FYSCAL TECHNOLOGIES

Fyscal ARCX Platform Guide

Step-by-step documentation for compliance teams using Fyscal ARCX.

Edition	2 November 2026
Online version	https://fyscal-arcx-user-guide.pages.dev/
Support	hello@fyscaltech.com

© 2026 Fyscal Technologies PTE LTD. All rights reserved. Screens may differ by deployment and configuration. Personal data in screenshots is blurred. 491 annotated screens.

Contents

1. Getting Started
- How Fyscal ARCX fits together
- Where to start, by role
- Signing in
- The Homepage and navigation
- Activity notifications
- The user menu
- Changing your password
- Roles
- How this guide is organised

2. AML Dashboard
- Dashboard layout
- Metric tiles
- Case Distribution controls
- By Status
- By Disposition (Closed)
- By Score and By Type (Alerts view)
- By Assignment
- STR Filed
- By Age
- Pending Review, Avg. Handling and Reopens
- Daily Jobs
- Team Performance
- Daily triage from the dashboard

3. Case Manager
- Cases list
- Filter and search cases
- Case statuses and dispositions
- Case Details
- Customer, accounts and matches
- Transaction Monitoring evidence tabs
- Timeline and notes
- Case Copilot
- Add alerts to a case
- Dispose alerts and close a case
- Review a case in Pending Review
- Reopen a case
- File an STR
- Open the STR wizard
- Step 1: Select Alerts
- Step 2: Report Type
- Step 3: Reason for suspicion
- Step 4: Transaction
- Step 5: Subject parties
- Step 6: Narratives
- After the STR is filed
- Common blocks
- Alerts list
- Alert Details: Name Screening
- Alert Details: Transaction Monitoring
- Work an alert

4. Case Manager Configuration
- Case Creation & Assignment: Active Configuration
- Edit the case creation configuration
- Configuration History
- Alert Assignment
- Agentic Workflows: Prompt Config
- Edit and publish a prompt
- Agentic Workflows: Model Config
- Team Management: the hierarchy list
- Add a hierarchy
- View a hierarchy's details
- The hierarchy builder: Template Builder tab
- The hierarchy builder: Hierarchy Builder tab

5. Customer 360
- The customer list
- Search and filter the list
- The Customer Profile
- Customer Risk Score tab
- Analytics tab
- Transactions tab
- Other Cases / Alerts tab
- Screening History tab
- STR History tab
- Review a customer during an investigation
- Customer risk profile (CRP)
- Set up the risk score attributes
- Set the score bands
- Configuration history

6. Regulatory Reports
- The STR register
- Search and filter the register
- Open a filed STR
- Step 1: Select Alerts
- Step 2: Report Type
- Step 3: Reason for suspicion
- Step 4: Transaction
- Step 5: Subject parties
- Step 6: Narratives
- Where STRs come from
- The CTR register
- How CTRs are generated
- Find and download a CTR

7. Name Screening
- Watchlist Search
- Watchlist Entity Details
- Manual Screening
- Batch Screening
- Delta Screening
- Alert Configuration
- Screening Configuration
- Review a name-screening match

8. Transaction Monitoring
- Typology list
- Filter and sort the list
- Typology detail
- Schedule Details (a typology's run history)
- Create Typology form
- Variables list
- View Variable
- Create a variable
- Schedules: Run History
- Schedules: Schedule List
- Build a typology from scratch: walkthrough
- Part 1: Plan the rule
- Part 2: Create the variable
- Part 3: Create the typology
- Part 4: Add the conditions
- Part 5: Choose or create a schedule
- Part 6: Save as draft
- Part 7: Next: test and activate
- How conditions are evaluated: an example

9. Typology Library
- Building blocks
- Rule index
- Before you build
- Rule 1 · Structuring
- Rule 2 · Velocity
- Rule 3 · High value
- Rule 4 · Dormant account
- Rule 5 · Fan-out
- Rule 6 · Fan-in
- Rule 7 · Large single transaction
- Rule 8 · Smurfing
- Rule 9 · Spike against own history
- Rule 10 · Many devices
- Rule 11 · Many IP addresses
- Rule 12 · Many instruments
- Rule 13 · Many currencies
- Rule 14 · Many destination countries
- Rule 15 · Cross-border volume
- Test a typology with Dry Run
- Request Shadow activation
- Tuning and false positives
- Proposed typologies

10. Data Ingestion
- Batch Ingestion
- Filter batch jobs
- Investigate skipped rows
- Change the ingestion schedule
- Watchlist Ingestion
- Search, filter and sort watchlist files
- Upload an Internal Watchlist file

11. Maker Checker Approval
- Configs
- Search and filter activities
- Activity actions
- Create an activity
- Tickets
- Search and filter tickets
- Ticket statuses
- View a ticket

12. FAQ & Glossary
- Frequently Asked Questions
- Glossary
- Help & Support

13. Release Notes
- 2 November 2026
- 29 October 2026
- 8 October 2026
- 7 October 2026

GET STARTED

1 Getting Started

Fyscal ARCX is the anti-money laundering (AML) platform from Fyscal Technologies. Compliance teams use it to screen customers against watchlists, monitor transactions, investigate the resulting alerts and cases, and file Suspicious Transaction Reports (STRs). Read this chapter before you start: it shows how to sign in, move between modules, check your notifications, manage your own account, and find the chapter for the task you want to do.

FOR
Everyone: analysts, supervisors and administrators

READING TIME
About 12 min

How Fyscal ARCX fits together: see how data becomes alerts, cases and STRs, and where approvals come in.

Where to start, by role: follow a reading order that matches your work.

Signing in: open Fyscal ARCX with your email and password.

The Homepage and navigation: find each module in the sidebar menu.

Activity notifications: read and clear the notifications you receive while signed in.

The user menu: change your password or log out.

Changing your password: verify your account and set a new password.

Roles: understand why pickers and buttons can differ from one user to another.

How this guide is organised: find the chapter that covers each module.

How Fyscal ARCX fits together

Fyscal ARCX takes in customer, account, transaction and watchlist data, checks it, and raises alerts. Analysts work the alerts, group them into cases, record a decision and, where a case calls for it, file an STR. Diagram 1.1 shows this main path. Diagram 1.2 shows the approval lane that some changes, such as activating a typology, go through before they take effect.

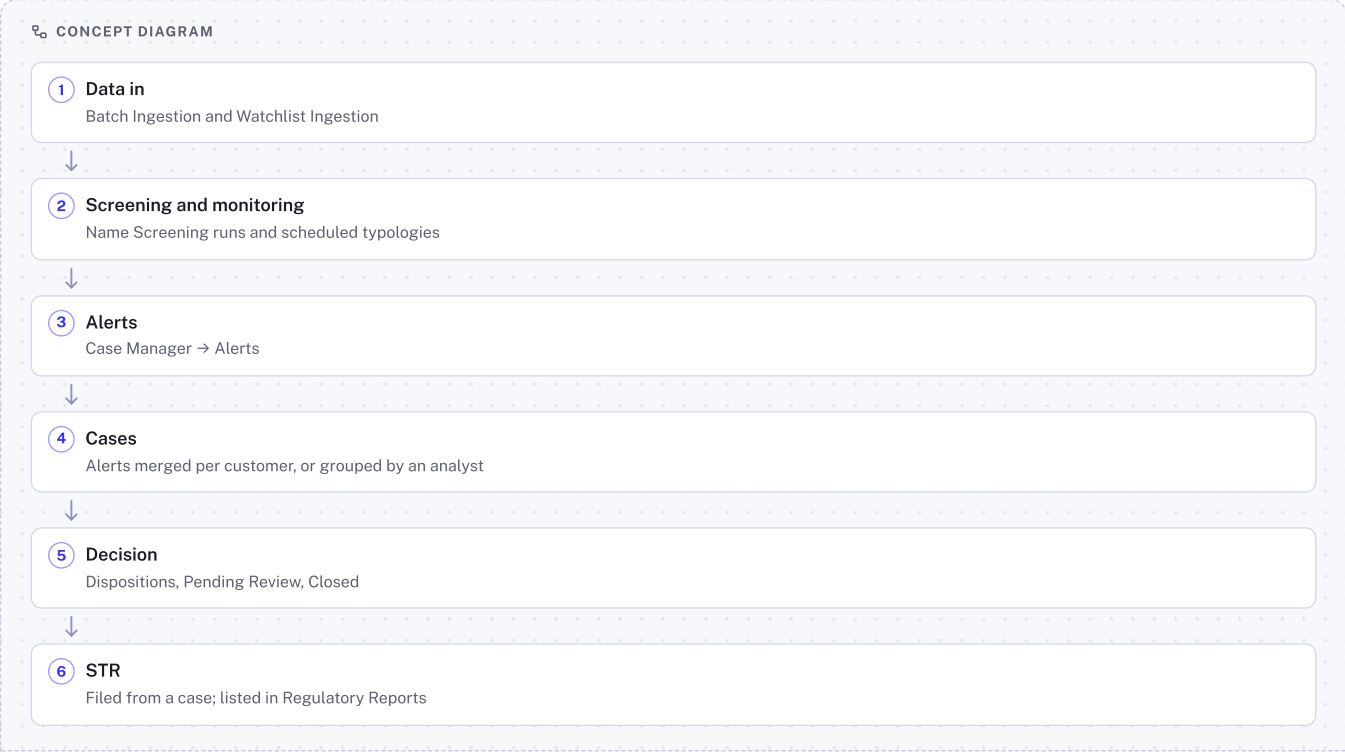


Diagram 1.1 — The main path: from data to alerts, cases and STRs

1. **Data in.** Batch Ingestion imports **Customers**, **Accounts** and **Transactions** files on a schedule. Watchlist Ingestion lists the watchlist files from **LSEG** and the **Internal Watchlist**.
2. **Screening and monitoring.** Name Screening compares customers with the watchlists; each Batch Screening and Delta Screening run shows the **Alerts Created**. Transaction Monitoring runs typologies (rules) on schedules against the transaction data.
3. **Alerts.** Both modules raise alerts into Case Manager → Alerts: Name Screening alert IDs start **ALT-NS**, Transaction Monitoring alert IDs **ALT-TMS**.
4. **Cases.** Case Creation & Assignment merges alerts into cases ("based on customer ID, case age, and status", as its banner states) and assigns them. An analyst can also use **Group into Case** on an alert or Add Alerts on a case. Customer 360 and Watchlist Search support the investigation.
5. **Decision.** The analyst records a disposition for each alert and for the case (Dispose alerts and close a case). A case can wait in **Pending Review** for a reviewer (Review a case in Pending Review) before it is **Closed**.
6. **STR.** From a case, **File STR** opens the six-step STR wizard (File an STR). Cases with an STR show the status **STR Draft** or **STR Created**, and a filed report appears in Regulatory Reports.

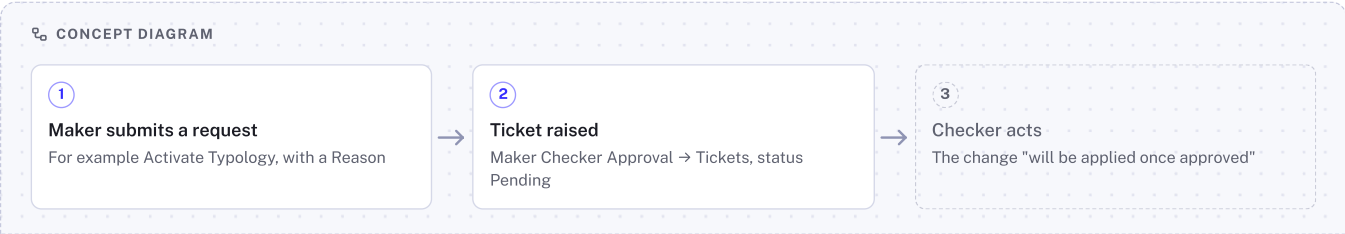


Diagram 1.2 — The approval side lane: changes that need a second person
Dashed items are steps not shown in this guide's screenshots.

The approval lane sits beside the main path. When you activate a typology, Fyscal ARCX asks for a **Reason** and confirms "Submitted for governance review (ticket …). It will be applied once approved." The typology stays **Draft** while the request waits (see Request Shadow activation). In **Shadow Mode** its alerts are shown on the rule's page; in **Published Mode** they "flow into Alert Manager". The activities that need approval, and their rules, are listed in Configs; the requests are in Tickets.

> **AML context**
> Screening asks who a customer is: does the name match a sanctioned person, a politically exposed person or another name of concern? Monitoring asks what the customer does: does their activity fit a known money-laundering pattern? Both lead to investigation, and activity found to be suspicious is reported to the financial intelligence unit.

Each kind of record has its own ID format:

Record	ID starts with	Example in this guide
Name Screening alert	**ALT-NS**	ALT-NS-05102026-000115
Transaction Monitoring alert	**ALT-TMS**	ALT-TMS-21072026-041467
Case	**CASE-**	CASE-2026-0034617
Customer	**CUST-**	CUST-FYSCAL-604554
Typology (rule)	**TMR-**	TMR-06102026-001090
Variable	**VAR-**	VAR-07102026-000736
Schedule (Transaction Monitoring)	**SCH-**	SCH-07102026-000397

Where to start, by role

Each path below lists the sections to read first for one kind of work, in the order you are likely to need them. If you are new to the platform, read How Fyscal ARCX fits together first. Your administrator decides what you can access, so some screens or buttons in a path may not be available to you (see Roles).

Investigating alerts and cases

For analysts who work alerts and cases.

1. The Homepage and navigation: find each module in the sidebar menu.
2. How Fyscal ARCX fits together: see where alerts come from and where a case can end.
3. Alerts list: find the alerts in your **My Queue**.
4. Work an alert: take an alert from **Not Started** to a decision.
5. Cases list: find the cases in your **My Queue**.
6. Case Details: see a case's alerts, customer and evidence.
7. The Customer Profile: check everything held on the customer.
8. Timeline and notes: add case notes and read what happened to the case.
9. Dispose alerts and close a case: record a disposition for each alert and for the case.

Reviewing and filing

For supervisors and team leads who review cases and file STRs.

1. Daily triage from the dashboard: check overdue, escalated and pending work and the daily jobs, then open the matching lists.
2. Case statuses and dispositions: know what each case status means.
3. Review a case in Pending Review: list the cases waiting for review and act on them.
4. Reopen a case: reopen a case in **Closed**, **STR Draft** or **STR Created**.
5. File an STR: prepare a Suspicious Transaction Report for the AMLC from a case.
6. After the STR is filed: download the STR and find it in Regulatory Reports.
7. The STR register: find and open filed STRs.

Configuring the platform

For administrators who set up screening, typologies, ingestion, assignment and approvals.

1. Team Management: the hierarchy list: set up hierarchies, their roles and members.
2. Case Creation & Assignment: Active Configuration: see which alert types become cases and who they are assigned to.
3. Alert Assignment: choose the alert types to assign and the people they go to.
4. Screening Configuration: set the weightage of each screening field.
5. Alert Configuration: set the alert bands that screening uses.
6. Build a typology from scratch: walkthrough: create a Transaction Monitoring rule from variable to saved draft.
7. Test a typology with Dry Run: see how many alerts a draft would have created on past records.
8. Request Shadow activation: send a tested rule for approval in Shadow Mode.
9. Batch Ingestion: confirm that customer, account and transaction files were imported.
10. Configs and Tickets: see which actions need approval, and follow the requests you have raised.

Signing in

Platform URL → Sign in

Use the sign-in page to open Fyscal ARCX with your account email and password. It is titled **Welcome back**, with the instruction **Enter your email and password to access your account.** It has two fields, **Email** and **Password**, a **Sign in** button and a **Forgot password?** button.

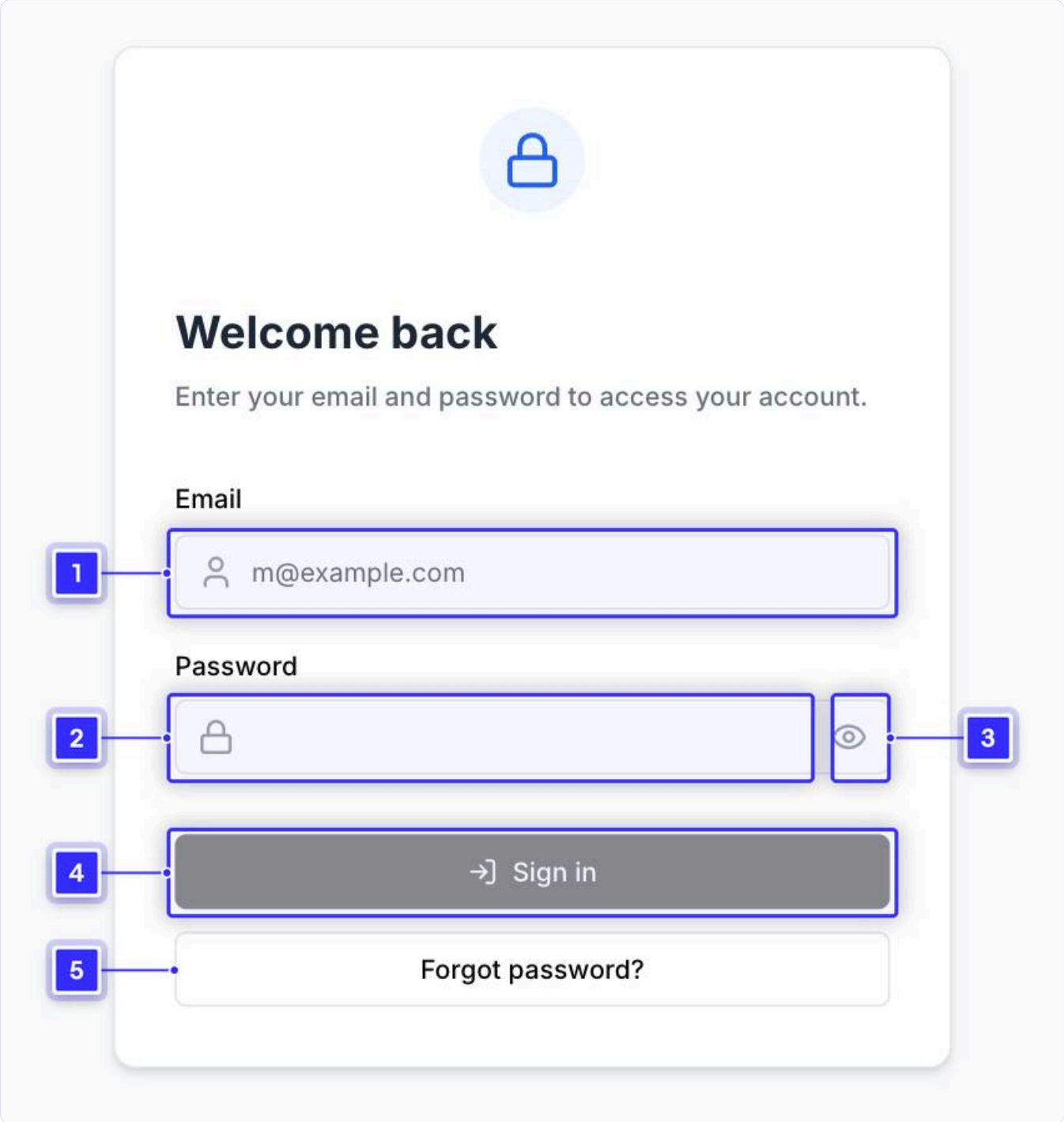


Figure 1.1 The sign-in page: Email (1), Password (2) with the eye icon (3), Sign in (4) and Forgot password? (5)

Field or control	What it expects or does
Email (1)	The email address of your Fyscal ARCX account. The placeholder reads **m@example.com**.
Password (2)	Your password. The eye icon (3) at the right of the field shows or hides the characters you type.
Sign in (4)	Submits your email and password.
Forgot password? (5)	Use it if you cannot sign in with your current password.

Step 1 **Open the platform**

Go to the Fyscal ARCX URL your institution has given you. The **Welcome back** page opens.

