>SELECT SUM(t.monitored_amount)
FROM transactions t
WHERE t.type = 'payment'
  AND (t.account_source_id = :context_source_id
    OR t.parent_account_source_id = :context_source_id)
  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 35 DAY)</pre></td></tr>
<tr><td><b>Expected</b></td><td><pre>SELECT SUM(t.monitored_amount) / 4.14
FROM transactions t
WHERE t.type = 'payment'
  AND (t.account_source_id = :context_source_id
    OR t.parent_account_source_id = :context_source_id)
  AND t.effective_date < DATE_SUB(CURDATE(), INTERVAL 35 DAY)
  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 180 DAY)</pre></td></tr>
<tr><td><b>Score</b></td><td><code>5</code></td></tr>
<tr><td><b>Threshold</b></td><td><code>100_000</code></td></tr>
<tr><td><b>Business Risk Alignment</b></td><td>Money Laundering Risk</td></tr>
<tr><td><b>Notes</b></td><td>As of 16 Jan 2025 - The “Expected” value is doubled and then compared against the “Actual” value (see Change log for more details)</td></tr>
</table>

Payment sender average value

Description: The total value of payments sent by a sender over the last 10 days is compared against that sender's 10-day average from the preceding 160 days.

Investigation tip: Conduct overall review as normal, while critically assessing the beneficiaries of payments.



<table>
<tr><td><b>Actual</b></td><td><pre>SELECT SUM(t.monitored_amount)
FROM transactions t
WHERE t.type = 'payment'
  AND t.account_source_id = :context_source_id
  AND t.sender_id = :context_sender_id
  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 10 DAY)</pre></td></tr>
</table>

Expected	`SELECT SUM(t.monitored_amount) / 16`
	`FROM transactions t`
	`WHERE t.type = 'payment'`
	`  AND t.account_source_id = :context_source_id`
	`  AND t.sender_id = :context_sender_id`
	`  AND t.effective_date < DATE_SUB(CURDATE(), INTERVAL 10 DAY)`
	`  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 170 DAY)`

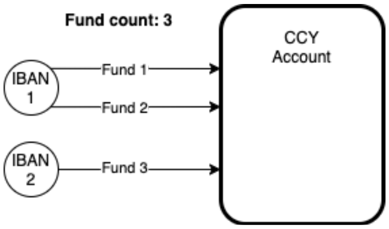
Score	`10`
Threshold	`15_000`
Business Risk Alignment	Money Laundering Risk
Notes	As of `16 Jan 2025` - The “Expected” value is doubled and then compared against the “Actual” value (see Change log for more details)

Average volume

Fund account average volume

Description: The total volume of funds received by an account over the last 15 days is compared against that account's 15-day average from the preceding 155 days (if the account is older than 6 months) or the expected value declared at onboarding (if the account is not older than 6 months).

Investigation tip: This can indicate scams and fraud, particularly in accounts with limited prior transactional activity.



Actual	`SELECT COUNT(t.id)`
	`FROM transactions t`
	`WHERE t.type = 'fund'`
	`  AND (t.account_source_id = :context_source_id`
	`    OR t.parent_account_source_id = :context_source_id)`
	`  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 15 DAY)`

Expected	`SELECT COUNT(t.id) / 10.33`
	`FROM transactions t`
	`WHERE t.type = 'fund'`
	`  AND (t.account_source_id = :context_source_id`
	`    OR t.parent_account_source_id = :context_source_id)`
	`  AND t.effective_date < DATE_SUB(CURDATE(), INTERVAL 15 DAY)`
	`  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 170 DAY)`

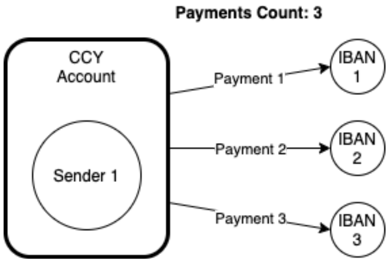
Score	`5`
Threshold	`10`

Business Risk Alignment	Fraud Risk
Notes	As of `16 Jan 2025` - The “Expected” value is doubled and then compared against the “Actual” value (see Change log for more details)

Payment account average volume

Description: The total volume of payments sent by an account over the last 30 days is compared against that account's 30-day average from the preceding 210 days (if the account is older than 6 months) or the expected value declared at onboarding (if the account is not older than 6 months).

Investigation tip: This can indicate scams and fraud, particularly in accounts with limited prior transactional activity.