Step 2 **Enter your email**

Type your account email address in **Email**.

Step 3 **Enter your password**

Type your password in **Password**. Click the eye icon if you want to check what you typed.

Step 4 **Sign in**

Click **Sign in**. If you cannot sign in, click **Forgot password?**.

The Homepage and navigation

Platform → Homepage

Use the sidebar to move between modules; this section shows where each menu leads. The **Homepage** shows **Welcome** followed by your name. Every module is opened from the sidebar on the left. The sidebar groups its menus under **Platform**; menus with a chevron (›) expand to show their pages, and the page you are on is highlighted.

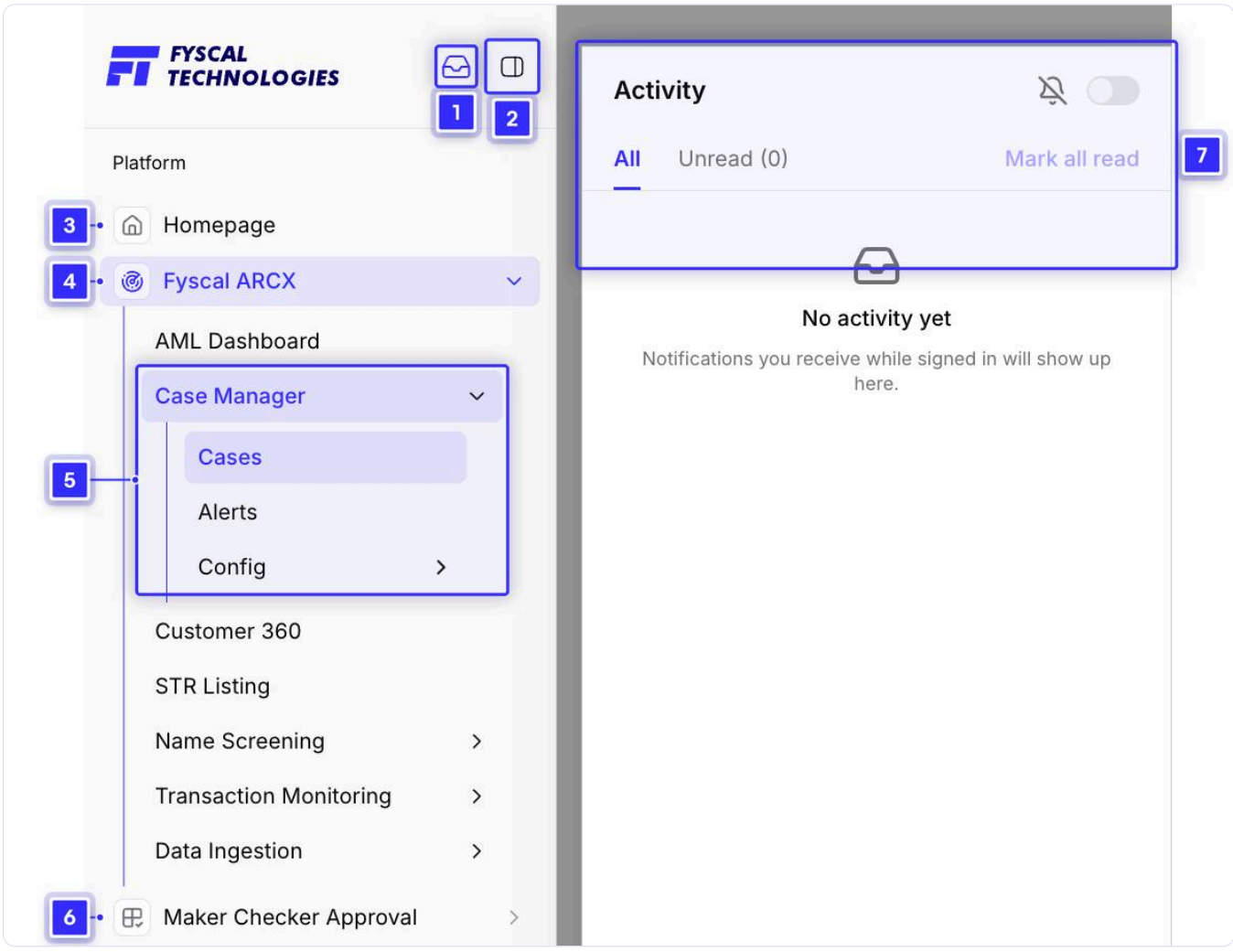


Figure 1.2 The sidebar with Fyscal ARCX and Case Manager expanded (1 to 6), and the Activity panel open (7)

1. **Activity** (inbox icon): opens the Activity notifications panel. See Activity notifications.
2. **Toggle Sidebar**: collapses the sidebar to a narrow rail, or expands it again.
3. **Homepage**: returns to the welcome page.
4. **Fyscal ARCX**: the AML modules described in this guide.
5. **Case Manager**, expanded to show **Cases**, **Alerts** and **Config**.
6. **Maker Checker Approval**: the approval menu.
7. The **Activity** panel.

The full menu is:

Menu	Pages	Chapter
Homepage	Welcome page	This chapter
Fyscal ARCX	**AML Dashboard**	AML Dashboard
	Case Manager → Cases, Alerts, Config	Case Manager, Case Manager Config
	Customer 360	Customer 360
	Regulatory Reports	Regulatory Reports
	Name Screening → Watchlist Search, Manual Screening, Batch Screening, Delta Screening, Configuration	Name Screening
	Transaction Monitoring → Schedules, Typology, Variables	Transaction Monitoring
	Data Ingestion → Batch Ingestion, Watchlist Ingestion, TMS	Data Ingestion
Maker Checker Approval	**Configs, Tickets**	Maker Checker Approval

Each page shows its title at the top with a breadcrumb beneath it, for example **Fyscal ARCX › AML Dashboard**. Your name and email are shown at the bottom of the sidebar; click them to open the user menu.

Activity notifications

Sidebar header → Activity (inbox icon)

The **Activity** panel lists notifications you receive while signed in. It opens over the current page, so you can check it from any screen (Figure 1.2, area 7).

Control	What it does
Enable notifications (bell icon and switch)	Turns notifications on or off. The switch is off in Figure 1.2.
All	Tab showing every notification.
Unread (0)	Tab showing unread notifications; the number in brackets is the unread count.
Mark all read	Marks every notification as read.

When there is nothing to show, the panel reads **No activity yet**: **Notifications you receive while signed in will show up here.**

Step 1 **Open the Activity panel**

Click the inbox icon at the top of the sidebar, next to the Fyscal Technologies logo. The **Activity** panel opens on the **All** tab.

Step 2 **Show unread notifications only**

Click **Unread**.

Step 3 **Clear the unread count**

Click **Mark all read**.

The user menu

Sidebar footer → your name

Open the user menu when you want to change your password or log out. The block at the bottom of the sidebar shows your initials, name and email address (the email is partly masked). Click it to open the user menu, which repeats your name and email and offers two actions.

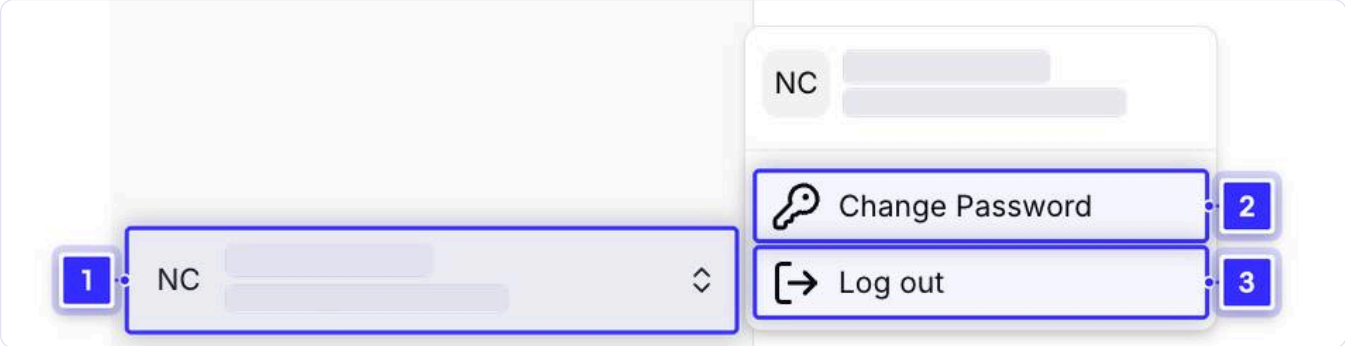


Figure 1.3 The user menu: your name and email (1, hidden in the figure), Change Password (2) and Log out (3)

- Your name and email (1): the block at the bottom of the sidebar that opens the menu.
- **Change Password** (2): opens the Change Password page. See Changing your password.
- **Log out** (3): signs you out of Fyscal ARCX.

Changing your password

User menu → Change Password

Follow these steps when you want to replace your current password. Before you can set a new password, the **Verify Your Account** page asks you to confirm who you are: **Enter your email and current password to continue with the password change process**.

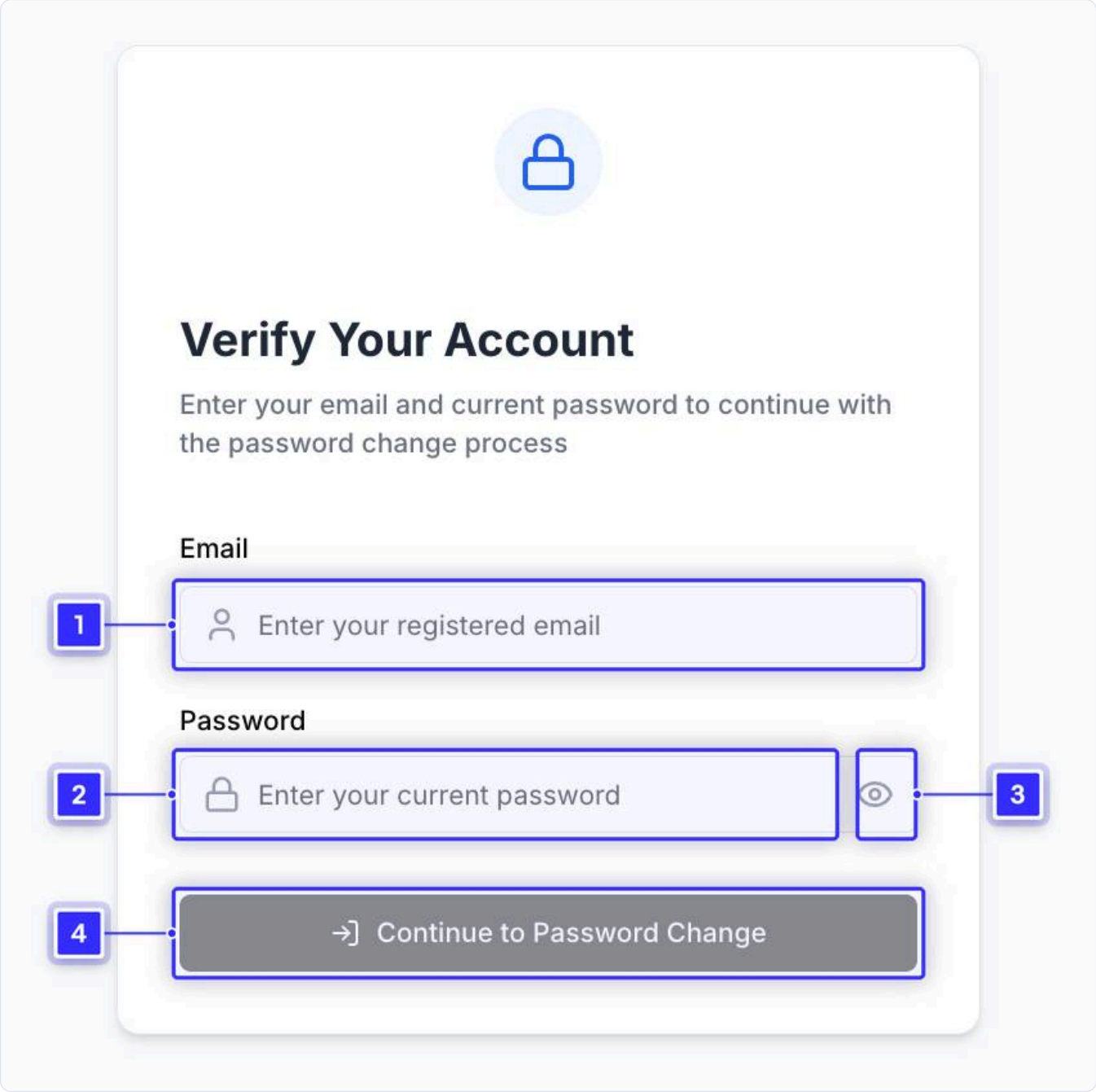


Figure 1.4 Change Password, Verify Your Account: Email (1), Password (2) with the eye icon (3) and Continue to Password Change (4)

Field or control	What it expects or does
Email (1)	Placeholder **Enter your registered email**: the email address of your account.
Password (2)	Placeholder **Enter your current password**. The eye icon (3) shows or hides the characters.
Continue to Password Change (4)	Verifies your email and current password and continues the password change. The button is greyed out while the fields are empty.

Step 1 **Open the user menu**

Click your name at the bottom of the sidebar.

Step 2 **Choose Change Password**

Click **Change Password**. The **Verify Your Account** page opens.

Step 3 **Verify your account**

Enter your registered email in **Email** and your current password in **Password**.

Step 4 **Continue**

Click **Continue to Password Change** and follow the on-screen instructions to set your new password.

Roles

Read this section if a picker or button you see in the guide looks different for you. Roles are defined per hierarchy in Case Manager → Config → Team Management. The AML hierarchy there has four levels: **AML Admin**, **AML Team Lead**, **AML Supervisor** and **AML Analyst**.

Some pickers and actions depend on the permissions of the signed-in user. For example, the list of people you can choose in an assignee picker, and whether a button is available to you, can differ from one user to another.

How this guide is organised

Use this list to find the chapter for the module you are working in.

- AML Dashboard: alert and case metrics, distribution charts and daily job outcomes.
- Case Manager: working cases and alerts.
- Case Manager Config: case creation and assignment, alert assignment, Agentic Workflows and Team Management.
- Customer 360: customer profiles and their history.
- Regulatory Reports: filed Suspicious Transaction Reports (STR tab) and automatically created Covered Transaction Reports (CTR tab).
- Name Screening: watchlist search, manual, batch and delta screening, and screening configuration.
- Transaction Monitoring: typologies, variables and schedules.
- Typology Library: reference typologies.
- Data Ingestion: batch ingestion and watchlist ingestion.
- Maker Checker Approval: approval configs and tickets.
- FAQ & Glossary: frequently asked questions, definitions of every term, and how to contact support.
- Release Notes: changes by release.

RELATED IN GET STARTED

AML Dashboard

GET STARTED

2 AML Dashboard

Fyscal ARCX → AML Dashboard

The AML Dashboard gives a single view of the alert and case workload. Analysts and reviewers use it to see how many alerts and cases are overdue, unassigned, escalated or pending, and how they are distributed by status, disposition, score, type, assignment and age. It also shows STRs filed over time and whether each day's screening, monitoring and ingestion jobs succeeded.

FOR	IN THE MENU	READING TIME
Analysts, supervisors and team leads	Fyscal ARCX → AML Dashboard	About 12 min

Dashboard layout: find each area of the page and see which charts each view shows.

Metric tiles: check the headline counts of overdue, unassigned, escalated and pending work.

Case Distribution controls: switch between cases and alerts and set the period the charts cover.

By Status: see how records are spread across statuses.

By Disposition (Closed): see how closed records were dispositioned.

By Score and By Type (Alerts view): break alerts down by score band and alert type.

By Assignment: see how much work is unassigned and who holds the rest.

STR Filed: follow the number of STRs filed per month.

By Age: see how many records fall in each age bucket.

Pending Review, Avg. Handling and Reopens: read three summary figures for cases.

Daily Jobs: check whether each scheduled job ran and succeeded.

Team Performance: find the link to team performance figures.

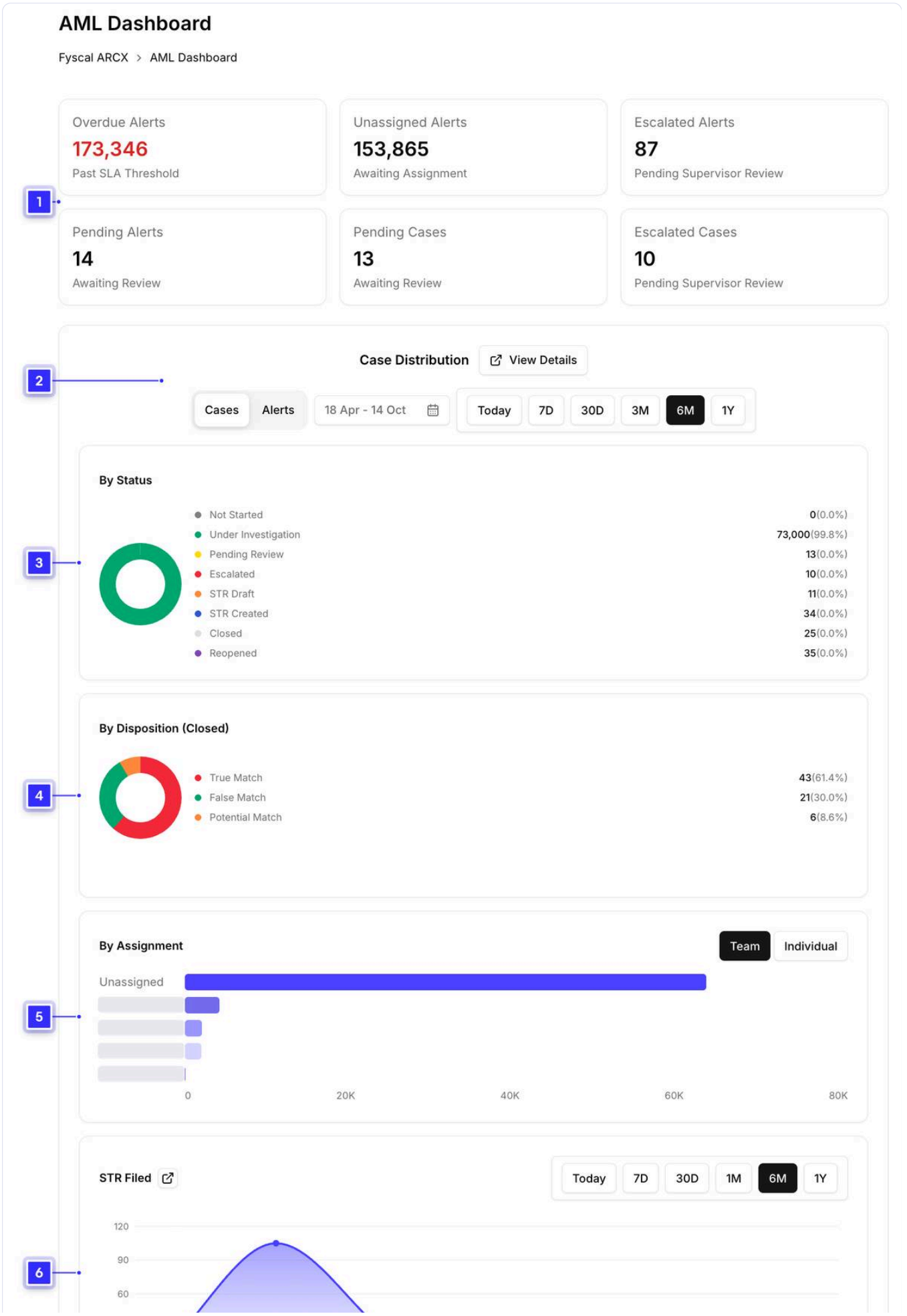
Daily triage from the dashboard: a short routine that goes from each tile to the list where you work it.

Dashboard layout

Fyscal ARCX → AML Dashboard

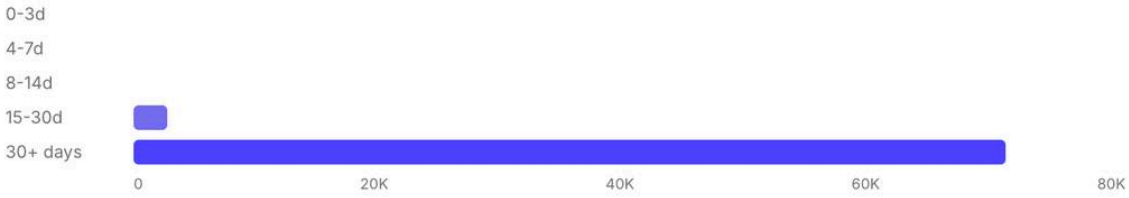
WHO	WHERE	VIEWS	WORK IT IN
Analysts, supervisors and team leads	Fyscal ARCX → AML Dashboard	Cases or Alerts, over a period you choose	Case Manager → Alerts or Cases

Use this overview to find each area of the dashboard before you read a chart. Open **Fyscal ARCX** in the sidebar and click **AML Dashboard**. The page is titled **AML Dashboard**, with the breadcrumb **Fyscal ARCX › AML Dashboard**. Scroll down to see every area. Figure 2.1 shows the whole page in the **Cases** view with the range set to **6M** (**18 Apr - 14 Oct**).


AML Dashboard
Fyscal ARCX > AML Dashboard
Overdue Alerts
173,346
Past SLA Threshold
Unassigned Alerts
153,865
Awaiting Assignment
Escalated Alerts
87
Pending Supervisor Review
1
Pending Alerts
14
Awaiting Review
Pending Cases
13
Awaiting Review
Escalated Cases
10
Pending Supervisor Review
Case Distribution
View Details
2
Cases
Alerts
18 Apr - 14 Oct
Today
7D
30D
3M
6M
1Y
By Status
3
Not Started 0(0.0%)
Under Investigation 73,000(99.8%)
Pending Review 13(0.0%)
Escalated 10(0.0%)
STR Draft 11(0.0%)
STR Created 34(0.0%)
Closed 25(0.0%)
Reopened 35(0.0%)
By Disposition (Closed)
4
True Match 43(61.4%)
False Match 21(30.0%)
Potential Match 6(8.6%)
By Assignment
Team
Individual
5
Unassigned
0
20K
40K
60K
80K
STR Filed
Today
7D
30D
1M
6M
1Y
6
120
90
60



By Age



7

Pending Review	Avg. Handling	Reopens
13	6.3d	218

8

Daily Jobs

Screening & Monitoring Runs

Job	14 Oct	13 Oct	12 Oct	11 Oct	10 Oct	9 Oct	8 Oct
Batch Screening	(96.6K)	—	—	—	—	x3 (3K)	—
Delta Screening	—	—	—	—	—	—	—
TM Runs	x2 (0)	x6 (263.6K)	x4 (0)	x2 (0)	x4 (0)	x2 (0)	x4 (5.5K)

9

Data Ingestion

Job	14 Oct	13 Oct	12 Oct	11 Oct	10 Oct	9 Oct	8 Oct
Customers	(100K)	x4 (0)	(0)	—	—	x8 (33K)	x8 (0)
Accounts	(150K)	—	—	—	—	x6 (24.7K)	—
Transactions	(422.8K)	x4 (17M)	(5M)	—	—	x7 (10.3M)	x12 (14M)
Watchlist	x2 (9.6K)	x2 (9.3K)	x2 (22)	x2 (2.8K)	x2 (9.9K)	x2 (10.1K)	x2 (8K)

Team Performance

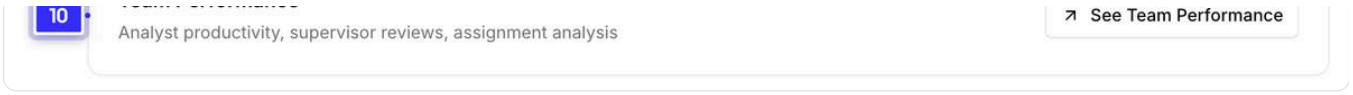


Figure 2.1 The AML Dashboard in the Cases view, with its areas numbered 1 to 10

1. **Metric tiles**: six headline counts for alerts and cases. See Metric tiles.
2. **Case Distribution** header and controls: **View Details**, the **Cases** / **Alerts** switch, the date range picker and the range presets. See Case Distribution controls.
3. **By Status**. See By Status.
4. **By Disposition (Closed)**. See By Disposition (Closed).
5. **By Assignment**, with the **Team** / **Individual** switch. See By Assignment.
6. **STR Filed** (Cases view only). See STR Filed.
7. **By Age**. See By Age.
8. **Pending Review**, **Avg. Handling** and **Reopens** tiles (Cases view only). See Pending Review, Avg. Handling and Reopens.
9. **Daily Jobs**: **Screening & Monitoring Runs** and **Data Ingestion**. See Daily Jobs.
10. **Team Performance**. See Team Performance.

Areas 3 to 8 sit inside the distribution panel and change with the **Cases** / **Alerts** switch. In the **Alerts** view the panel is titled **Alert Distribution** and shows these charts, in order:

Chart or tile	Cases view	Alerts view
By Status	Yes	Yes
By Disposition (Closed)	Yes	Yes
By Score	No	Yes
By Type	No	Yes
By Assignment	Yes	Yes
STR Filed	Yes	No
By Age	Yes (case age buckets)	Yes (alert age buckets)
Pending Review, **Avg. Handling**, **Reopens**	Yes	No

The metric tiles, **Daily Jobs** and **Team Performance** appear in both views.

> **Note**
> The counts in this chapter are example values from the test environment where the screens were captured. Some of them do not add up across charts (for example, in the Cases view **By Status** shows 25 **Closed** cases, while **By Disposition (Closed)** adds up to 70), so read them as examples of the layout, not as figures to reconcile.

Metric tiles

Use the metric tiles for a quick count of the alerts and cases that are overdue, unassigned, escalated or pending. Six tiles at the top of the page each show a label, a count and a sub-label. The **Overdue Alerts** count is shown in red.



Figure 2.2 The six metric tiles, numbered 1 to 6

Tile	Sub-label	Value in **Figure 2.2**
Overdue Alerts (1)	Past SLA Threshold	173,346
Unassigned Alerts (2)	Awaiting Assignment	153,865
Escalated Alerts (3)	Pending Supervisor Review	87
Pending Alerts (4)	Awaiting Review	14
Pending Cases (5)	Awaiting Review	13
Escalated Cases (6)	Pending Supervisor Review	10

The tiles are counts only. To work the alerts or cases behind a tile, open the list in Case Manager. The table shows where each count can be found again. In the captures, the chip counts on the **All Alerts** and **All Cases** tabs matched the tiles.

Tile	Where to work it	Matching count in the captures
Overdue Alerts	Case Manager → Alerts → **All Alerts**. Click **Show Filters** and set **SLA** to **Breached** (Alerts list).	Chip **SLA Breached** 173346 = tile 173,346
Unassigned Alerts	Case Manager → Alerts → **All Alerts**. The **Unassigned** chip shows the count (Alerts list).	Chip **Unassigned** 153888, tile 153,865 (the two counts differ)
Escalated Alerts	Case Manager → Alerts → **All Alerts**. Set **Status** to **Escalated**.	Chip **Escalated** 87 = tile 87
Pending Alerts	Case Manager → Alerts → **All Alerts**. Set **Status** to **Pending Review**.	No matching chip
Pending Cases	Case Manager → Cases → **All Cases**, chip **Pending Approval**, which sets **Status** to **Pending Review** (Filter and search cases). Act on each case as in Review a case in Pending Review.	Chip **Pending Approval** 13 = tile 13
Escalated Cases	Case Manager → Cases → **All Cases**. Click **Show Filters** and set **Status** to **Escalated** (Filter and search cases).	Chip **Escalated** 10 = tile 10

AML context

An alert that nobody is working is a risk that nobody is managing. Overdue and unassigned counts show where the backlog is, and escalations show where a senior judgement is waiting. Teams often review these counts at the start of each day.

Case Distribution controls

Use these controls before reading the charts below: they set whether the charts count cases or alerts, and over which period. The distribution panel has its own header and controls.

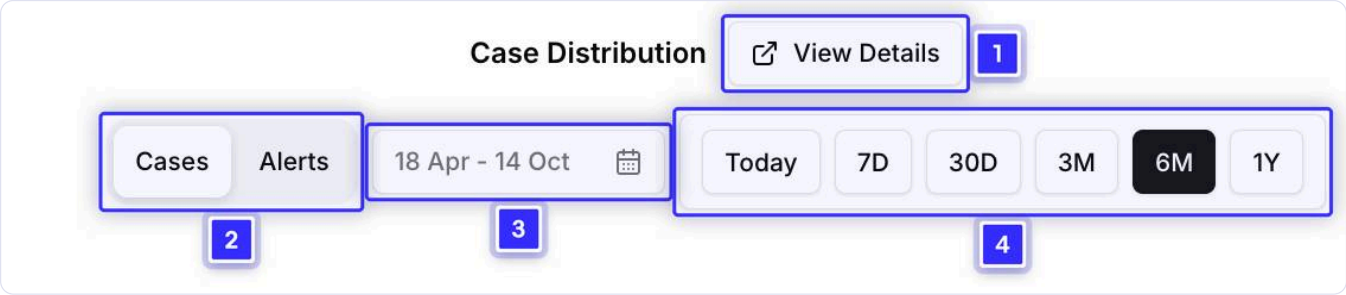


Figure 2.3 Case Distribution controls: View Details (1), the Cases / Alerts switch (2), the date range (3) and the range presets (4)

1. **View Details**: in the Cases view, opens the Cases list in Case Manager.
2. **Cases** / **Alerts**: switches the panel between cases (**Case Distribution**) and alerts (**Alert Distribution**). The selected option is shown in white.
3. Date range picker: shows the period the charts cover, for example **18 Apr - 14 Oct**, with a calendar icon at the right. When the page was opened for these captures, it showed **8 Oct - 14 Oct**.
4. Range presets: **Today**, **7D**, **30D**, **3M**, **6M** and **1Y**. The selected preset is shown in black; in Figure 2.3 it is **6M**, which sets the range to **18 Apr - 14 Oct**.

Step 1 **Choose cases or alerts**

Click **Cases** or **Alerts**. The panel title changes to **Case Distribution** or **Alert Distribution** and the charts redraw.

Step 2 **Set the period**

Click a preset such as **30D**. The date range picker updates to show the new period.

Step 3 **Open the underlying list**

In the Cases view, click **View Details** to open the Cases list.

By Status

Use By Status to see how cases or alerts are spread across statuses. It is a donut chart with a legend that gives, for each status, the count and its share of the total in brackets.

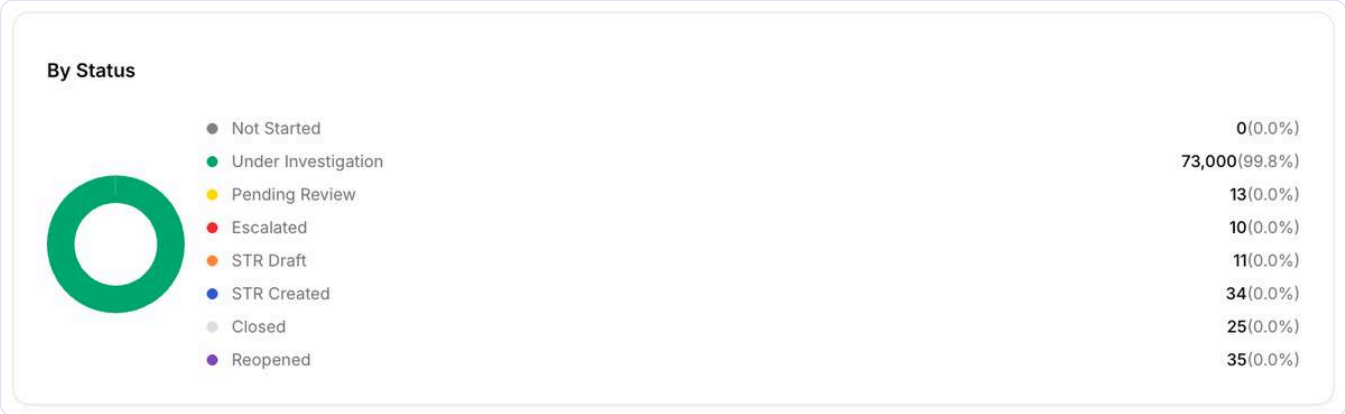


Figure 2.4 By Status in the Cases view, range 6M

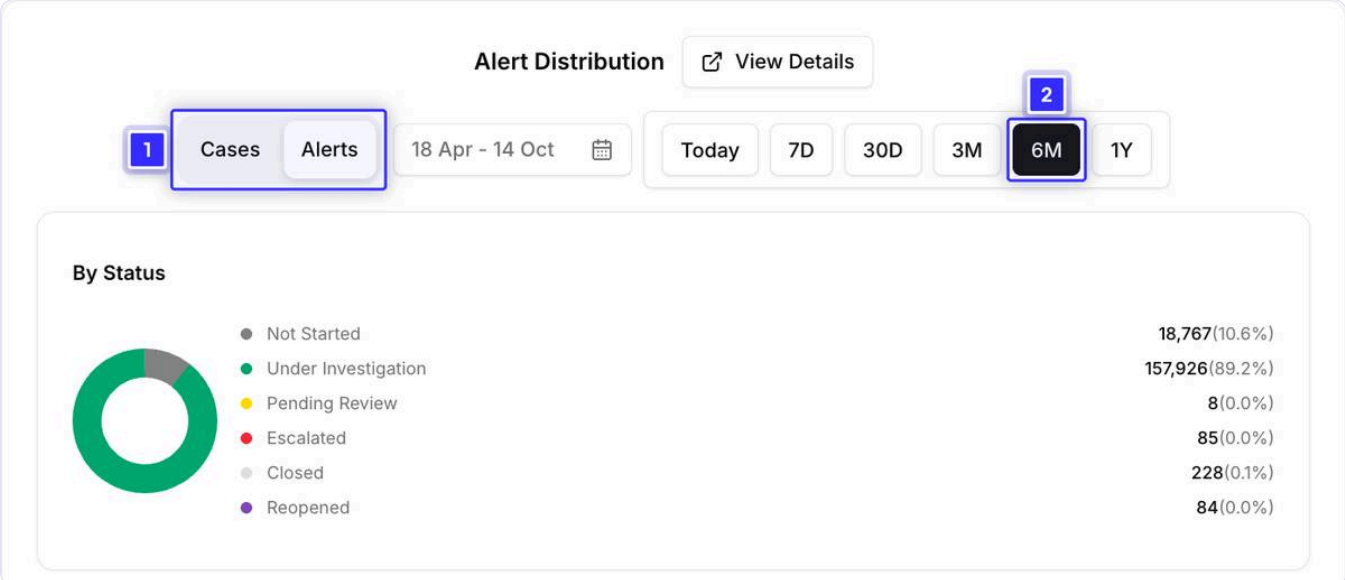


Figure 2.5 Alert Distribution: the switch on Alerts (1), the range set to 6M (2) and By Status

Status	Cases view (Figure 2.4)	Alerts view (Figure 2.5)
Not Started	0 (0.0%)	18,767 (10.6%)
Under Investigation	73,000 (99.8%)	157,926 (89.2%)
Pending Review	13 (0.0%)	8 (0.0%)

Status	Cases view (Figure 2.4)	Alerts view (Figure 2.5)
Escalated	10 (0.0%)	85 (0.0%)
STR Draft	11 (0.0%)	Not shown
STR Created	34 (0.0%)	Not shown
Closed	25 (0.0%)	228 (0.1%)
Reopened	35 (0.0%)	84 (0.0%)

Cases have eight statuses and alerts six: **STR Draft** and **STR Created** apply to cases only. The statuses are described in Case Manager.

By Disposition (Closed)

Use this chart to see how closed cases or alerts were dispositioned. It is a donut chart of closed records by disposition: **True Match**, **False Match** and **Potential Match**, each with its count and share.

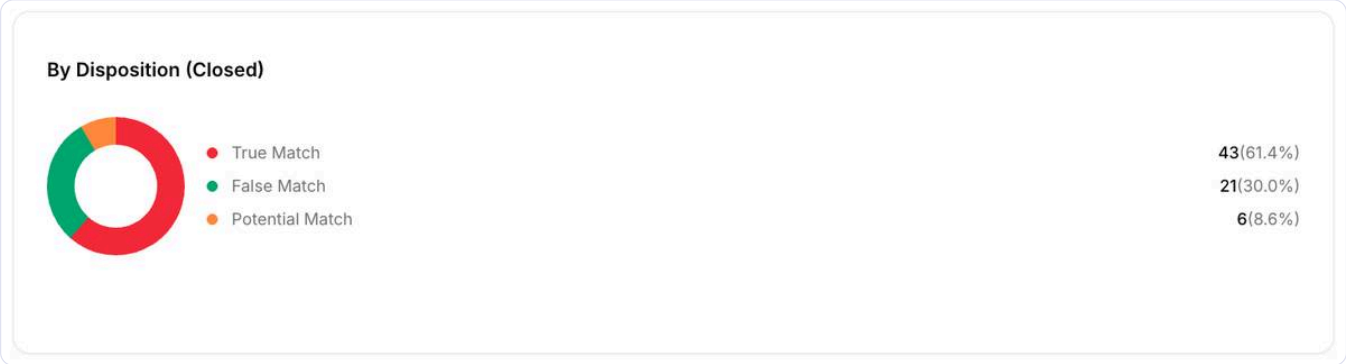


Figure 2.6 By Disposition (Closed) in the Cases view, range 6M

Disposition	Cases view	Alerts view
True Match	43 (61.4%)	113 (49.6%)
False Match	21 (30.0%)	97 (42.5%)
Potential Match	6 (8.6%)	18 (7.9%)

By Score and By Type (Alerts view)

Use these charts to break alerts down by score band and by alert type. They appear only in the **Alerts** view, between **By Disposition (Closed)** and **By Assignment**.

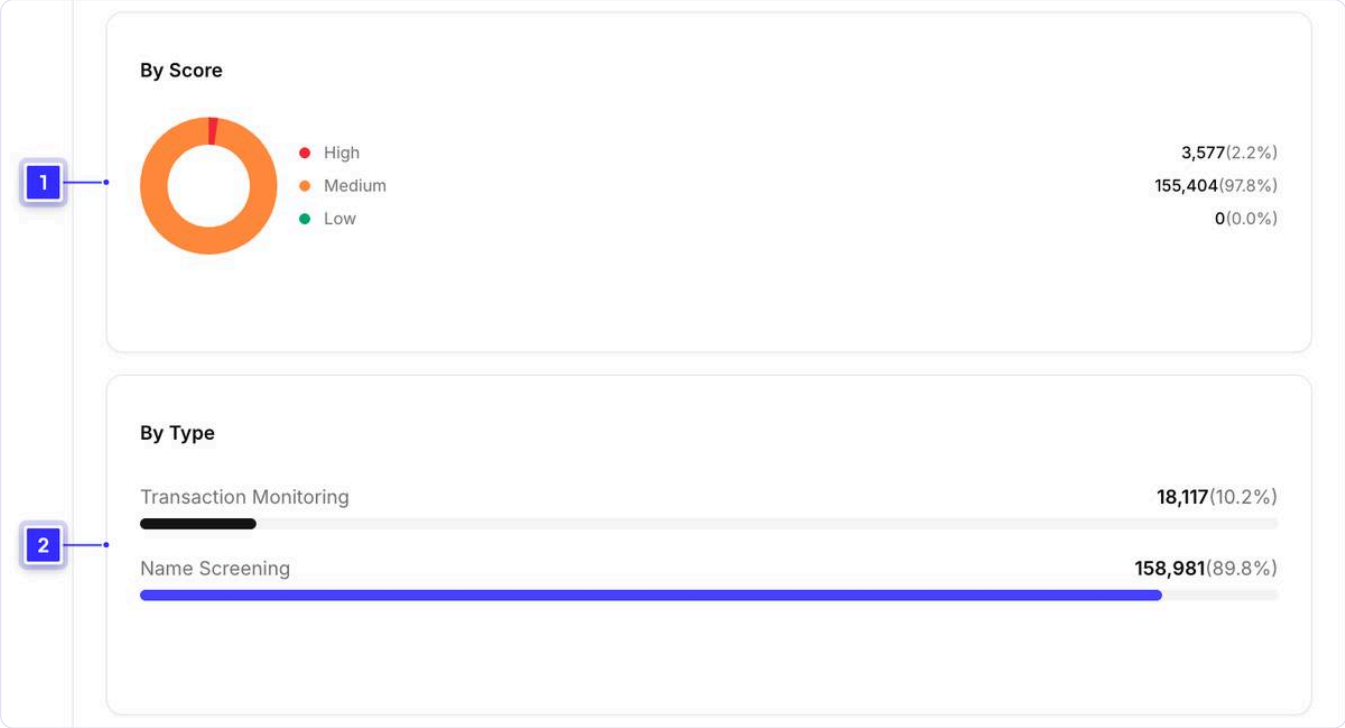


Figure 2.7 By Score (1) and By Type (2) in the Alerts view

- **By Score** (1): a donut chart of alerts by score band, **High**, **Medium** and **Low**, each with its count and share. In Figure 2.7: High 3,577 (2.2%), Medium 155,404 (97.8%), Low 0 (0.0%).
- **By Type** (2): a horizontal bar for each alert type, with its count and share at the right. In Figure 2.7: **Transaction Monitoring** 18,117 (10.2%) and **Name Screening** 158,981 (89.8%).