Actual	`SELECT COUNT(t.id)`
	`FROM transactions t`
	`WHERE t.type = 'payment'`
	`  AND (t.account_source_id = :context_source_id`
	`    OR t.parent_account_source_id = :context_source_id)`
	`  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 30 DAY)`

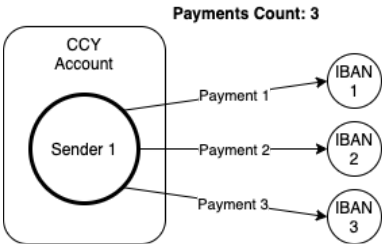
Expected	`SELECT COUNT(t.id) / 6`
	`FROM transactions t`
	`WHERE t.type = 'payment'`
	`  AND (t.account_source_id = :context_source_id`
	`    OR t.parent_account_source_id = :context_source_id)`
	`  AND t.effective_date < DATE_SUB(CURDATE(), INTERVAL 30 DAY)`
	`  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 210 DAY)`

Score	`5`
Threshold	`20`
Business Risk Alignment	Fraud Risk
Notes	As of `16 Jan 2025` - The “Expected” value is doubled and then compared against the “Actual” value (see Change log for more details)

Payment sender average volume

Description: The total volume of payments sent by a sender over the last 30 days is compared against that sender's 30-day average from the preceding 150 days.

Investigation tip: This can indicate scams and fraud, particularly in senders with limited prior transactional activity.



Actual	`SELECT COUNT(t.id)`
	`FROM transactions t`
	`WHERE t.type = 'payment'`
	`  AND t.account_source_id = :context_source_id`
	`  AND t.sender_id = :context_sender_id`
	`  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 30 DAY)`

Expected	`SELECT COUNT(t.id) / 5`
	`FROM transactions t`
	`WHERE t.type = 'payment'`
	`  AND t.account_source_id = :context_source_id`
	`  AND t.sender_id = :context_sender_id`
	`  AND t.effective_date < DATE_SUB(CURDATE(), INTERVAL 30 DAY)`
	`  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 180 DAY)`

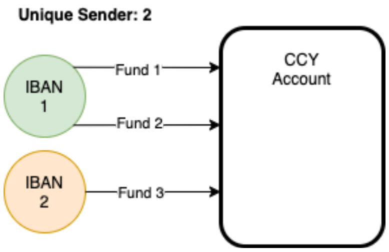
Score	`20`
Threshold	`24`
Business Risk Alignment	Fraud Risk
Notes	As of `16 Jan 2025` - The “Expected” value is doubled and then compared against the “Actual” value (see Change log for more details)

Unique bank account digests

Fund account unique senders

Description: The number of unique senders sending funds to an account over the last 30 days is compared against a value of 5.

Investigation tip: This can indicate scams and fraud, particularly in accounts with limited prior transactional activity.



Actual	`SELECT COUNT(DISTINCT(t.sender_bank_account_digest))`
	`FROM transactions t`
	`WHERE t.type = 'fund'`

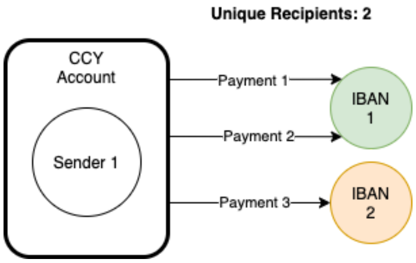
	`  AND (t.account_source_id = :context_source_id`
	`    OR t.parent_account_source_id = :context_source_id)`
	`  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 30 DAY)`

Expected	`5`
Score	`5`
Threshold	`0`
Business Risk Alignment	Fraud Risk

Payment account unique recipients

Description: The number of unique payment recipients for an account over the last 30 days is compared against a value of 10.

Investigation tip: This can indicate scams and fraud, particularly in accounts with limited prior transactional activity.



Actual	`SELECT COUNT(DISTINCT(t.recipient_bank_account_digest))`
	`FROM transactions t`
	`WHERE t.type = 'payment'`
	`  AND (t.account_source_id = :context_source_id`
	`    OR t.parent_account_source_id = :context_source_id)`
	`  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 30 DAY)`

Expected	`10`
Score	`5`
Threshold	`0`
Business Risk Alignment	Fraud and Money Laundering Risk

Bank account digest outlier

Fund account senders outlier

Description: The number of unique senders sending funds to an account over the last 30 days is compared against 2 standard deviations greater than the mean of unique funding senders for each of the accounts in the account family from the preceding 180 days.

Investigation tip: This can indicate scams and fraud, particularly in accounts with limited prior transactional activity.