By Assignment

Use By Assignment to see how many records are unassigned and how the rest are spread across assignees. It is a horizontal bar chart of records by assignee. The first bar is **Unassigned** (1); the other bars are named users. Names are hidden in this guide.

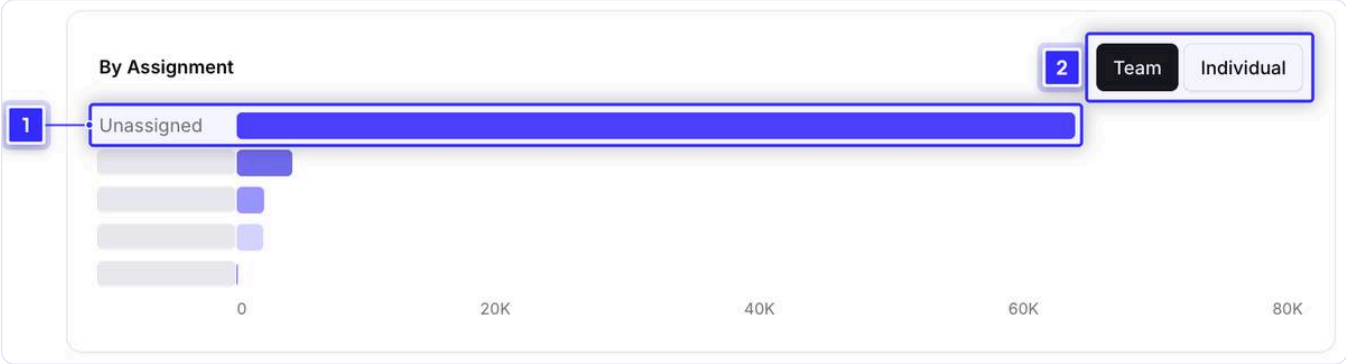


Figure 2.8 By Assignment: the Unassigned bar (1) and the Team / Individual switch (2); user names hidden

The **Team** / **Individual** switch (2) at the top right changes the grouping. **Team** is selected (shown in black) in Figure 2.8. The horizontal axis scale follows the counts; in Figure 2.8 it runs from 0 to 80K.

STR Filed

Use STR Filed to follow the number of STRs filed per month. It is shown in the **Cases** view only: a line chart of STRs filed per month, with its own range presets **Today**, **7D**, **30D**, **1M**, **6M** and **1Y** at the top right (2). The title carries a link icon (1). In Figure 2.9 the **6M** preset is selected and the chart runs from **Apr '26** to **Sep**.

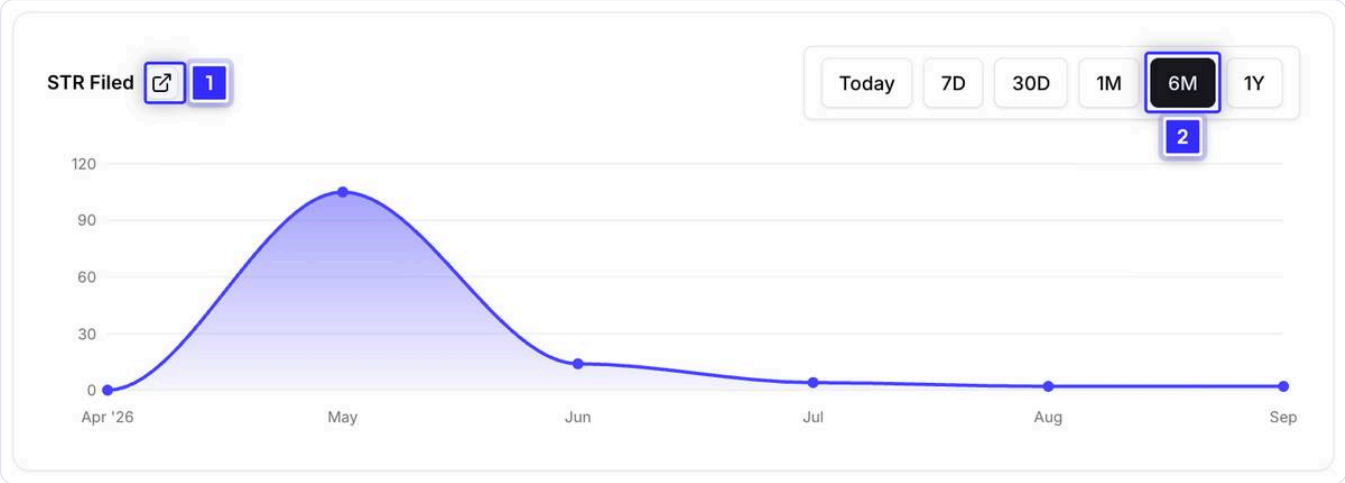


Figure 2.9 STR Filed: the link icon (1) and its own range presets, with 6M selected (2)

For the filed reports themselves, see Regulatory Reports.

By Age

Use By Age to see how many records fall in each age bucket. It is a horizontal bar chart of records by age bucket. The buckets differ between the two views:

View	Age buckets
Cases	0-3d, 4-7d, 8-14d, 15-30d, 30+ days
Alerts	0-24h, 1-3d, 4-7d, 8-14d, 14+ days



Figure 2.10 By Age (1), followed by the Pending Review (2), Avg. Handling (3) and Reopens (4) tiles (Cases view)

Pending Review, Avg. Handling and Reopens

Use these tiles for three summary figures on cases: how many are pending review, the average handling time and the number of reopens. In the **Cases** view, three tiles close the distribution panel (Figure 2.10):

Tile	Value in **Figure 2.10**
Pending Review (2)	13
Avg. Handling (3)	6.3d (days)
Reopens (4)	218

Daily Jobs

Check **Daily Jobs** to see, day by day, whether the screening, monitoring and ingestion jobs ran and succeeded. It shows the outcome of the platform's scheduled jobs. It has two blocks: **Screening & Monitoring Runs** and **Data Ingestion**.

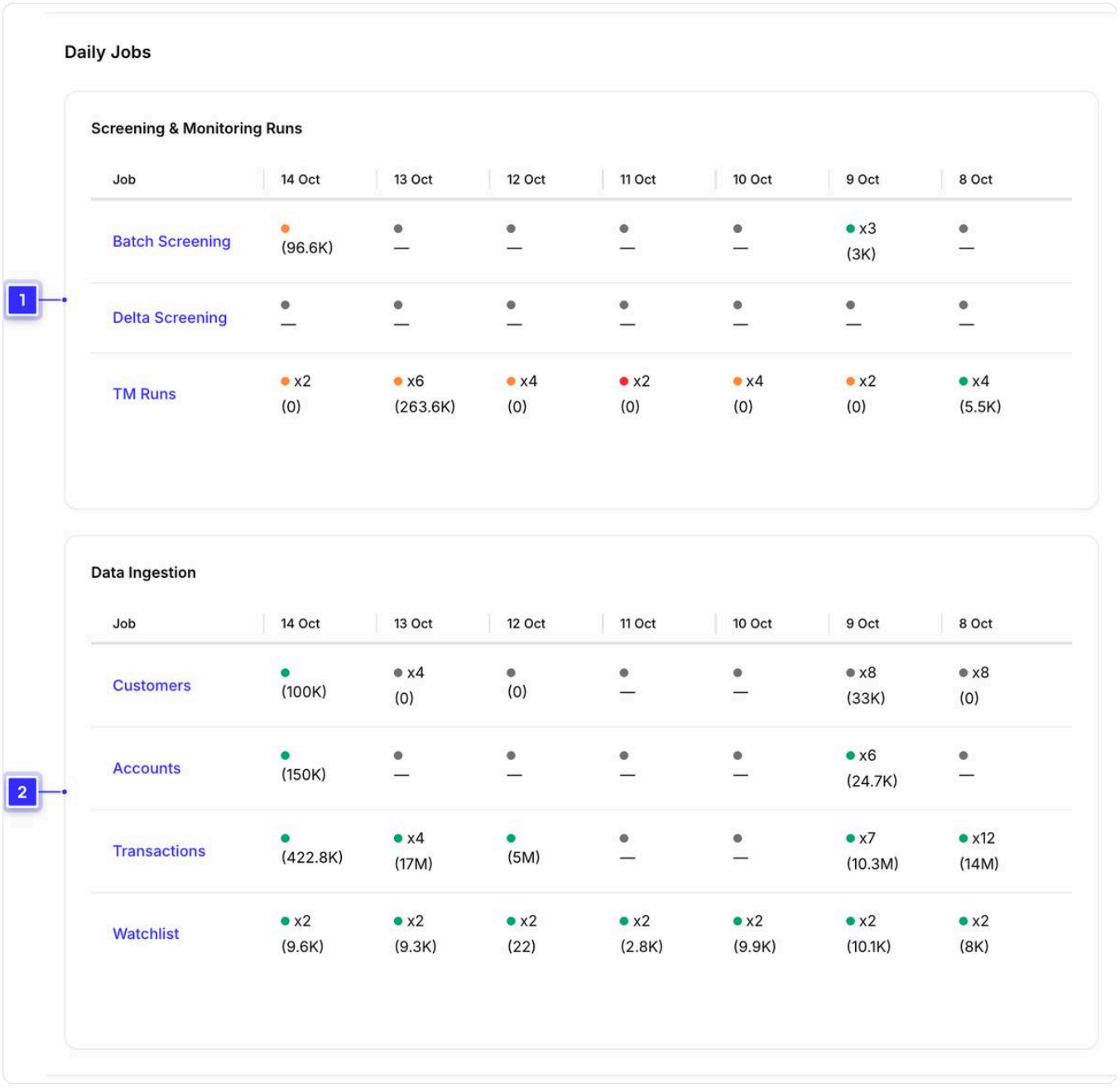


Figure 2.11 Daily Jobs: Screening & Monitoring Runs (1) and Data Ingestion (2), from 14 Oct back to 8 Oct

Both blocks are grids with one row per job and one column per day, newest first. The day columns in Figure 2.11 run from **14 Oct** back to **8 Oct**. The first column, **Job**, shows the job name as a link (shown in blue) to the screen where the job is managed.

Block	Jobs (rows)	Related chapter
Screening & Monitoring Runs (1)	**Batch Screening**, **Delta Screening**, **TM Runs**	Name Screening (Batch and Delta Screening), Transaction Monitoring (TM Runs)
Data Ingestion (2)	**Customers**, **Accounts**, **Transactions**, **Watchlist**	Data Ingestion

Each day cell shows a coloured dot for the outcome of that job on that day. When the job ran, the dot is followed by a figure in brackets, in most cells with a multiplier before it (for example **x2 (0)**).

Dot	Outcome	Example in **Figure 2.11**
Green	**Succeeded**	Batch Screening on 9 Oct: **x3 (3K)**; every Watchlist day
Red	**Failed**	TM Runs on 11 Oct: **x2 (0)**
Orange	**Mixed outcomes**	TM Runs on 13 Oct: **x6 (263.6K)**
Orange, pulsing	**In progress**	Batch Screening on 14 Oct: **(96.6K)**
Grey, with a dash (—) or a figure	**No status**	Delta Screening on every day shown

Tip
A red or orange dot is the cue to open the job: click its name. For file imports, check Batch Ingestion and Watchlist Ingestion.

Team Performance

Look here for analyst productivity, supervisor reviews and assignment analysis. The last panel on the page is **Team Performance**, described as **Analyst productivity, supervisor reviews, assignment analysis**, with a **See Team Performance** button at the right.

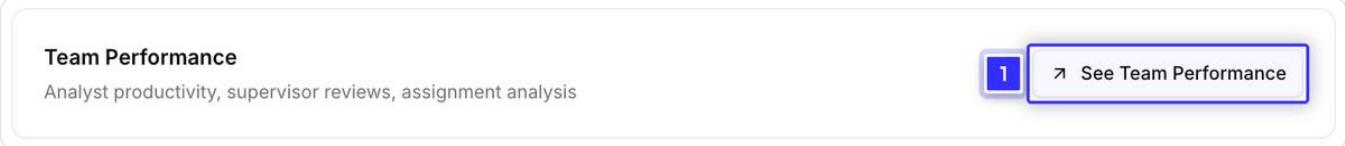


Figure 2.12 The Team Performance panel and the See Team Performance button (1)

Daily triage from the dashboard

Fyscal ARCX → AML Dashboard → Case Manager

Use this routine to go from the dashboard counts to the lists where the work is done. It uses only the tiles, chips and filters described in this guide. Adapt the order to your team's procedures.

WHO	WHERE	OUTPUT
Supervisors and team leads; analysts for their own queue	AML Dashboard, then Case Manager → Alerts and Cases	The day's backlog listed and the job runs checked

Step 1 **Read the tiles**

Open **Fyscal ARCX** → **AML Dashboard**. Note the counts on **Overdue Alerts**, **Escalated Alerts**, **Pending Cases** and **Escalated Cases** (Metric tiles).

Step 2 **List the overdue alerts**

Open **Case Manager** → **Alerts** and click **All Alerts**. Click **Show Filters** and set **SLA** to **Breached**. To work one module at a time, also set **Module** to **Name Screening** or **Transaction Monitoring** (Alerts list).

Step 3 **List the escalated alerts**

On the same tab, set **SLA** back to **All SLAs** and **Status** to **Escalated**.

Step 4 **Review the cases waiting for you**

Open **Case Manager** → **Cases**, click **All Cases**, then click the **Pending Approval** chip. The list shows the cases in **Pending Review**. Open each case and act on it as in Review a case in Pending Review. For escalated cases, click **Show Filters** and set **Status** to **Escalated**.

Step 5 **Check that the daily jobs ran**

Back on the dashboard, scroll to **Daily Jobs**. For **Batch Screening**, **Delta Screening** and **TM Runs**, look at the latest day columns: green marks **Succeeded**, red **Failed**, orange **Mixed outcomes** or **In progress**, and grey **No status** (Daily Jobs). In the **Data Ingestion** block, check the **Customers**, **Accounts**, **Transactions** and **Watchlist** rows the same way.

RELATED IN GET STARTED

Getting Started

CORE WORKFLOW

3 Case Manager

Fyscal ARCX → Case Manager

Case Manager is where analysts and reviewers work the alerts raised by Name Screening and Transaction Monitoring, group them into cases, record dispositions and prepare Suspicious Transaction Reports (STRs). The menu has three items: **Cases**, **Alerts** and **Config**. This chapter covers Cases and Alerts; Config is described in Case Manager Config.

FOR	IN THE MENU	READING TIME
Analysts, supervisors and team leads	Fyscal ARCX → Case Manager	About 50 min

The sections below follow the Case Manager menu (Cases, then Alerts). To follow an investigation from start to finish, read them in this order:

- **1. Triage alerts**: Alerts list, Alert Details: Name Screening, Alert Details: Transaction Monitoring and Work an alert.
- **2. Investigate a case**: Cases list, Filter and search cases, Case statuses and dispositions, Case Details, the evidence in Customer, accounts and matches and Transaction Monitoring evidence tabs, Timeline and notes, Case Copilot and Add alerts to a case.
- **3. Decide and review**: Dispose alerts and close a case, Review a case in Pending Review and Reopen a case.
- **4. File an STR**: File an STR, Open the STR wizard, the six steps (1, 2, 3, 4, 5, 6), After the STR is filed and Common blocks.

CONCEPT DIAGRAM

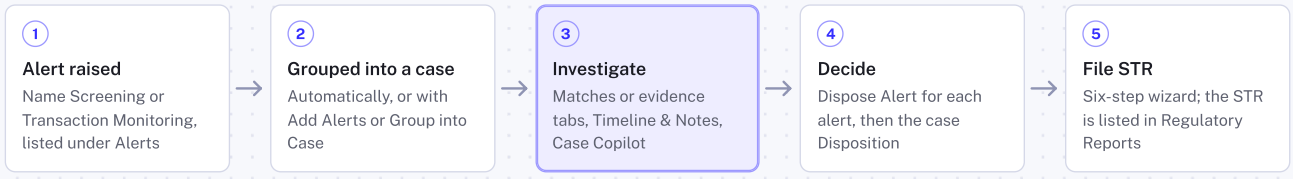


Diagram 3.1 — From alert to STR in Case Manager

An alert is raised by Name Screening or Transaction Monitoring and appears under **Alerts**. Alerts are merged into cases automatically, as set in Case Creation & Assignment (Case Manager Config), or by hand with Add Alerts on a case or Group into Case on an alert. On the case you review the evidence, record a disposition for each alert and for the case, and, where the activity is suspicious, file a Suspicious Transaction Report (STR) from the case. A filed STR is listed in Regulatory Reports.

AML context

An alert is a single detection: one screening match or one rule breach. A case brings together the alerts about one customer so that the evidence, the decision and its rationale are recorded once and can be reviewed later. An STR is the report sent to the financial intelligence unit when the investigation concludes that the activity is suspicious.

Cases list

Fyscal ARCX → Case Manager → Cases

The **Cases** screen lists cases in two tabs. **My Queue** shows the cases assigned to you. **All Cases** shows every case you can see, with summary chips above the list. Each tab shows its count (in the example, My Queue 4 and All Cases 73.1K).

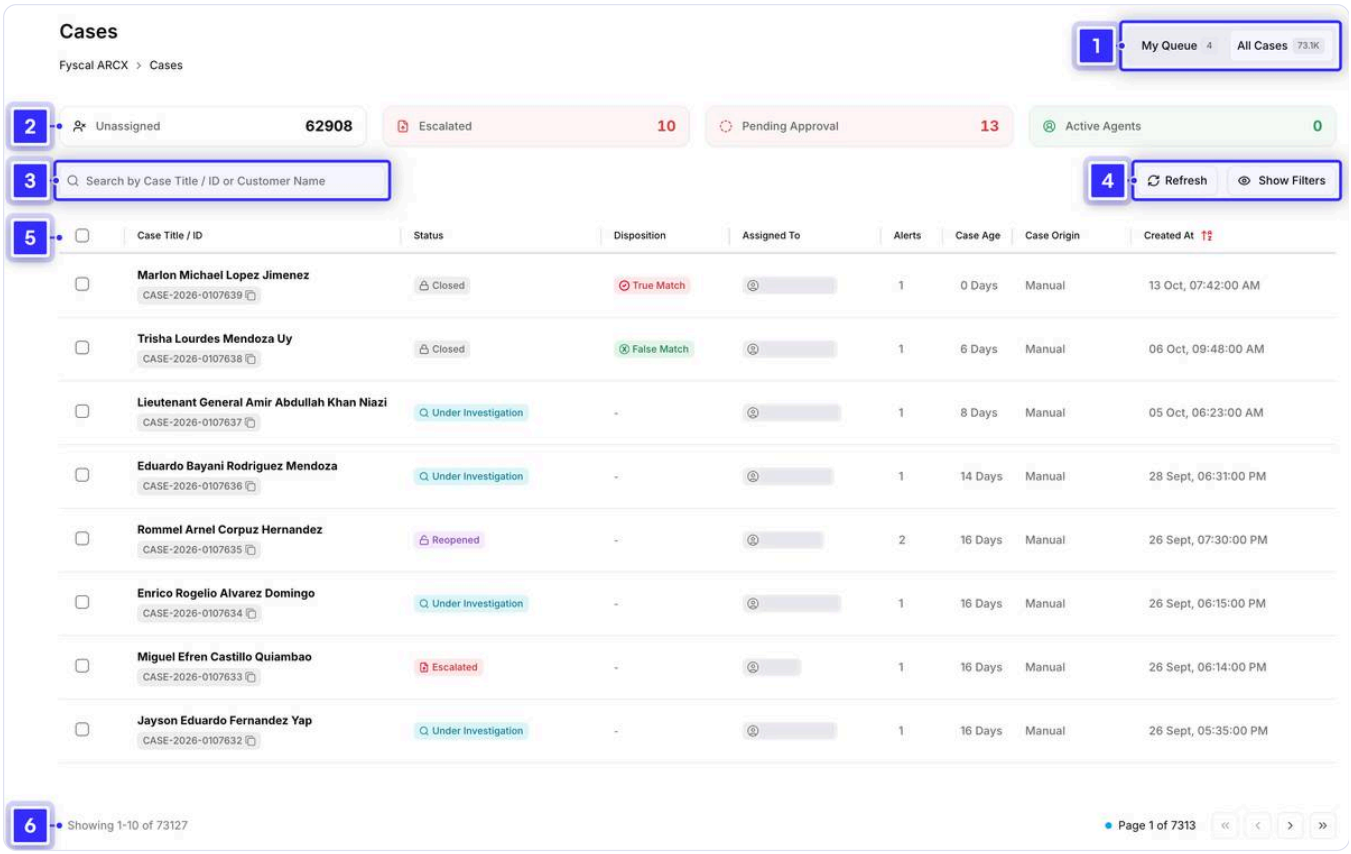


Figure 3.1 The Cases screen on the All Cases tab, with the summary chips, search and the case list

1. **My Queue** and **All Cases** tabs, each with a count.
2. Summary chips (All Cases only): **Unassigned**, **Escalated**, **Pending Approval** and **Active Agents**, each with a count. Clicking **Pending Approval** filters the list to cases in **Pending Review** (see Filter and search cases).
3. Search box: *Search by Case Title / ID or Customer Name*.
4. **Refresh** reloads the list. **Show Filters** opens the filter bar (the button then reads **Hide Filters**).
5. The case list. On All Cases, each row and the header have a checkbox.
6. Pagination: *Showing 1-10 of 73127* on the left; *Page 1 of 7313* with first, previous, next and last page buttons on the right.

Column	What it shows
Case Title / ID	The case title (the customer name or, for some cases, an alert ID) and the case ID, for example *CASE-2026-0034617*, with a copy icon.
Status	The case status as a coloured tag (see Case statuses and dispositions).
Disposition	The case disposition, for example **True Match**, or **-** when none has been recorded.
Assigned To	The user the case is assigned to, or **-**.
Alerts	The number of alerts in the case.
Case Age	Days since the case was created, for example *9 Days*.
Case Origin	**Manual** or **Automated**.
Created At	Creation date and time, for example *26 Sept, 06:14:00 PM*. The column header carries a sort indicator.

Click a row to open the case in Case Details.

Filter and search cases

Fyscal ARCX → Case Manager → Cases → Show Filters

The filter bar narrows the current tab. Filters combine with each other and with the search box.

Filter	Default	Options
Status	All Statuses	All Statuses, Not Started, Under Investigation, Pending Review, Escalated, STR Draft, STR Created, Closed, Reopened
Creation Period	Pick a date range	A two-month calendar for choosing a start and end date
Age Period	Any Age	Any Age, Less than a day, 1 to 3 days, 3 to 7 days, 7 to 30 days, More than 30 days
Case Origin	All Origins	All Origins, Manual, Automated
Assignee	All Assignees	A list of users. The signed-in user is labelled *(You)*.

Step 1 **Open the filter bar**

Click **Show Filters**. The **Status**, **Creation Period**, **Age Period**, **Case Origin** and **Assignee** filters appear below the search box.

Step 2 **Filter by status**

Open **Status** and choose one status. The current choice is ticked.

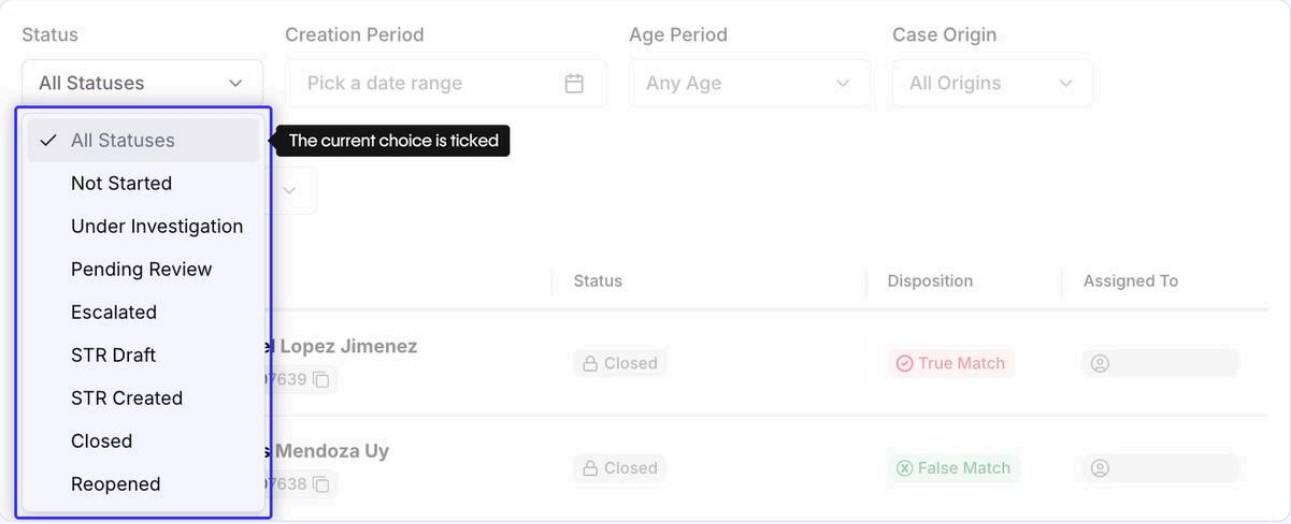


Figure 3.2 The Status filter open, with its nine options; the current choice is ticked

Step 3 **Filter by creation date**

Click **Creation Period**. A calendar showing two months opens; use the arrows to move between months, then click the first and last day of the range.

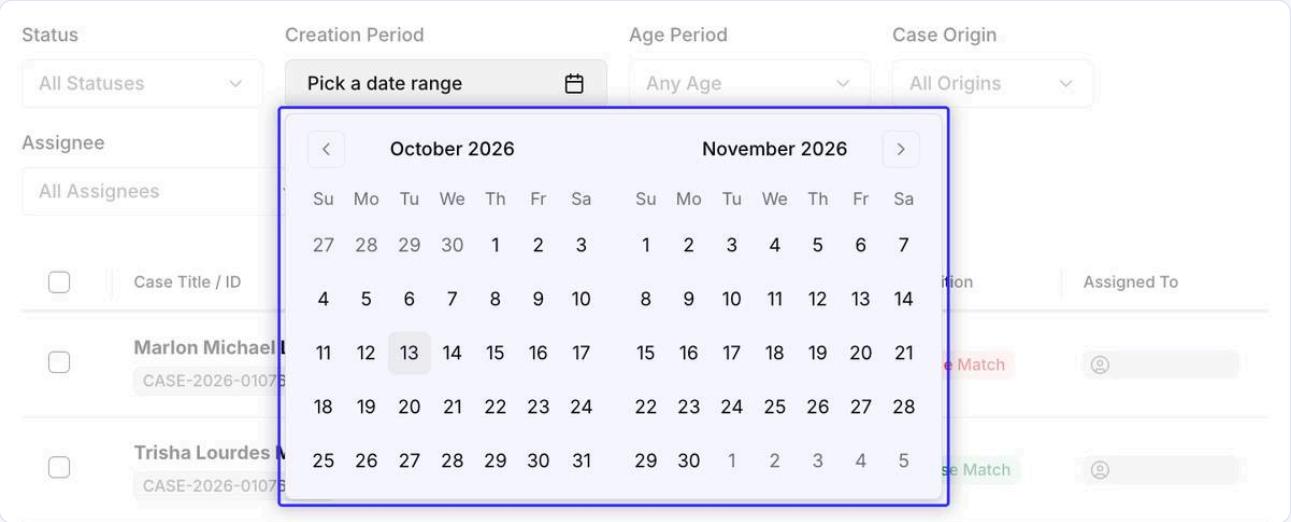


Figure 3.3 The Creation Period calendar

Step 4 **Filter by age or origin**

Open **Age Period** to choose how long cases have been open, or **Case Origin** to show only **Manual** or **Automated** cases.

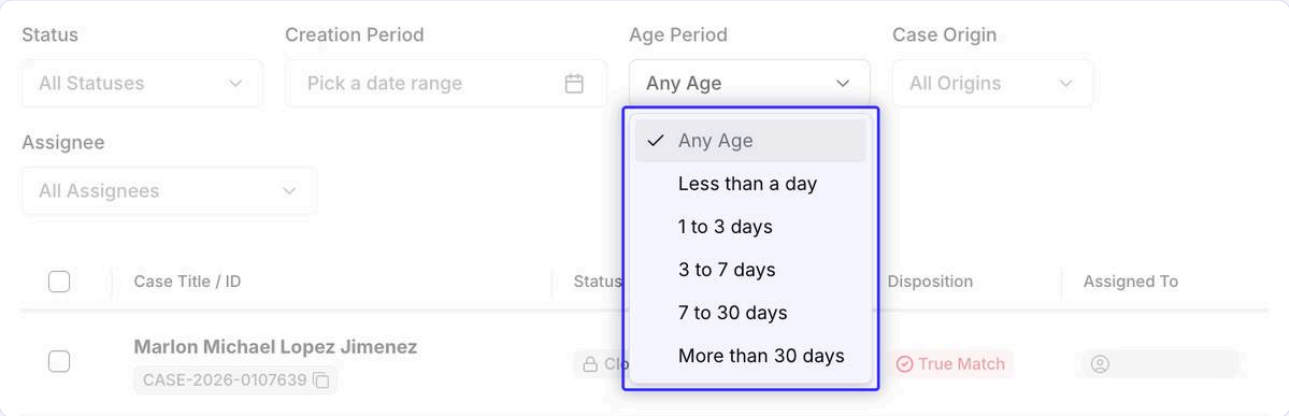


Figure 3.4 The Age Period filter

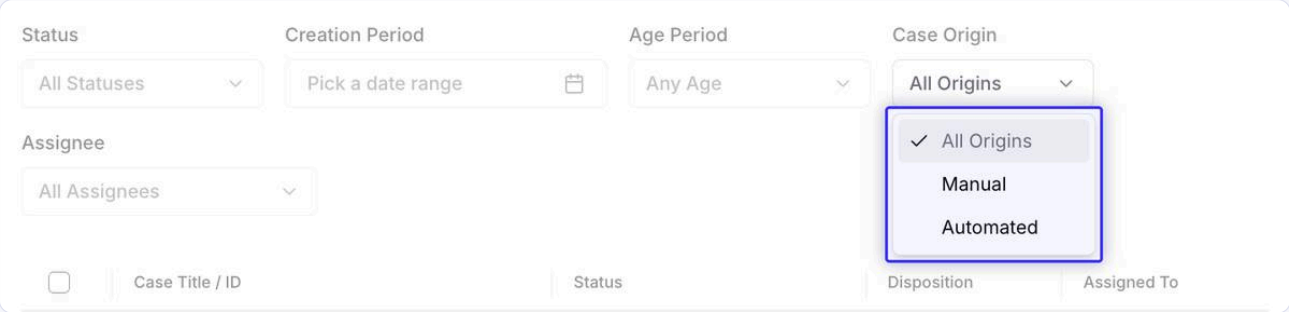


Figure 3.5 The Case Origin filter

Step 5 **Use a summary chip**

On All Cases, click the **Pending Approval** chip (1). The **Status** filter is set to **Pending Review** (2), an active-filter tag *Status: Pending Review* appears with an **×** to remove it (3), **RESET FILTERS** appears beside it (4), and the **All Cases** count changes to the filtered total, 13 in the example (5).

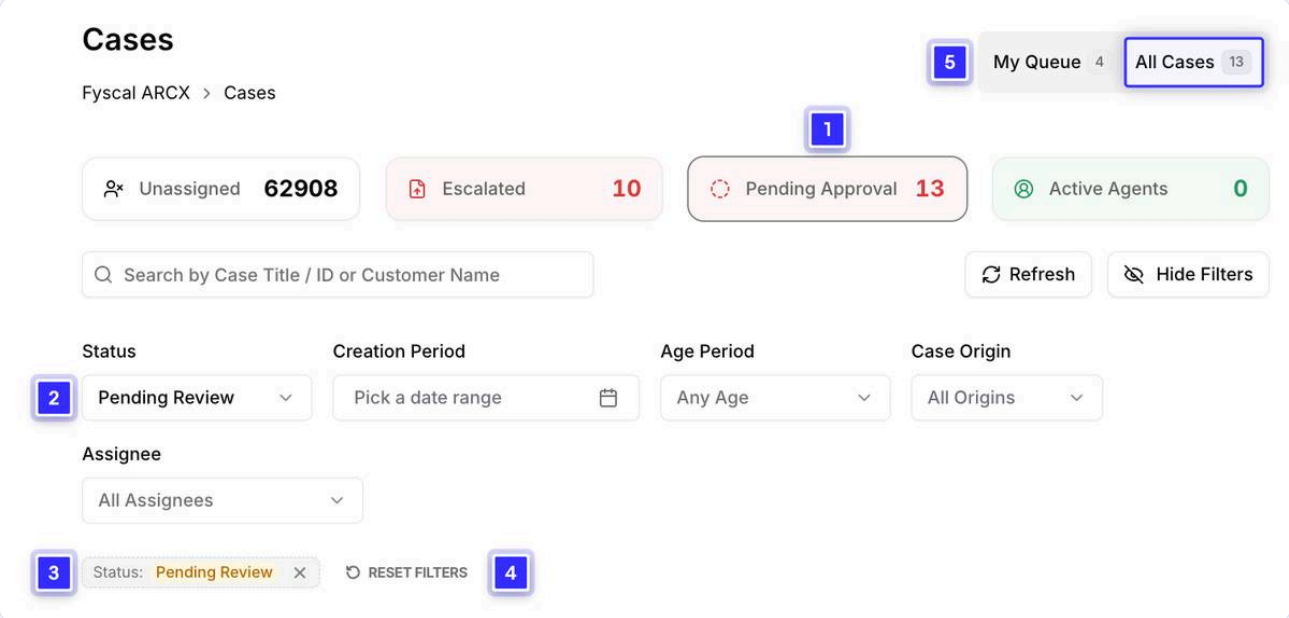


Figure 3.6 All Cases after clicking Pending Approval (1): the Status filter (2), the active-filter tag (3), RESET FILTERS (4) and the filtered count (5)

Step 6 **Clear the filters**

Click **×** on an active-filter tag to remove that filter, or click **RESET FILTERS** to remove them all.

Case statuses and dispositions

These are the values offered by the **Status** filter and the case **Disposition** dropdown, with what the case screen shows for each.

Status	What the screen shows
Not Started	Offered by the Status filter. No case in this status was captured for this guide.
Under Investigation	Offered by the Status filter, and one of the **Case Status** values of the case-creation group in Case Creation & Assignment. No case in this status was captured for this guide.
Pending Review	A disposition is waiting for a reviewer. The case shows the **Pending Review** panel with **Review Decision**, **Reject** and **Approve** (see Review a case in Pending Review). Counted by the **Pending Approval** chip.
Escalated	Counted by the **Escalated** chip. The escalated example case shows **Add Alerts**, with **Disposition** (*Select Outcome*) and **Dispose Alert** greyed out (Figure 3.7).
STR Draft	The case bar shows **Preview STR** and **ReOpen**.
STR Created	The case bar shows **Download STR** and **ReOpen**.
Closed	The case bar shows the decision (Rationale Code, Details, Decided On, Decided By). The example Closed case, with disposition True Match, shows **File STR** and **ReOpen**.
Reopened	A closed case that has been reopened. Its timeline records a **Reopened** event with *previous_status: closed*. The reopened example case (Figure 3.8) shows **Add Alerts**, the alert strip and **Dispose Alert**, and **Disposition** reads *Select Outcome*.

What the case bar shows in each status

The buttons in the case bar change with the status. The table records what each example case shows; a status with no captured example is left out. **Yes**: shown; **Partial**: shown greyed out; **No**: not shown.

Case bar control	Reopened	Escalated	Pending Review	Closed	STR Draft	STR Created
Add Alerts	✓ Yes	✓ Yes	✕ No	✕ No	✕ No	✕ No
Dispose Alert	✓ Yes	◑ Partial Greyed out	✕ No	✕ No	✕ No	✕ No
Disposition reads ***Select Outcome***	✓ Yes	✓ Yes Greyed out	✕ No Shows True Match	✕ No Shows True Match	✕ No Shows True Match	✕ No Shows True Match
Reject / Approve	✕ No	✕ No	✓ Yes	✕ No	✕ No	✕ No
File STR	✕ No	✕ No	✕ No	✓ Yes	✕ No	✕ No
Preview STR	✕ No	✕ No	✕ No	✕ No	✓ Yes	✕ No
Download STR	✕ No	✕ No	✕ No	✕ No	✕ No	✓ Yes
ReOpen	✕ No	✕ No	✕ No	✓ Yes	✓ Yes	✓ Yes

Example cases: Reopened CASE-2026-0034617 (Figure 3.8), Escalated CASE-2026-0107633 (Figure 3.7), Pending Review CASE-2026-0034612 (Review a case in Pending Review), Closed CASE-2026-0034613 (Dispose alerts and close a case), STR Draft CASE-2026-0107624 and STR Created CASE-2026-0034611 (Open the STR wizard and After the STR is filed). The escalated example is assigned to another user; the screen does not say why its controls are greyed out.