Actual

```
SELECT COUNT(DISTINCT(t.sender_bank_account_digest))
AS senderCount
FROM transactions t
WHERE t.type = 'fund'
  AND t.account_source_id = :context_source_id
  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 30 DAY)
```

Expected

```
SELECT FORMAT(AVG(senderCount) + 2 * STD(senderCount), 2)
FROM (
  SELECT COUNT(DISTINCT(t.sender_bank_account_digest))
  AS senderCount
  FROM transactions t
  WHERE t.type = 'fund'
    AND (t.account_source_id = :context_parent_source_id
      OR t.parent_account_source_id = :context_parent_source_id)
    AND t.effective_date < DATE_SUB(CURDATE(), INTERVAL 30 DAY)
    AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 180 DAY)
  GROUP BY t.account_source_id
)
```

Score	`15`
Threshold	`5`
Business Risk Alignment	Fraud and Money Laundering Risk

Payment account recipients outlier

Description: The number of unique payment recipients for an account over the last 30 days is compared against 2 standard deviations greater than the mean of unique payment recipients for each of the accounts in the account family from the preceding 180 days.

Investigation tip: This can indicate scams and fraud, particularly in accounts with limited prior transactional activity.

Actual

```
SELECT COUNT(DISTINCT(t.recipient_bank_account_digest))
AS recipientCount
FROM transactions t
WHERE t.type = 'payment'
  AND t.account_source_id = :context_source_id
  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 30 DAY)
```

Expected

```
SELECT FORMAT(AVG(recipientCount) + 2 * STD(recipientCount), 2)
FROM (
  SELECT COUNT(DISTINCT(t.recipient_bank_account_digest))
  AS recipientCount
  FROM transactions t
  WHERE t.type = 'payment'
    AND (t.account_source_id = :context_parent_source_id
      OR t.parent_account_source_id = :context_parent_source_id)
    AND t.effective_date < DATE_SUB(CURDATE(), INTERVAL 30 DAY)
    AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 180 DAY)
  GROUP BY t.account_source_id
)
```

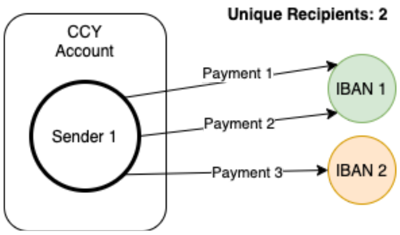
Score	`5`

Threshold	10
Business Risk Alignment	Fraud and Money Laundering Risk

Payment sender recipients outlier

Description: The number of unique payment recipients for a sender over the last 30 days is compared against 2 standard deviations greater than the mean of unique payment recipients for each of the account's senders from the preceding 180 days.

Investigation tip: This can indicate scams and fraud, particularly in senders with limited prior transactional activity.



<table>
<tr><td><b>Actual</b></td><td>

```
SELECT COUNT(DISTINCT(t.recipient_bank_account_digest))
AS recipientCount
FROM transactions t
WHERE t.type = 'payment'
  AND t.account_source_id = :context_source_id
  AND t.sender_id = :context_sender_id
  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 30 DAY)
```

</td></tr>
<tr><td><b>Expected</b></td><td>

```
SELECT FORMAT(AVG(recipientCount) + 2 * STD(recipientCount), 2)
FROM (
  SELECT COUNT(DISTINCT(t.recipient_bank_account_digest))
  AS recipientCount
  FROM transactions t
  WHERE t.type = 'payment'
    AND t.account_source_id = :context_source_id
    AND t.effective_date < DATE_SUB(CURDATE(), INTERVAL 30 DAY)
    AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 180 DAY)
  GROUP BY t.sender_id
)
```

</td></tr>
<tr><td><b>Score</b></td><td>5</td></tr>
<tr><td><b>Threshold</b></td><td>10</td></tr>
<tr><td><b>Business Risk Alignment</b></td><td>Fraud and Money Laundering Risk</td></tr>
</table>

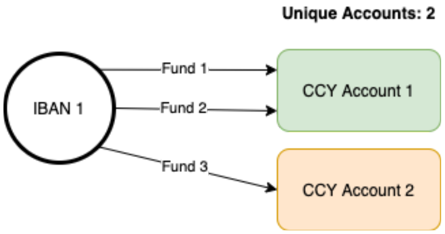
Common bank account digest

Fund account common sender

Description: The number of accounts that have received a fund from a common sender over the last 20 days is compared against a value of 2. The partial score is assigned to the account.

Investigation tip: Evaluate the recipient accounts profile (e.g. Are funds being sent to random individuals?) and the profile of the common sender. Can indicate scams, fraud, or networks of suspicious accounts.

Update (Mar '24): If the TMS service does not receive the required underlying transactional data to execute the behaviour (e.g. bank account details for the ultimate sender of an inbound fund, where there are limitations in the scope of transactional data CC has received via local inbound funding routes), then that specific behaviour will be "skipped" - and no partial scores for that behaviour will be triggered for the specific entity in that's the subject of the skipped behaviour.