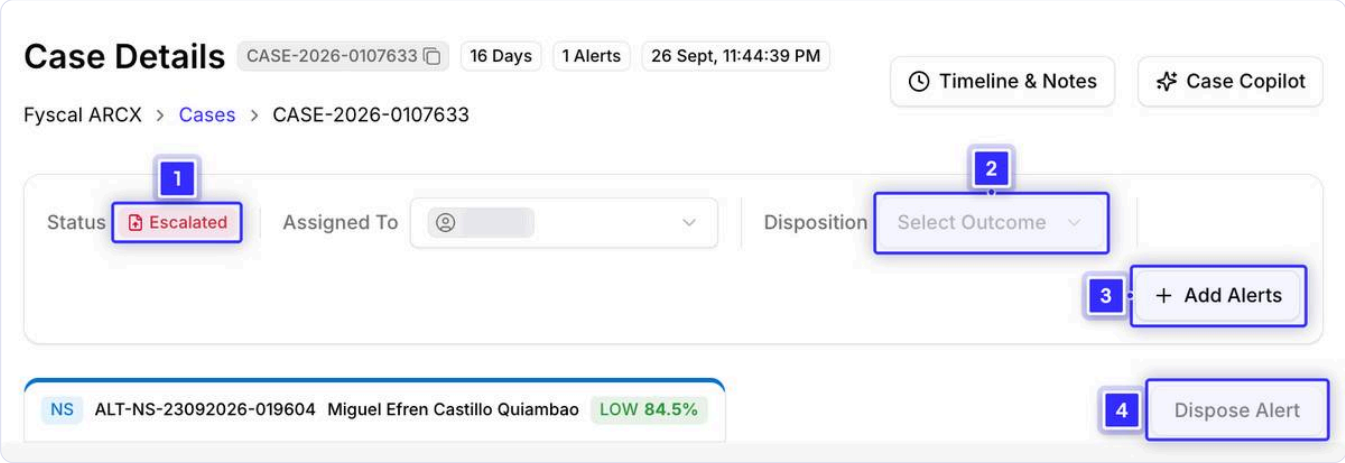


Figure 3.7 An Escalated case (CASE-2026-0107633): the Escalated status (1), Disposition greyed out (2), Add Alerts (3) and Dispose Alert greyed out (4)

Status changes recorded on screen



Diagram 3.2 — Case status changes recorded in a case timeline

The timeline of CASE-2026-0034617 records both changes. **ReOpen** on a Closed case gives the status **Reopened**, and the **Reopened** event shows *previous_status: closed*. On the reopened case, a **Disposition Submitted** event tagged **Case closed** closes it again; the next **Reopened** event again shows *previous_status: closed*. The STR statuses are covered in File an STR.

Disposition	Where it appears
True Match	The case **Disposition** dropdown, the alert **Disposition** dropdown and the **Dispose Alert** dialog. Before a disposition is chosen, the case dropdown reads *Select Outcome* and the alert dropdown *Select outcome*; list columns show **-**.
False Match	
Potential Match	

AML context

In general use, **True Match** means the customer is the listed party or the activity is confirmed as suspicious; **False Match** means it is a different party or the activity is explained; **Potential Match** means a match cannot be ruled out without more information. How a Potential Match affects the case in Fyscal ARCX has not been confirmed.

Case Details

Fyscal ARCX → Case Manager → Cases → (click a case)

Case Details shows one case: its status and owner, the alerts it contains, the customer, and the evidence behind each alert. The example is CASE-2026-0034617 for the customer Pooja Sharma, with six Name Screening alerts.

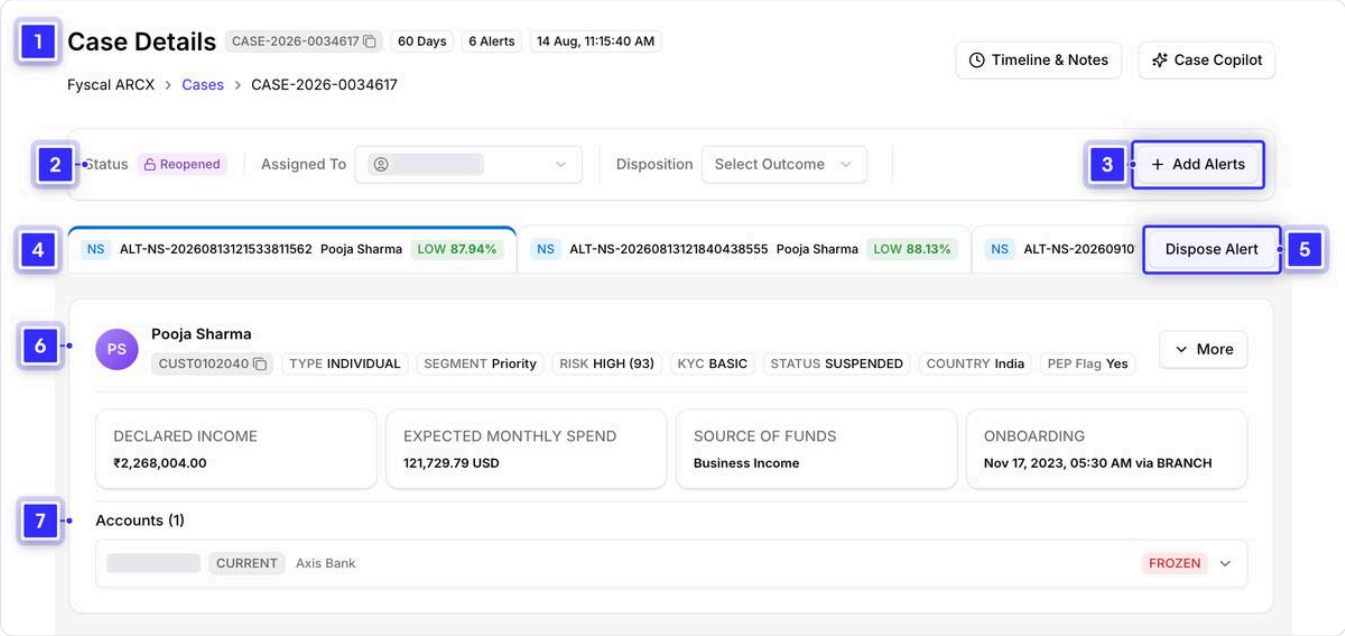


Figure 3.8 Top of Case Details for CASE-2026-0034617

1. Header: **Case Details**, the case ID (with a copy icon), the case age (*60 Days* in the example), the number of alerts (*6 Alerts*) and the creation date and time, with the breadcrumb *Fyscal ARCX › Cases › CASE-2026-0034617*. At the right are **Timeline & Notes** (see Timeline and notes) and **Case Copilot** (see Case Copilot).
2. Case bar: **Status**, **Assigned To** (a dropdown of users) and **Disposition** (a dropdown with **True Match**, **False Match** and **Potential Match**).
3. **Add Alerts** adds ungrouped alerts to this case (see Add alerts to a case).
4. Alert strip: one tab per alert, showing the module (**NS** for Name Screening, **TM** for Transaction Monitoring), the alert ID, the customer name, the alert's disposition once recorded, and the score band with its percentage. The selected tab is underlined in blue and the rest of the page shows that alert. When there are more tabs than fit, the strip continues to the right.
5. **Dispose Alert** records a disposition for the selected alert (see Dispose alerts and close a case).
6. Customer card (see Customer, accounts and matches).
7. **Accounts**, with the number of accounts in brackets.

Below the customer card, a Name Screening alert shows **Matches**; a Transaction Monitoring alert shows the tabs **Analytics**, **Transactions**, **Other Cases / Alerts** and **Rule Analysis** (see Transaction Monitoring evidence tabs). The buttons in the case bar change with the status: see the table in Case statuses and dispositions.

Customer, accounts and matches

The customer card identifies the customer behind the selected alert. For the full customer profile, see Customer 360.

Area	What it shows
Card header	Customer name and customer ID (with a copy icon), then tags: **TYPE** (for example INDIVIDUAL, CORPORATE), **SEGMENT**, **RISK** (band and score, for example HIGH (93)), **KYC**, **STATUS**, **COUNTRY** and **PEP Flag**.
Tiles	**DECLARED INCOME**, **EXPECTED MONTHLY SPEND**, **SOURCE OF FUNDS** and **ONBOARDING** (date, time and channel, for example *via BRANCH*). A tile is left out when the value is missing.
More / Less	**More** expands three panels and changes to **Less**: **BUSINESS & EMPLOYMENT** (Designation, Employer, Segment, Source of Funds, Country of Operations), **FINANCIAL INFORMATION** (Declared Income, Expected Monthly Spend, Purpose, Onboarding Channel, Expected Txn Frequency) and **Additioanl Details** (City, Country, Sanctions).
Accounts (n)	One row per account: account number, account type (for example CURRENT), bank and status (for example ACTIVE, FROZEN, CLOSED). The arrow at the right expands the row to show **Type**, **Bank**, **Holding**, **Currency**, **Bank Country** and **Opened**.

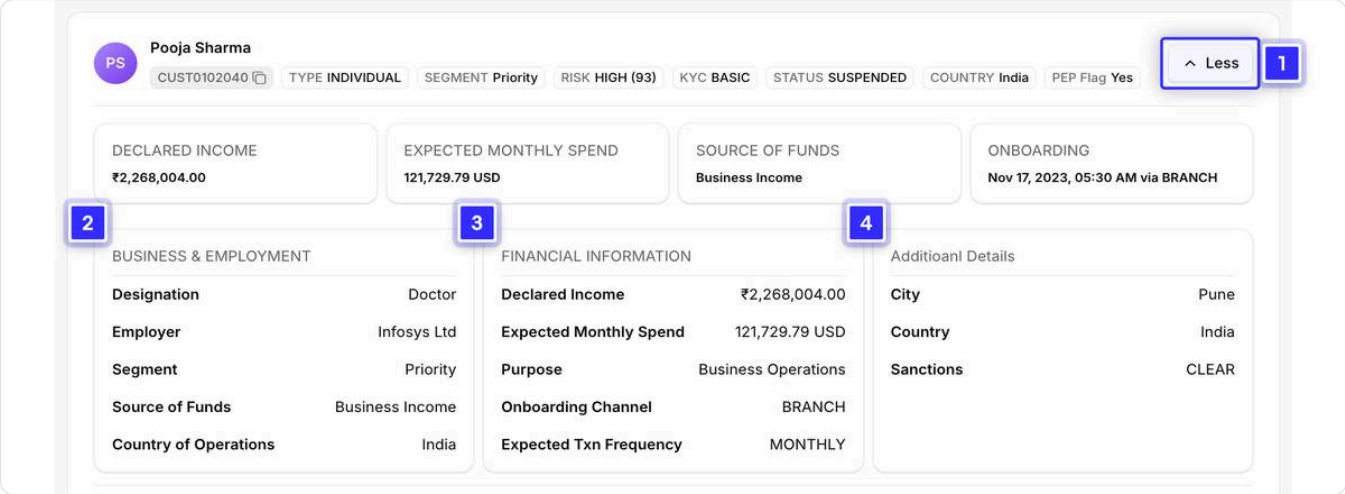


Figure 3.9 The customer card expanded: Less (1), BUSINESS & EMPLOYMENT (2), FINANCIAL INFORMATION (3) and Additioanl Details (4)

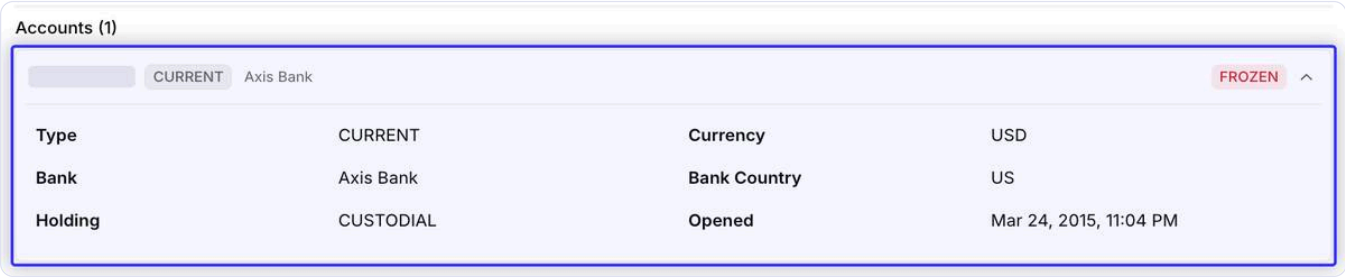


Figure 3.10 An account row expanded: Type, Bank, Holding, Currency, Bank Country and Opened

Matches (Name Screening alerts)

Matches compares the customer with each watchlist candidate found for the selected alert. The red tag gives the number of candidates (*Matches: 1*).

- The grey left column (1) lists the customer's own values for **Name**, **Nationality**, **Date of Birth**, **Address** and **Entity Type**, under the row labels **Match Score** and **UID (watchlist)**.
- Each candidate column (2) shows the score band and percentage (for example *LOW 87.94%*), the watchlist category (for example INDIVIDUAL), the watchlist **UID**, and for each field the watchlist value with its **Weightage** and **Score**.
- The candidate with the blue border is the one shown in the panel below (3), headed **Selected:** with the candidate's name, band, **UID**, **Screening** number and **Category**.

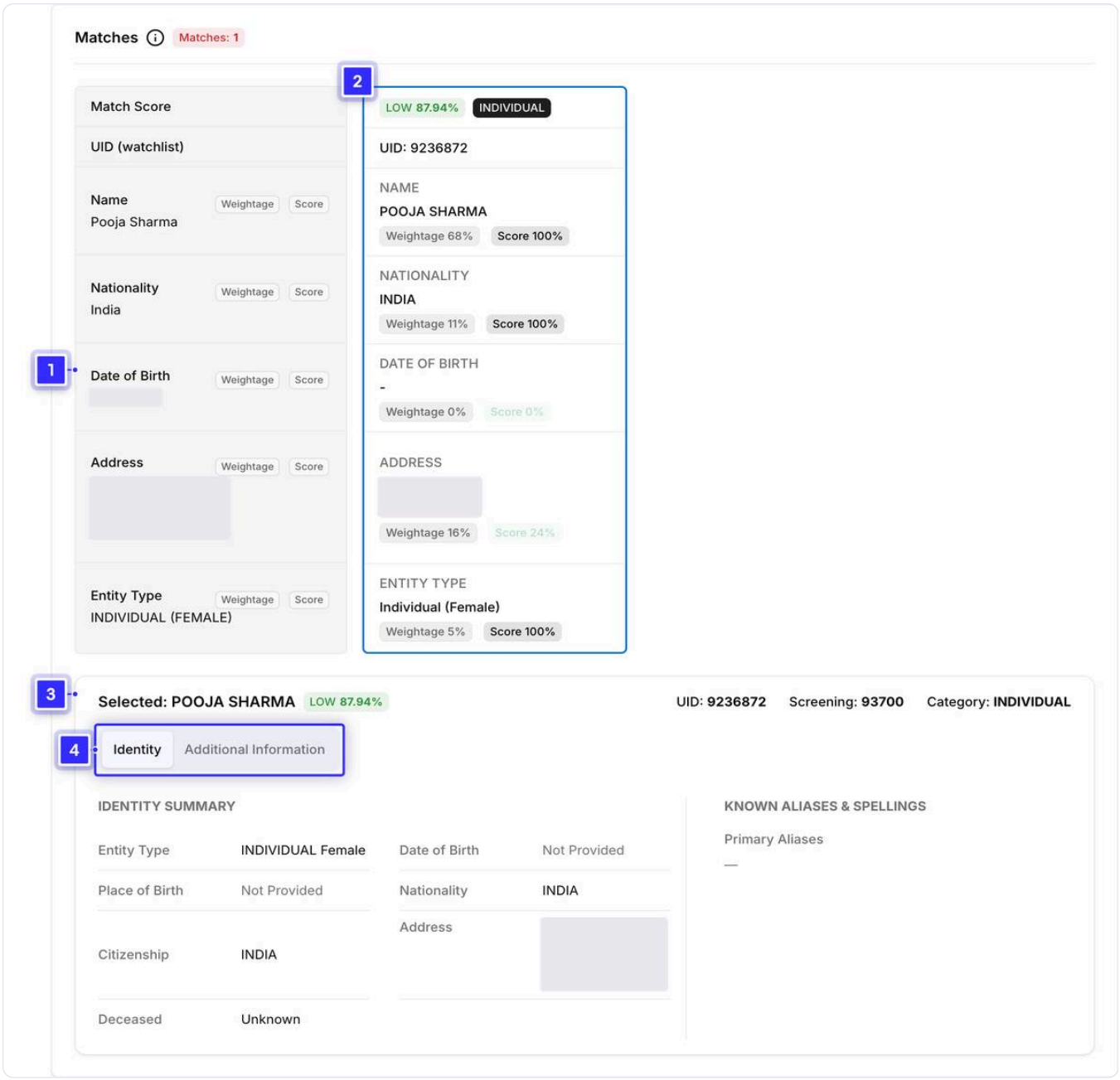


Figure 3.11 Matches for CASE-2026-0034617: the customer column (1), one watchlist candidate (2) and the Selected panel (3) on the Identity tab (4)

The **Selected** panel has two tabs (4):

Tab	Sections and fields
Identity	**IDENTITY SUMMARY**: Entity Type, Date of Birth, Place of Birth, Nationality, Citizenship, Address, Deceased. **KNOWN ALIASES & SPELLINGS**: Primary Aliases. Missing values read *Not Provided*, *Unknown* or —.
Additional Information	**LIST CLASSIFICATION**: Category, Sub-Category. **ASSOCIATES**: watchlist UIDs of associated entries. **FURTHER INFORMATION**: BIOGRAPHY, IDENTIFICATION, REPORTS. **LIST METADATA**: List Entry Date, Last Updated. **KEYWORDS & SOURCES**: External Sources, with the number of sources and a link for each.

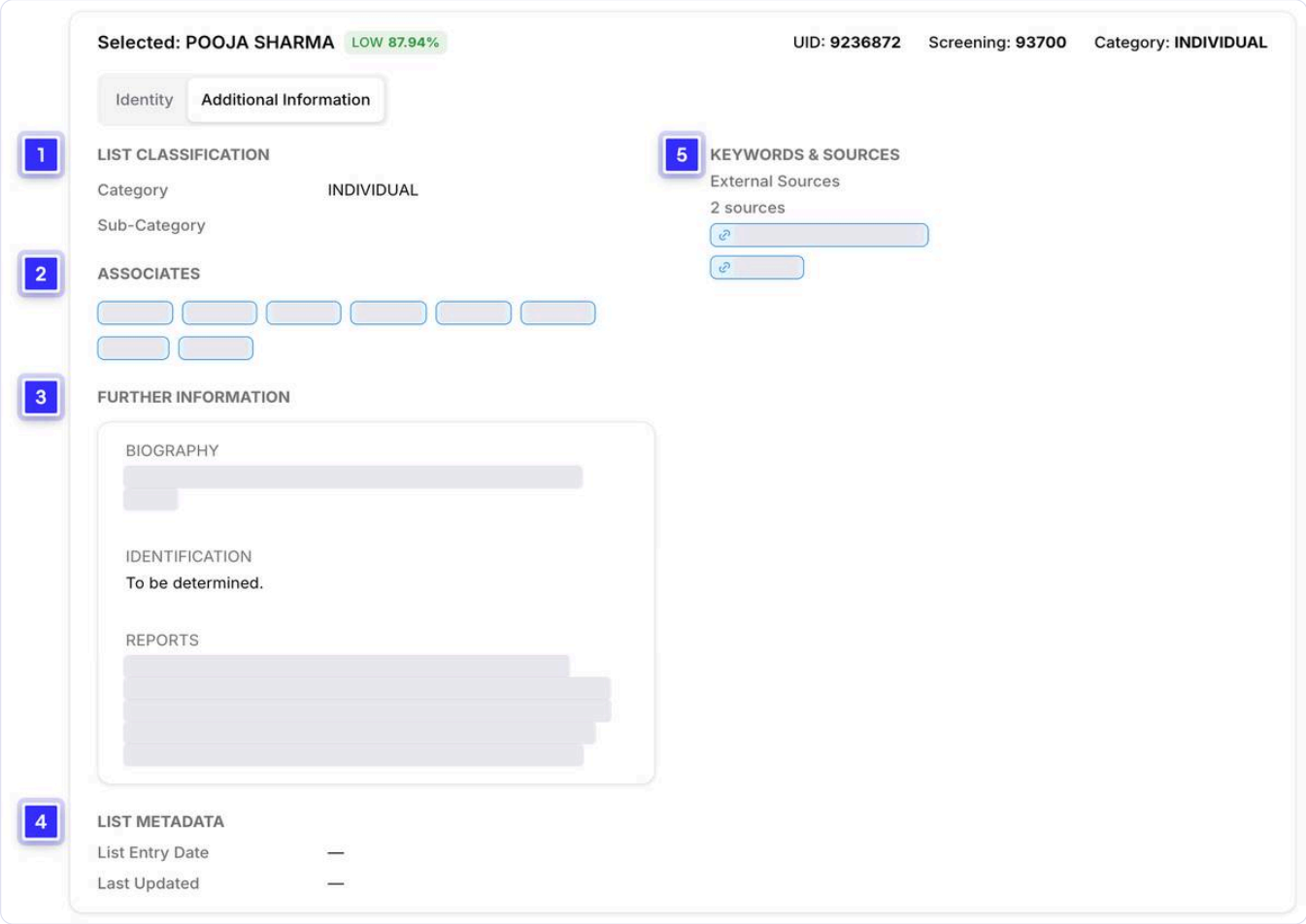


Figure 3.12 The Additional Information tab: LIST CLASSIFICATION (1), ASSOCIATES (2), FURTHER INFORMATION (3), LIST METADATA (4) and KEYWORDS & SOURCES (5)

> **Note**
> The Weightage and Score shown are those recorded for the alert. How weightages are configured is described in Name Screening.