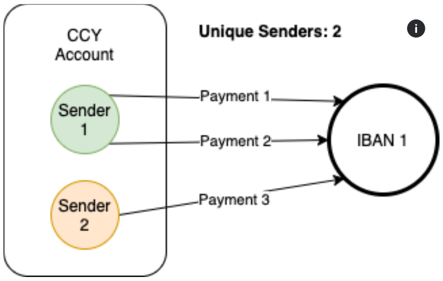
Actual	`SELECT COUNT(DISTINCT(t.account_source_id))`
	`AS accountCount`
	`FROM transactions t`
	`WHERE t.type = 'fund'`
	`  AND t.sender_bank_account_digest = :context_bank_account_digest`
	`  AND t.effective_date > DATE_SUB(CURDATE(), INTERVAL 20 DAY)`

Expected	`2`
Score	`5`
Threshold	`0`
Business Risk Alignment	Fraud and Money Laundering Risk

Payment account common recipient

Description: The number of accounts that have sent a payment to a common recipient over the last 40 days is compared against a value of 2. The partial score is assigned to the account.

Investigation tip: Evaluate the recipient bank account profile (e.g. Can they feasibly receive funds from multiple entities?) and which other accounts have sent payments to this bank account (e.g. Do you have concerns about other accounts?). Can indicate scams, fraud, or networks of suspicious accounts.



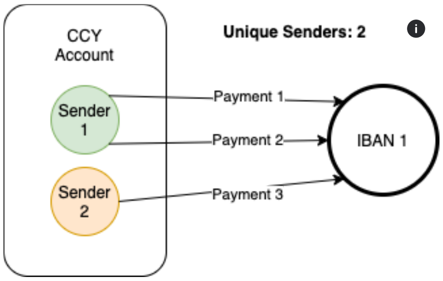
Actual	`SELECT COUNT(DISTINCT(t.account_source_id))`
	`AS accountCount`
	`FROM transactions t`
	`WHERE t.type = 'payment'`
	`  AND t.recipient_bank_account_digest = :context_bank_account_digest`
	`  AND t.effective_date > DATE_SUB(CURDATE(), INTERVAL 40 DAY)`

Expected	`2`
Score	`10`
Threshold	`0`
Business Risk Alignment	Fraud and Money Laundering Risk

Payment sender common recipient

Description: The number of senders that have sent a payment to a common recipient over the last 45 days is compared against a value of 2. The partial score is assigned to the account's sender.

Investigation tip: Evaluate the recipient bank account profile (e.g. Can they feasibly receive funds from multiple entities?) and which other accounts have sent payments to this bank account (e.g. Do you have concerns about other accounts?). Can indicate scams, fraud, or networks of suspicious accounts.



Actual	`SELECT COUNT(DISTINCT(t.account_source_id))`
	`AS accountCount`
	`FROM transactions t`
	`WHERE t.type = 'payment'`
	`  AND t.recipient_bank_account_digest = :context_bank_account_digest`
	`  AND t.effective_date > DATE_SUB(CURDATE(), INTERVAL 45 DAY)`

Expected	`2`
Score	`5`

Threshold	`0`
Business Risk Alignment	Fraud and Money Laundering Risk

Value outlier

Fund account value outlier

Description: The total value of funds received by an account over the last 30 days is compared against 2 standard deviations greater than the mean of total fund values for each of the accounts in the account family from the preceding 150 days.

This behaviour is only applied to house and sub accounts with at least 10 subs/senders under the house.

Investigation tip: Conduct overall review as normal, while critically assessing any reason for this higher value relative to other subs (clients) for the house (e.g. Is this just a large client of the house?).

Actual	`SELECT SUM(t.monitored_amount)`
	`AS accountValue`
	`FROM transactions t`
	`WHERE t.type = 'fund'`
	`  AND t.account_source_id = :context_source_id`
	`  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 30 DAY)`

Expected	`SELECT FORMAT(AVG(accountAmount) + 2 * STD(accountAmount), 2)`
	`FROM (`
	`  SELECT SUM(t.monitored_amount) / 5`
	`  AS accountValue`
	`  FROM transactions t`
	`  WHERE t.type = 'fund'`
	`    AND (t.account_source_id = :context_parent_source_id`
	`      OR t.parent_account_source_id = :context_parent_source_id)`
	`    AND t.effective_date < DATE_SUB(CURDATE(), INTERVAL 30 DAY)`
	`    AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 180 DAY)`
	`  GROUP BY t.account_source_id`
	`)`

Score	`20`
Threshold	`16_000`
Business Risk Alignment	Money Laundering Risk

Payment account value outlier

Description: The total value of payments sent by an account over the last 30 days is compared against 2 standard deviations greater than the mean of total payment values for each of the accounts in the account family from the preceding 140 days.

This behaviour is only applied to house and sub accounts with at least 10 subs/senders under the house.

Investigation tip: Conduct overall review as normal, while critically assessing any reason for this higher value relative to other subs (clients) for the house (e.g. Is this just a large client of the house?).

Actual

```
SELECT SUM(t.monitored_amount)
AS accountValue
FROM transactions t
WHERE t.type = 'payment'
  AND t.account_source_id = :context_source_id
  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 30 DAY)
```

Expected

```
SELECT FORMAT(AVG(accountAmount) + 2 * STD(accountAmount), 2)
FROM (
  SELECT SUM(t.monitored_amount) / 4.66
  AS accountValue
  FROM transactions t
  WHERE t.type = 'payment'
    AND (t.account_source_id = :context_parent_source_id
      OR t.parent_account_source_id = :context_parent_source_id)
    AND t.effective_date < DATE_SUB(CURDATE(), INTERVAL 30 DAY)
    AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 170 DAY)
  GROUP BY t.account_source_id
)
```

Score	`25`
Threshold	`15_000`
Business Risk Alignment	Money Laundering Risk

Payment sender value outlier

Description: The total value of payments sent by a sender over the last 30 days is compared against 2.3 standard deviations greater than the mean of total payment values for each of the account's senders from the preceding 150 days.

This behaviour is only applied to senders under a house account that has at least 10 senders under the house.

Investigation tip: Conduct overall review as normal, while critically assessing any reason for this higher value relative to other subs (clients) for the house (e.g. Is this just a large client of the house?).

Actual

```
SELECT SUM(t.monitored_amount)
AS senderValue
FROM transactions t
WHERE t.type = 'payment'
  AND t.account_source_id = :context_source_id
  AND t.sender_id = :context_sender_id
  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 30 DAY)
```

Expected

```
SELECT FORMAT(AVG(senderAmount) + 2 * STD(senderAmount), 2.3)
FROM (
  SELECT SUM(t.monitored_amount) / 5
  AS senderValue
  FROM transactions t
  WHERE t.type = 'payment'
    AND t.account_source_id = :context_source_id
    AND t.effective_date < DATE_SUB(CURDATE(), INTERVAL 30 DAY)
    AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 180 DAY)
  GROUP BY t.sender_id
)
```

Score	`15`
Threshold	`150_000`
Business Risk Alignment	Money Laundering Risk

Volume outlier

Fund account volume outlier

Description: The total volume of funds received by an account over the last 10 days is compared against 2 standard deviations greater than the mean of fund volume for each of the accounts in the account family from the preceding 170 days.

This behaviour is only applied to house and sub accounts with at least 10 subs/senders under the house.

Investigation tip: Conduct overall review as normal, while critically assessing any reason for this higher volume relative to other subs (clients) for the house (e.g. Is this just a large client of the house?).

<table>
<tr><td><b>Actual</b></td><td>

```
SELECT COUNT(t.id)
AS accountVolume
FROM transactions t
WHERE t.type = 'fund'
  AND t.account_source_id = :context_source_id
  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 10 DAY)
```

</td></tr>
<tr><td><b>Expected</b></td><td>

```
SELECT FORMAT(AVG(accountVolume) + 2 * STD(accountVolume), 2)
FROM (
  SELECT COUNT(t.id) / 17
  AS accountVolume
  FROM transactions t
  WHERE t.type = 'fund'
    AND (t.account_source_id = :context_parent_source_id
      OR t.parent_account_source_id = :context_parent_source_id)
    AND t.effective_date < DATE_SUB(CURDATE(), INTERVAL 10 DAY)
    AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 180 DAY)
  GROUP BY t.account_source_id
)
```

</td></tr>
<tr><td><b>Score</b></td><td>5</td></tr>
<tr><td><b>Threshold</b></td><td>11</td></tr>
<tr><td><b>Business Risk Alignment</b></td><td>Money Laundering Risk</td></tr>
</table>

Payment account volume outlier

Description: The total volume of payments sent by an account over the last 30 days is compared against 2 standard deviations greater than the mean of fund volume for each of the accounts in the account family from the preceding 150 days.

This behaviour is only applied to house and sub accounts with at least 10 subs/senders under the house.

Investigation tip: Conduct overall review as normal, while critically assessing any reason for this higher volume relative to other subs (clients) for the house (e.g. Is this just a large client of the house?).