Transaction Monitoring evidence tabs

When the selected alert is a Transaction Monitoring (**TM**) alert, four tabs appear below the customer card. The same tabs appear on a Transaction Monitoring alert in Alert Details.

Tab	What it shows
Analytics	For the customer, period buttons **1D**, **7D**, **30D**, **All** and an **Alert Window** checkbox. **INCOMING** and **OUTGOING** each give, per currency, **TOTAL** (with the number of transactions and senders or recipients), **AVG** and **MAX** (with the transaction ID). Below: **Top Counterparties by Amount** and **Transaction Types**, five of each, with buttons such as *14 more Counterparties* and *4 more Types*.
Transactions (n)	**Transaction Pattern** with **Transaction Trends** and **Volume Heatmap** views, a date range, **Day**, **Week** and **Month**, and the charts **Transaction Volume** and **Transaction Count**. **Transaction Table** with the filters **All Types**, **All Channels**, **Price range**, **Pick a date range**, **Sender ID**, **Receiver ID** and the **Triggered Txns** checkbox, and the columns Txn ID, Sender, Receiver, Amount, Type, Channel, Date. Each row has an arrow at the right to expand it. **Export CSV** sits at the top right.
Other Cases / Alerts	A **Cases** / **Alerts** switch, each with a count. Cases uses the case-list columns with **Status** and **Date Range** filters; Alerts uses the alert-list columns with **Status**, **Disposition** and **Date Range** filters.
Rule Analysis	**RULE TRIGGERED**: the rule name with a tag (for example *internal*), the **Window** start and frequency (for example *every 1 Month*), the number of breaches, and each breached condition (for example *transactions.amount > 10000*) tagged **Breach**.

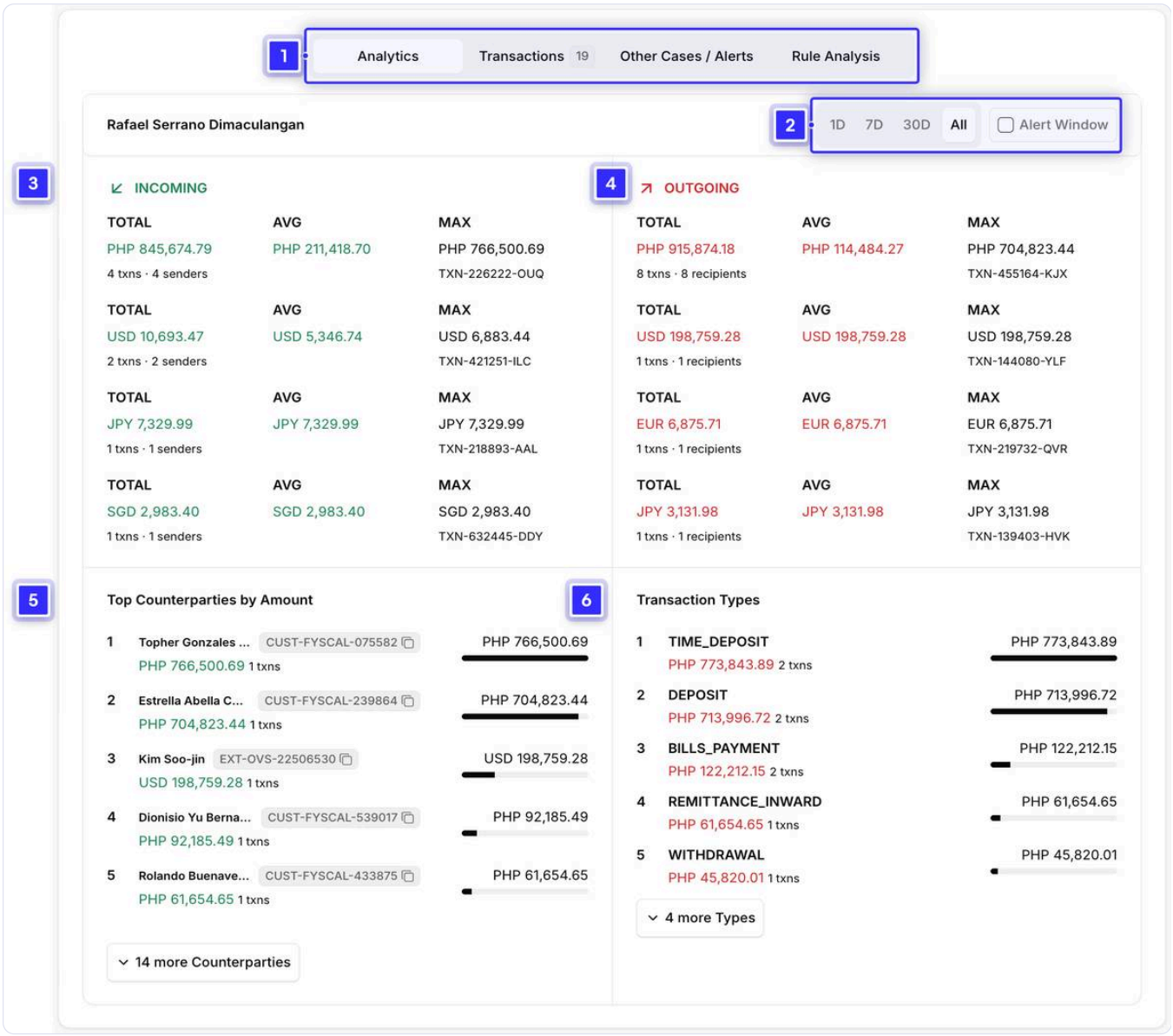


Figure 3.13 Analytics tab for CASE-2026-0034611 (Rafael Serrano Dimaculangan): the evidence tabs (1), period buttons and Alert Window (2), INCOMING (3) and OUTGOING (4) totals per currency, Top Counterparties by Amount (5) and Transaction Types (6)

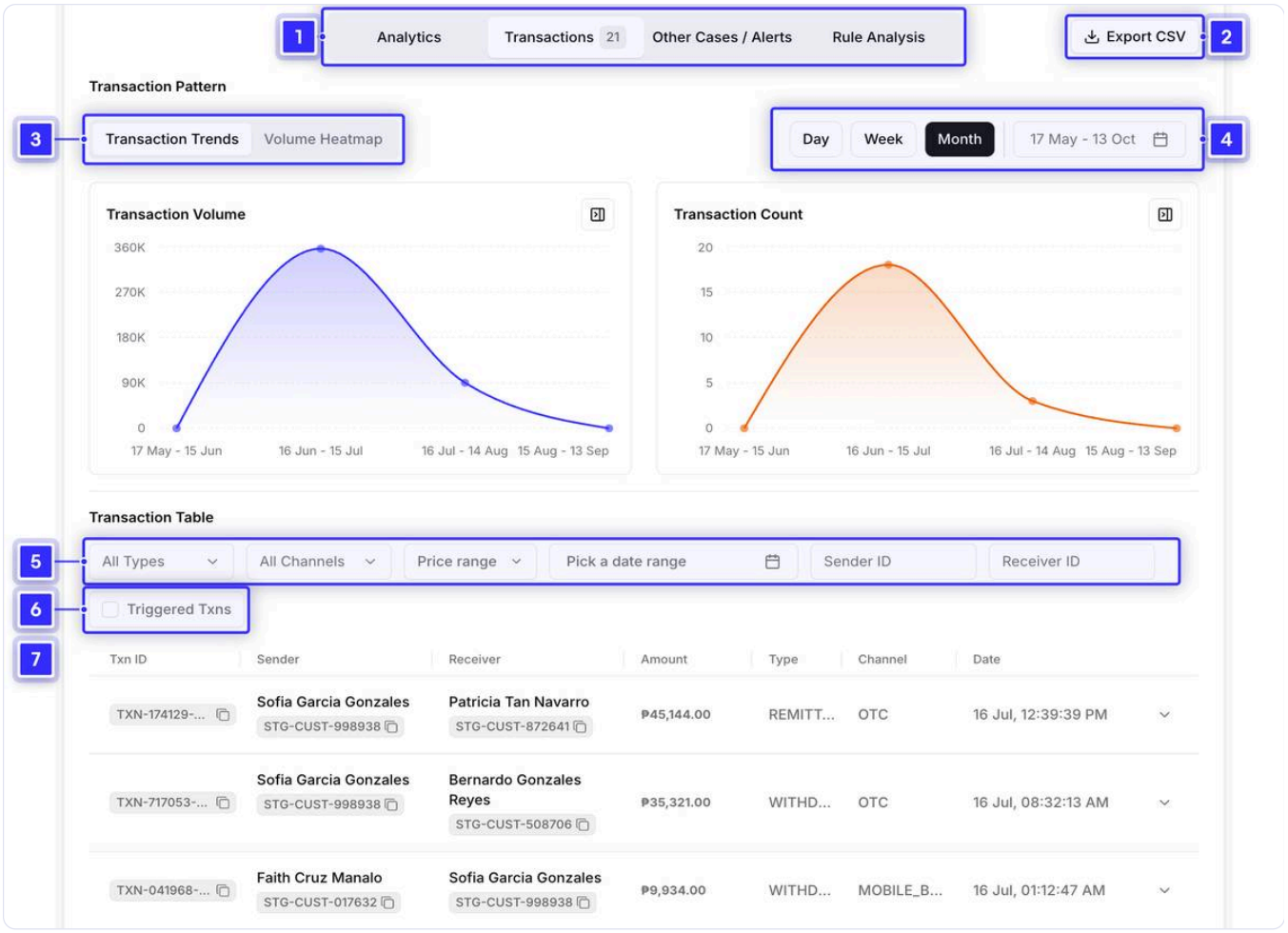


Figure 3.14 Transactions tab with the Month view: the evidence tabs (1), Export CSV (2), Transaction Trends and Volume Heatmap (3), Day, Week, Month and the date range (4), the table filters (5), Triggered Txns (6) and the table columns (7)

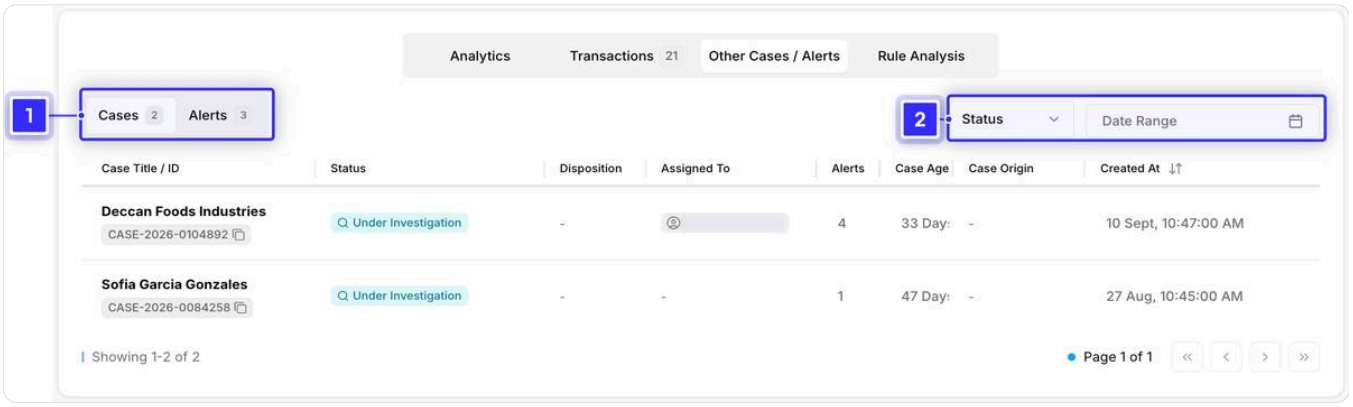


Figure 3.15 Other Cases / Alerts tab: the Cases and Alerts switch with counts (1) and the Status and Date Range filters (2)



Figure 3.16 Rule Analysis tab: rule H_V_T with its tag and window (1), the breach count (2) and the breached condition transactions.amount > 10000 (3)

Timeline and notes

Case Details → Timeline & Notes

Timeline & Notes opens the **Activity Timeline** panel on the right, headed with the case ID. It holds the case notes and a dated log of what happened to the case, newest first.

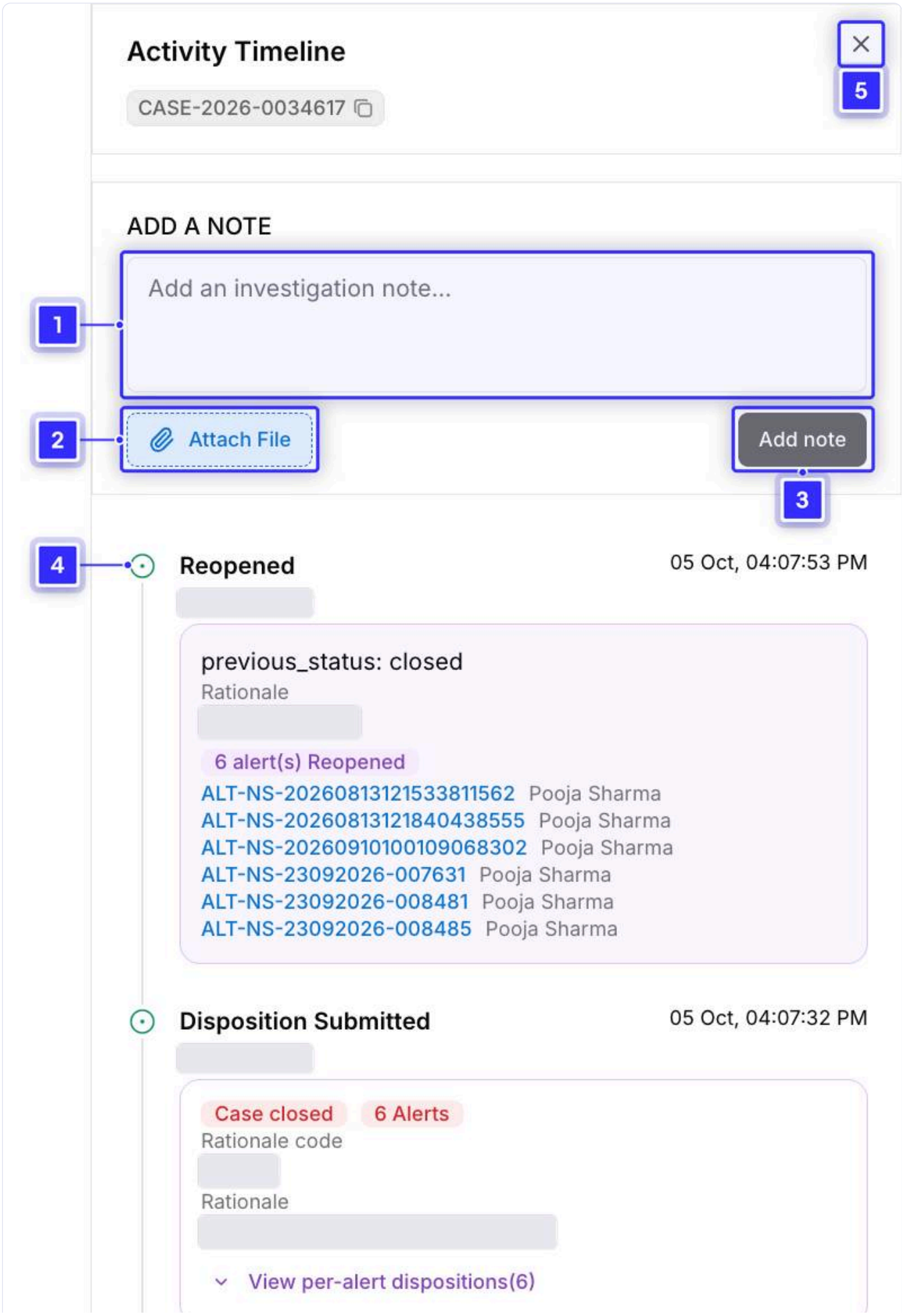

Activity Timeline
CASE-2026-0034617
5
ADD A NOTE
Add an investigation note...
1
2
Attach File
Add note
3
4
Reopened
05 Oct, 04:07:53 PM
previous_status: closed
Rationale
6 alert(s) Reopened
ALT-NS-20260813121533811562 Pooja Sharma
ALT-NS-20260813121840438555 Pooja Sharma
ALT-NS-20260910100109068302 Pooja Sharma
ALT-NS-23092026-007631 Pooja Sharma
ALT-NS-23092026-008481 Pooja Sharma
ALT-NS-23092026-008485 Pooja Sharma
Disposition Submitted
05 Oct, 04:07:32 PM
Case closed
6 Alerts
Rationale code
Rationale
View per-alert dispositions(6)

Figure 3.17 Activity Timeline for CASE-2026-0034617: the note box (1), Attach File (2), Add note, greyed out while the box is empty (3), the newest event (4) and the close button (5)

Step 1 **Add a note**

Type in **ADD A NOTE** (*Add an investigation note...*) (1). To attach a document, click **Attach File** (2). Click **Add note** (3); it is greyed out while the note box is empty.

Step 2 **Read the events**

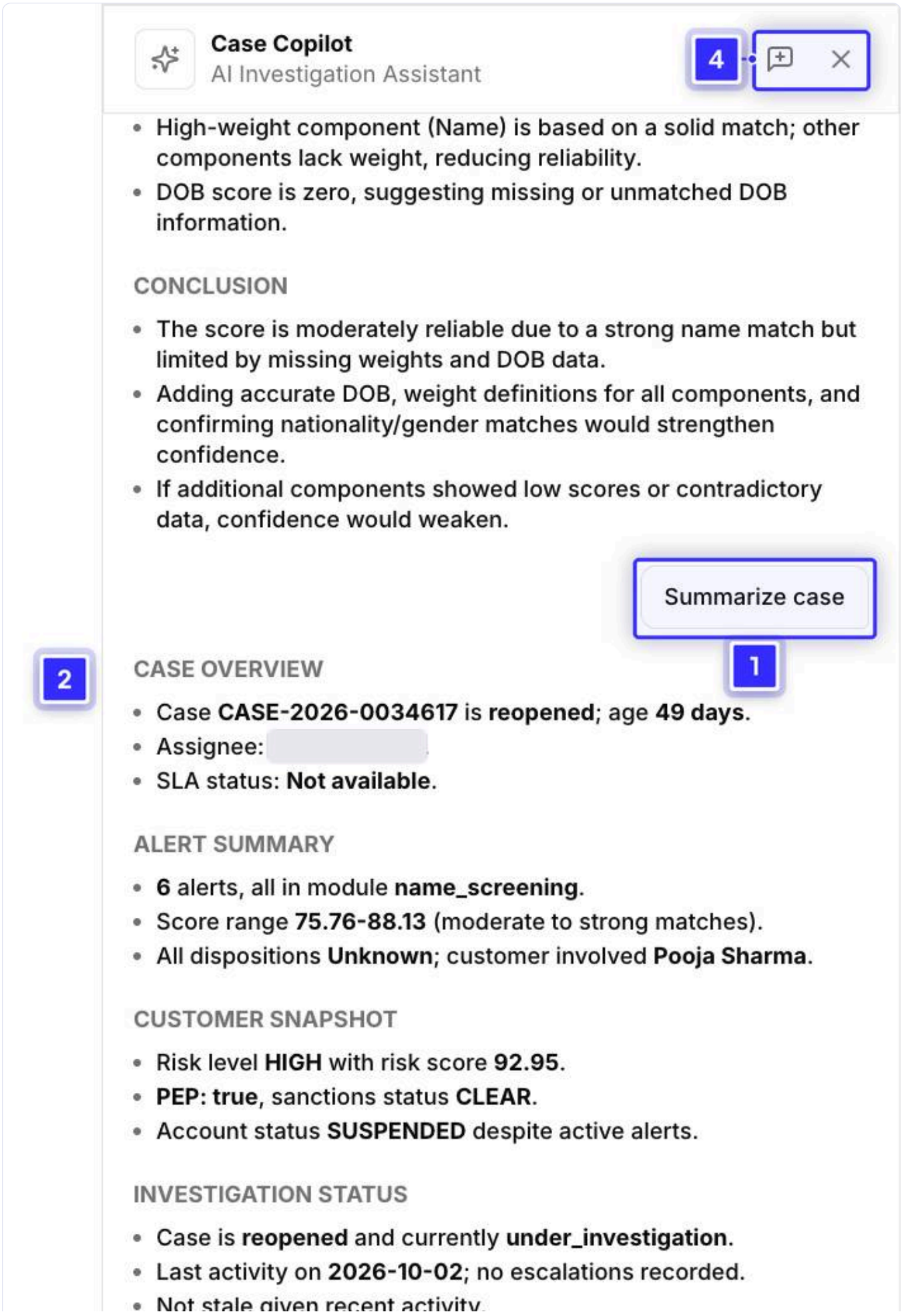
Each event (4) shows its type, the user (or *System*) and the date and time. The events seen on cases are listed below. Click **×** (5) to close the panel.