<table>
<tr><td><b>Actual</b></td><td>

```
SELECT COUNT(t.id)
AS accountVolume
FROM transactions t
WHERE t.type = 'payment'
  AND t.account_source_id = :context_source_id
  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 30 DAY)
```

</td></tr>
<tr><td><b>Expected</b></td><td>

```
SELECT FORMAT(AVG(accountAmount) + 2 * STD(accountAmount), 2)
FROM (
  SELECT COUNT(t.id) / 5
  AS accountVolume
  FROM transactions t
  WHERE t.type = 'payment'
    AND (t.account_source_id = :context_parent_source_id
      OR t.parent_account_source_id = :context_parent_source_id)
    AND t.effective_date < DATE_SUB(CURDATE(), INTERVAL 30 DAY)
    AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 180 DAY)
  GROUP BY t.account_source_id
)
```

</td></tr>
<tr><td><b>Score</b></td><td><code>5</code></td></tr>
<tr><td><b>Threshold</b></td><td><code>19</code></td></tr>
<tr><td><b>Business Risk Alignment</b></td><td>Fraud Risk</td></tr>
</table>

Payment sender volume outlier

Description: The total volume of payments sent by a sender over the last 20 days is compared against 2 standard deviations greater than the mean of payment volume for each of the account's senders from the preceding 160 days.

This behaviour is only applied to senders under a house account that has at least 10 senders under the house.

Investigation tip: Conduct overall review as normal, while critically assessing any reason for this higher volume relative to other subs (clients) for the house (e.g. Is this just a large client of the house?).

<table>
<tr><td><b>Actual</b></td><td>

```
SELECT COUNT(t.id)
AS senderVolume
FROM transactions t
WHERE t.type = 'payment'
  AND t.account_source_id = :context_source_id
  AND t.sender_id = :context_sender_id
  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 20 DAY)
```

</td></tr>
<tr><td><b>Expected</b></td><td>

```
SELECT FORMAT(AVG(senderVolume) + 2 * STD(senderVolume), 2)
FROM (
  SELECT COUNT(t.id) / 8
  AS senderVolume
  FROM transactions t
  WHERE t.type = 'payment'
    AND t.account_source_id = :context_source_id
    AND t.effective_date < DATE_SUB(CURDATE(), INTERVAL 20 DAY)
    AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 180 DAY)
```

</td></tr>
</table>

	`  GROUP BY t.sender_id`
	`)`

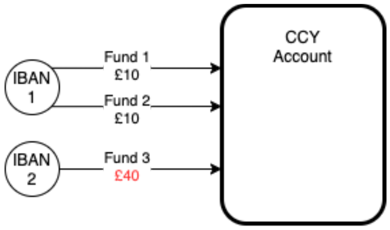
Score	`10`
Threshold	`19`
Business Risk Alignment	Fraud Risk

Transaction outlier

Fund account transaction outlier

Description: The value of a single fund is compared against 2 standard deviations greater than the mean of fund values for that account over the last 180 days.

Investigation tip: Investigate the transaction in question while assessing overall account activity.



Actual	`SELECT :context_monitored_amount`
	`AS monitoredAmount`

Expected	`SELECT FORMAT(AVG(monitoredAmount) + 2 * STD(monitoredAmount), 2)`
	`FROM (`
	`  SELECT t.monitored_amount`
	`  AS monitoredAmount`
	`  FROM transactions t`
	`  WHERE t.type = 'fund'`
	`    AND (t.account_source_id = :context_source_id`
	`      OR t.parent_account_source_id = :context_source_id)`
	`    AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 180 DAY)`
	`)`

Score	`5`
Threshold	`20_000`
Business Risk Alignment	Money Laundering Risk

Payment account transaction outlier

Description: The value of a single payment is compared against 2 standard deviations greater than the mean of payment values for that account over the last 180 days.

Investigation tip: Investigate the transaction in question while assessing overall account activity.

Actual	`SELECT :context_monitored_amount`
	`AS monitoredAmount`

Expected	`SELECT FORMAT(AVG(monitoredAmount) + 2 * STD(monitoredAmount), 2)`
	`FROM (`
	`  SELECT t.monitored_amount`
	`  AS monitoredAmount`
	`  FROM transactions t`
	`  WHERE t.type = 'payment'`
	`    AND (t.account_source_id = :context_source_id`
	`      OR t.parent_account_source_id = :context_source_id)`
	`    AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 180 DAY)`
	`)`

Score	`5`
Threshold	`20_000`
Business Risk Alignment	Money Laundering Risk

Payment sender transaction outlier

Description: The value of a single payment is compared against 2 standard deviations greater than the mean of payment values for that sender over the last 180 days.

Investigation tip: Investigate the transaction in question while assessing overall account activity.

Actual	`SELECT :context_monitored_amount`
	`AS monitoredAmount`

Expected	`SELECT FORMAT(AVG(monitoredAmount) + 2 * STD(monitoredAmount), 2)`
	`FROM (`
	`  SELECT t.monitored_amount`
	`  AS monitoredAmount`
	`  FROM transactions t`
	`  WHERE t.type = 'payment'`
	`    AND t.account_source_id = :context_source_id`
	`    AND t.sender_id = :context_sender_id`
	`    AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 180 DAY)`
	`)`

Score	`10`
Threshold	`20_000`
Business Risk Alignment	Money Laundering Risk

Extended transaction outlier

Fund account extended transaction outlier

Description: The value of a single fund is compared against 2 standard deviations greater than the mean of fund values for all accounts in the account family over the last 180 days.

Investigation tip: Investigate the transaction in question while assessing overall account activity.

Actual	`SELECT :context_monitored_amount`
	`AS monitoredAmount`

Expected	`SELECT FORMAT(AVG(monitoredAmount) + 2 * STD(monitoredAmount), 2)`
	`FROM (`
	`  SELECT t.monitored_amount`
	`  AS monitoredAmount`
	`  FROM transactions t`
	`  WHERE t.type = 'fund'`
	`    AND (t.account_source_id = :context_parent_source_id`
	`      OR t.parent_account_source_id = :context_parent_source_id)`
	`    AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 180 DAY)`
	`)`

Score	`15`
Threshold	`20_000`
Business Risk Alignment	Money Laundering Risk

Payment account extended transaction outlier

Description: The value of a single payment is compared against 2 standard deviations greater than the mean of payment values for all accounts in the account family over the last 180 days.

Investigation tip: Investigate the transaction in question while assessing overall account activity.

Actual	`SELECT :context_monitored_amount`
	`AS monitoredAmount`

Expected	`SELECT FORMAT(AVG(monitoredAmount) + 2 * STD(monitoredAmount), 2)`
	`FROM (`
	`  SELECT t.monitored_amount`
	`  AS monitoredAmount`
	`  FROM transactions t`
	`  WHERE t.type = 'payment'`
	`    AND (t.account_source_id = :context_parent_source_id`
	`      OR t.parent_account_source_id = :context_parent_source_id)`
	`    AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 180 DAY)`
	`)`

Score	`15`
Threshold	`20_000`

Business Risk Alignment	Money Laundering Risk

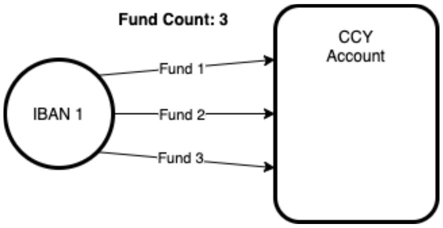
Structuring

Fund account structuring

Description: The number of funds with the same sender and recipient over the last 2 days is compared against a value of 3.

Investigation tip: Structuring can be linked to scams and fraud, particularly when coupled with rounded transaction values and common sender/recipient alerts.

Update (Mar '24): If the TMS service does not receive the required underlying transactional data to execute the behaviour (e.g. bank account details for the ultimate sender of an inbound fund, where there are limitations in the scope of transactional data CC has received via local inbound funding routes), then that specific behaviour will be "skipped" - and no partial scores for that behaviour will be triggered for the specific entity in that's the subject of the skipped behaviour.



<table>
<tr><td><b>Actual</b></td><td>

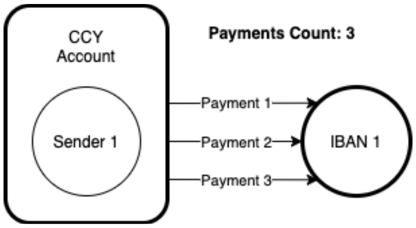
```
SELECT COUNT(t.id)
FROM transactions t
WHERE t.type = 'fund'
  AND (t.account_source_id = :context_source_id
    OR t.parent_account_source_id = :context_source_id)
  AND t.sender_bank_account_digest = :context_bank_account_digest
  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 1 DAY)
```

</td></tr>
<tr><td><b>Expected</b></td><td><code>3</code></td></tr>
<tr><td><b>Score</b></td><td><code>10</code></td></tr>
<tr><td><b>Threshold</b></td><td><code>0</code></td></tr>
<tr><td><b>Business Risk Alignment</b></td><td>Fraud and Compliance Risk</td></tr>
</table>

Payment account structuring

Description: The number of payments with the same sender and recipient over the last 2 days is compared against a value of 3.

Investigation tip: Structuring can be linked to scams and fraud, particularly when coupled with rounded transaction values and common sender/recipient alerts.



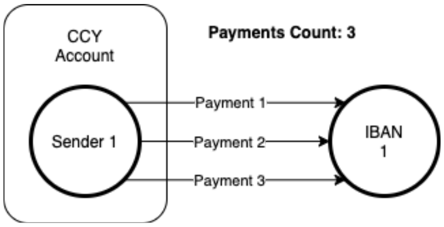
Actual	`SELECT COUNT(t.id)`
	`FROM transactions t`
	`WHERE t.type = 'payment'`
	`  AND (t.account_source_id = :context_source_id`
	`    OR t.parent_account_source_id = :context_source_id)`
	`  AND t.sender_bank_account_digest = :context_bank_account_digest`
	`  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 1 DAY)`

Expected	`3`
Score	`5`
Threshold	`0`
Business Risk Alignment	Fraud and Compliance Risk

Payment sender structuring

Description: The number of payments with the same sender and recipient over the last 2 days is compared against a value of 3.

Investigation tip: Structuring can be linked to scams and fraud, particularly when coupled with rounded transaction values and common sender/recipient alerts.



Actual	`SELECT COUNT(t.id)`
	`FROM transactions t`
	`WHERE t.type = 'payment'`
	`  AND t.account_source_id = :context_source_id`
	`  AND t.sender_id = :context_sender_id`
	`  AND t.sender_bank_account_digest = :context_bank_account_digest`
	`  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 1 DAY)`

Expected	`3`
Score	`15`
Threshold	`0`

Business Risk Alignment	Fraud and Compliance Risk

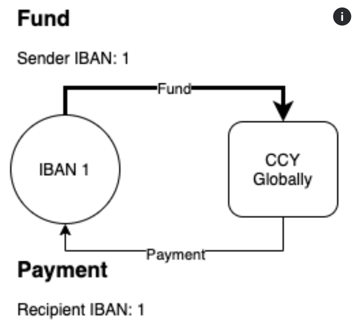
Circular transaction

Fund account circular transaction

Description: The number of payments with a recipient equal to a fund’s sender over the last 30 days is compared against a value of 0.

Investigation tip: Can indicate companies under a single point of control are processing transactions to inflate the revenue of one or more of the companies. Legitimate cases could include refunds to the same bank account.

Update (Mar '24): If the TMS service does not receive the required underlying transactional data to execute the behaviour (e.g. bank account details for the ultimate sender of an inbound fund, where there are limitations in the scope of transactional data CC has received via local inbound funding routes), then that specific behaviour will be "skipped" - and no partial scores for that behaviour will be triggered for the specific entity in that's the subject of the skipped behaviour.



Fund Sender IBAN = Payment Recipient IBAN

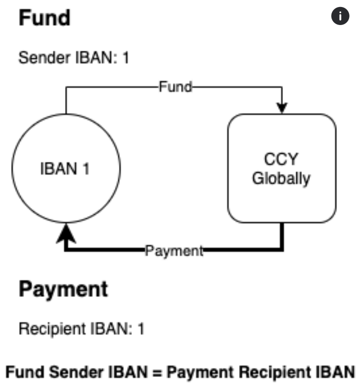
Actual	`SELECT COUNT(t.id)`
	`FROM transactions t`
	`WHERE t.type = 'payment'`
	`  AND t.recipient_bank_account_digest = :context_bank_account_digest`
	`  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 30 DAY)`

Expected	`0`
Score	`5`
Threshold	`0`
Business Risk Alignment	Money Laundering Risk

Payment account circular transaction

Description: The number of funds with a sender equal to a payment’s recipient over the last 30 days is compared against a value of 0.

Investigation tip: Can indicate companies under a single point of control are processing transactions to inflate the revenue of one or more of the companies. Legitimate cases could include refunds to the same bank account.



Actual	`SELECT COUNT(t.id)`
	`FROM transactions t`
	`WHERE t.type = 'fund'`
	`  AND t.sender_bank_account_digest = :context_bank_account_digest`
	`  AND t.effective_date >= DATE_SUB(CURDATE(), INTERVAL 30 DAY)`

Expected	`0`
Score	`5`
Threshold	`0`
Business Risk Alignment	Money Laundering Risk

Customer risk and PEP

Customer risk

Description: If the account’s "customer_risk" attribute = "high", then when the account executes a transaction it triggers this behaviour and is assigned a partial score of 5. This effectively lowers the entity’s investigation threshold to 25. But if the account does not trigger other behaviours and ultimately breach the investigation threshold within 30 days, then this +5 partial score expires.

Investigation tip: Consider common red flags such as location, country risk of recipient payment countries (e.g. off-shore jurisdictions), and complex structures.

PEP

Description: If the account’s connected_politically_exposed_persons attribute = "true", then when the account executes a transaction it triggers this behaviour and is assigned a partial score of 5. This effectively lowers the entity’s investigation threshold to 25. But if the account does not trigger other behaviours and ultimately breach the investigation threshold within 30 days, then this +5 partial score expires.

Investigation tip: Consider common red flags such as location, country risk of recipient payment countries (e.g. off-shore jurisdictions), and complex structures.