Event	Details shown
Created	The first event. *Alert Added* with the alert and a **View alert timeline** link.
Linked to Case	Each alert added to the case, with customer name, alert ID, band and score, and **View alert timeline**.
Disposition Submitted	Tags such as **Case closed** and the number of alerts, the **Rationale code** and **Rationale**. **View per-alert dispositions(n)** expands to list each alert with its band and score, disposition, rationale code and rationale.
Reopened	*previous_status* (for example closed), the **Rationale**, and *n alert(s) Reopened* with a link to each alert.

Case Copilot

Case Details → Case Copilot

Case Copilot (*AI Investigation Assistant*) is a chat panel that answers questions about the open case. On first use it greets you by first name and asks *How can I help you with this case?*. Its prompt and model are set in Agentic Workflows (see Case Manager Config).


Case Copilot
AI Investigation Assistant
4
High-weight component (Name) is based on a solid match; other components lack weight, reducing reliability.
DOB score is zero, suggesting missing or unmatched DOB information.
CONCLUSION
The score is moderately reliable due to a strong name match but limited by missing weights and DOB data.
Adding accurate DOB, weight definitions for all components, and confirming nationality/gender matches would strengthen confidence.
If additional components showed low scores or contradictory data, confidence would weaken.
Summarize case
1
2
CASE OVERVIEW
Case CASE-2026-0034617 is reopened; age 49 days.
Assignee:
SLA status: Not available.
ALERT SUMMARY
6 alerts, all in module name_screening.
Score range 75.76-88.13 (moderate to strong matches).
All dispositions Unknown; customer involved Pooja Sharma.
CUSTOMER SNAPSHOT
Risk level HIGH with risk score 92.95.
PEP: true, sanctions status CLEAR.
Account status SUSPENDED despite active alerts.
INVESTIGATION STATUS
Case is reopened and currently under_investigation.
Last activity on 2026-10-02; no escalations recorded.
Not stale given recent activity.

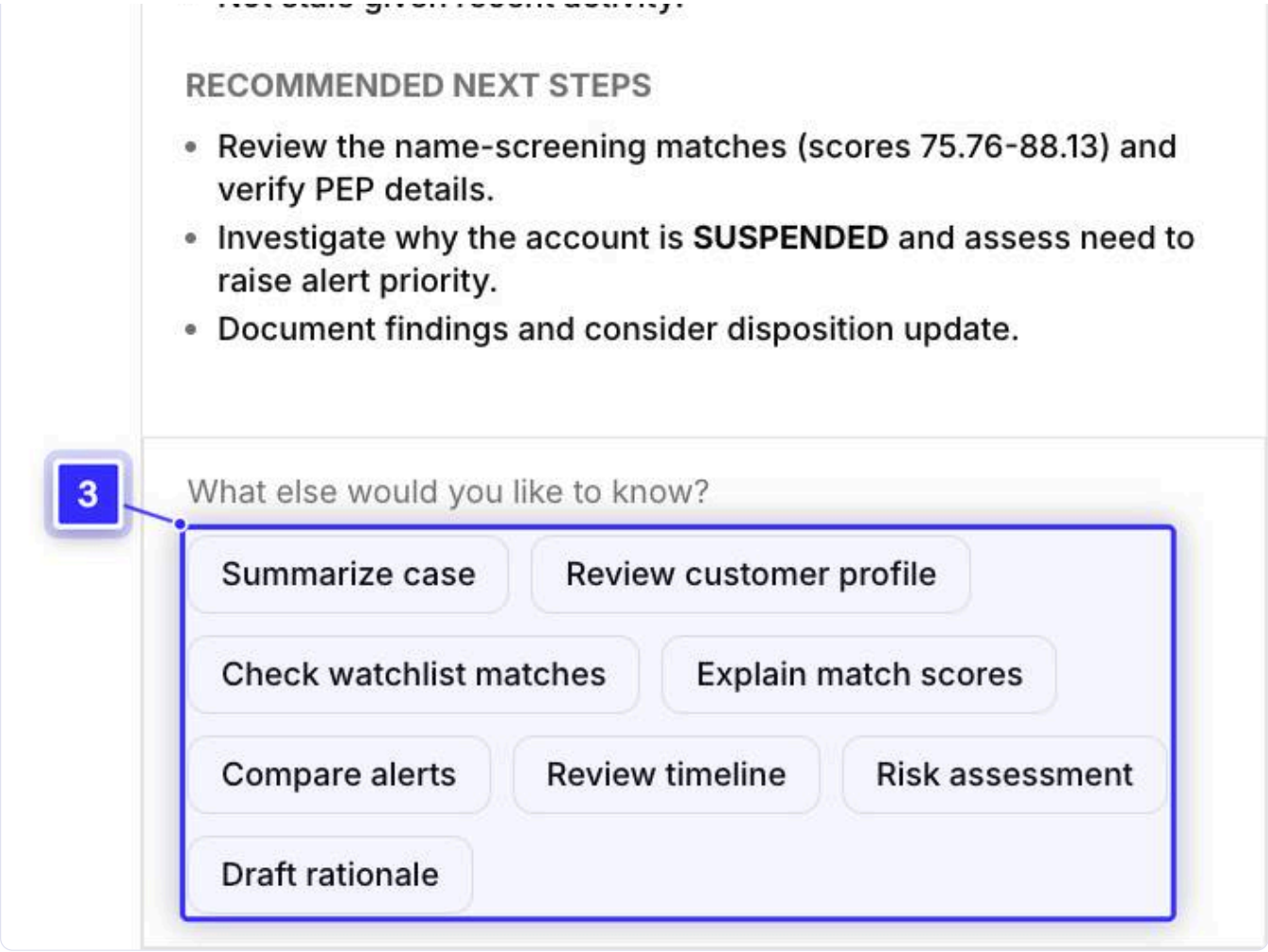


Figure 3.18 Case Copilot after Summarize case (1): the answer in headed sections (2), the suggested prompts (3), and the new-chat and close icons (4)

Step 1 **Ask a question**

Click **Case Copilot**, then click one of the prompts under *What else would you like to know?*: **Summarize case**, **Review customer profile**, **Check watchlist matches**, **Explain match scores**, **Compare alerts**, **Review timeline**, **Risk assessment** or **Draft rationale**.

Step 2 **Read the answer**

Each answer appears under the prompt you chose, in headed sections. **Summarize case** returns CASE OVERVIEW, ALERT SUMMARY, CUSTOMER SNAPSHOT, INVESTIGATION STATUS and RECOMMENDED NEXT STEPS. **Explain match scores** returns OVERALL SCORE, COMPONENT ANALYSIS, SCORE RELIABILITY and CONCLUSION. Earlier answers stay in the panel.

Step 3 **Start again or close**

The icon at the top right starts a new chat; **×** closes the panel.

Note

Check Copilot answers against the case before relying on them. In Figure 3.18 the summary gives the case age as 49 days, while the case header in Figure 3.8 shows 60 Days.

Add alerts to a case

Case Details → Add Alerts

Add Alerts to Case lists alerts that are not yet in a case (*Select ungrouped alerts to merge into* the case ID).

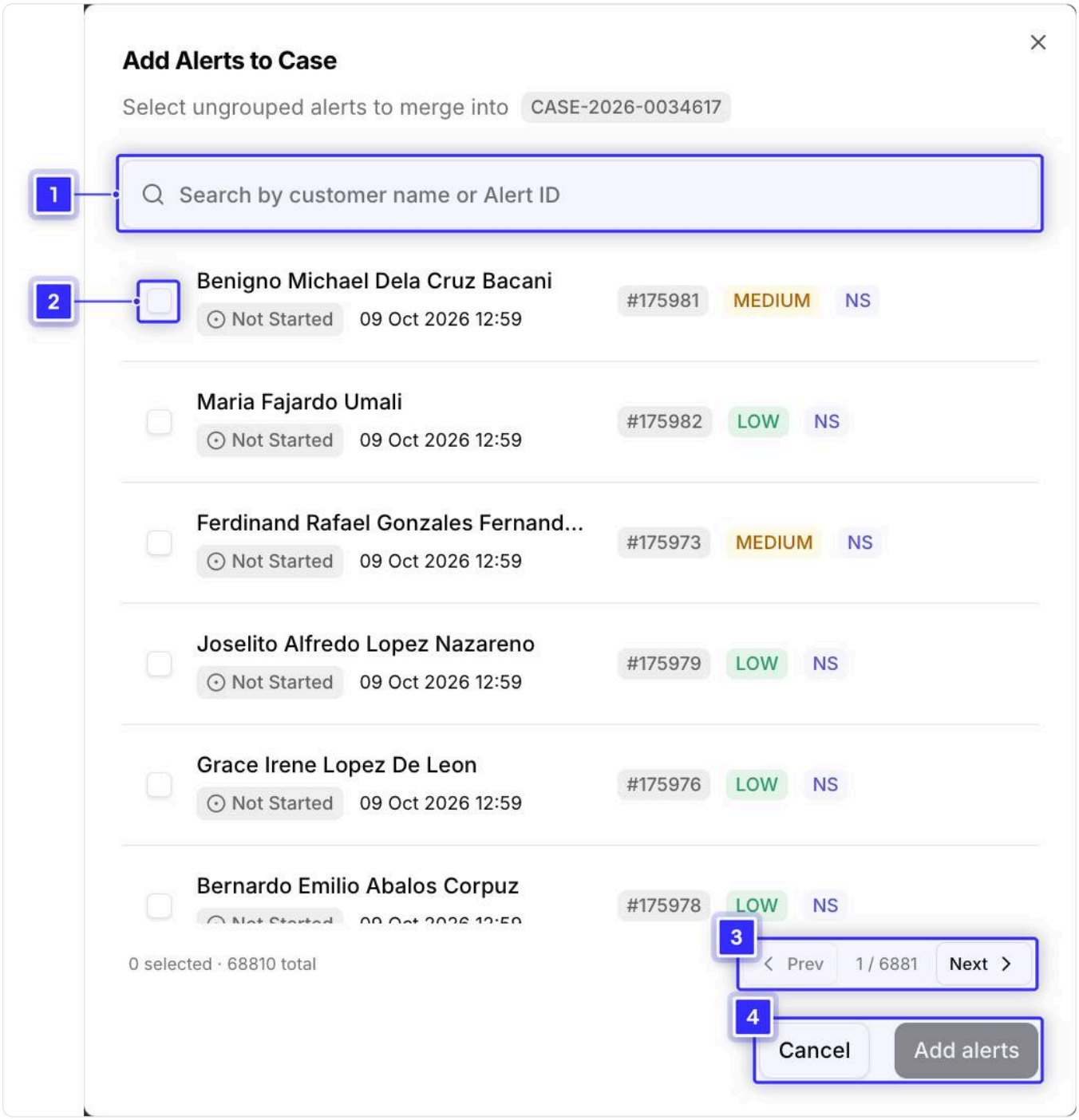


Figure 3.19 The Add Alerts to Case dialog with nothing selected: search (1), an ungrouped alert (2), the counter and paging (3), Cancel and Add alerts (4)

Step 1 **Find the alerts**

Click **Add Alerts**. Search with *Search by customer name or Alert ID*, or page through the list with **Prev** and **Next** (the page indicator reads, for example, *1 / 6738*). Each row shows the customer name, status, date and time, alert number (for example *#174489*), score band and module.

Step 2 **Select and add**

Tick the alerts to add. The counter at the bottom shows how many are selected out of the total (*0 selected · 68810 total* in the example). Click **Add alerts**, or **Cancel** to close without changes.

Which alerts are grouped into cases automatically is set in Case Creation & Assignment (see Case Manager Config).

Dispose alerts and close a case

WHERE	REQUIRED	OPTIONAL	RECORDED AS
Case Details → Dispose Alert, then the case bar Disposition	Disposition, Rationale Code, Rationale Details (10 characters or more)	Supporting Documents	A Disposition Submitted event in the case timeline

Each alert in a case gets its own disposition through **Dispose Alert**. The case has its own **Disposition** in the case bar.

Step 1 **Select the alert**

In the alert strip, click the alert's tab and review its customer, matches or transaction evidence.

Step 2 **Open Dispose Alert**

Click **Dispose Alert**. The **Dispose Alert** dialog opens for the selected alert, whose ID appears under the title.

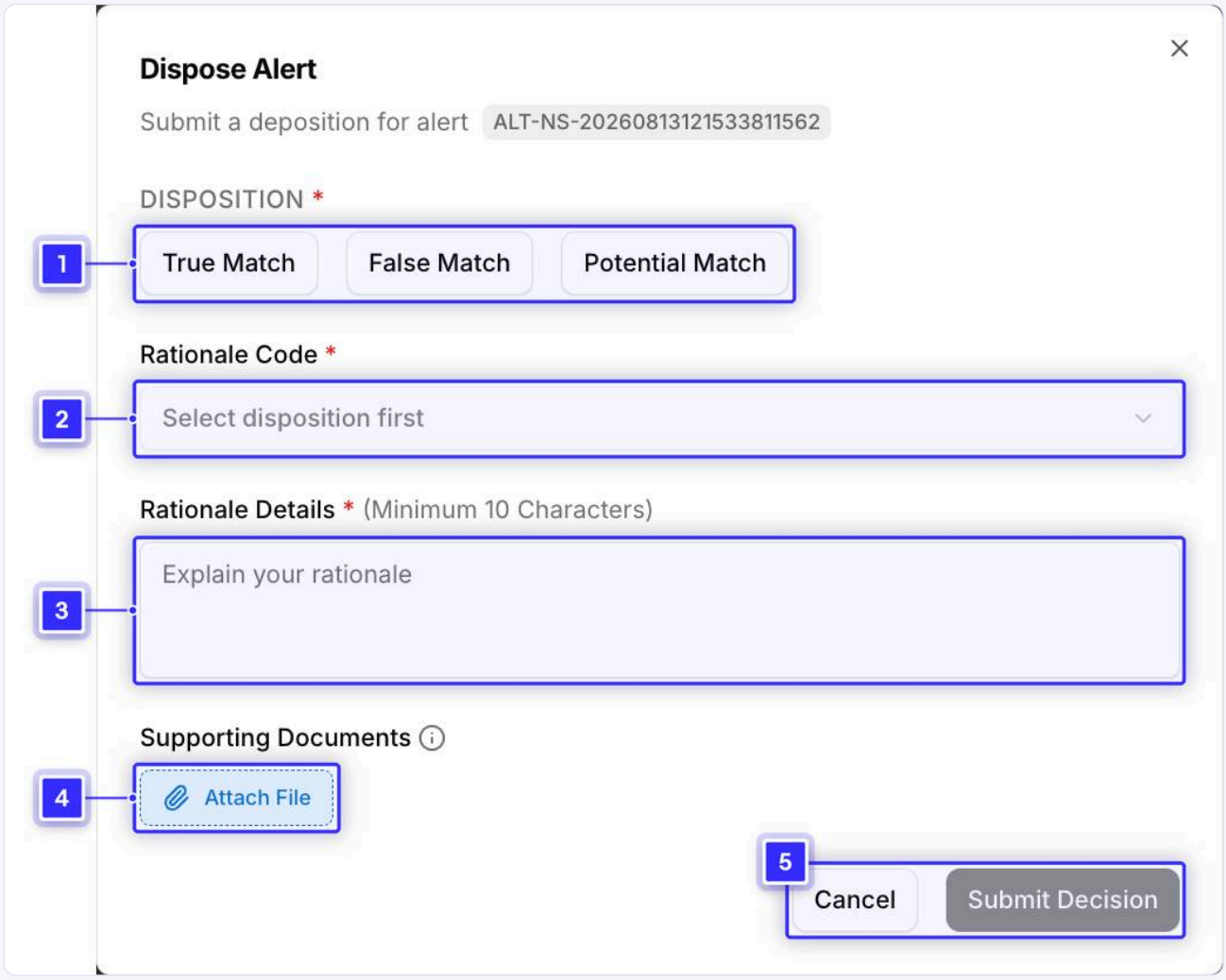


Figure 3.20 The Dispose Alert dialog: DISPOSITION (1), Rationale Code (2), Rationale Details (3), Supporting Documents (4), Cancel and Submit Decision (5)

Step 3 **Fill in the decision**

Complete the fields in the table below, then click **Submit Decision**. **Cancel** closes the dialog without saving. Repeat for each alert in the case.

Field	What it expects	Required	Options or format
DISPOSITION	The outcome for this alert	Yes	True Match, False Match, Potential Match
Rationale Code	The coded reason for the outcome	Yes	A dropdown. It reads *Select disposition first* until a disposition is chosen. Example code: *Identification number of the user is the same as the watchlist*.

Field	What it expects	Required	Options or format
Rationale Details	Your explanation (*Explain your rationale*)	Yes	Minimum 10 Characters
Supporting Documents	Files that support the decision	No	**Attach File**

Step 4 **Set the case disposition**

In the case bar, open **Disposition** (*Select Outcome*) and choose **True Match**, **False Match** or **Potential Match**.

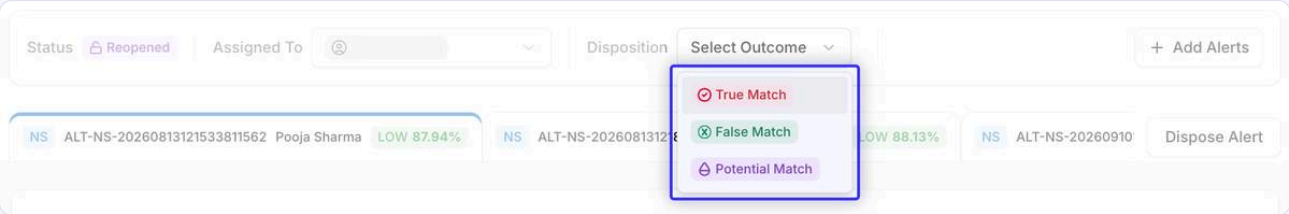


Figure 3.21 The case Disposition list open on a Reopened case: True Match, False Match and Potential Match

A closed case shows **Status** Closed, the chosen **Disposition**, and a decision block with **Rationale Code**, **Details**, **Decided On** and **Decided By**. Each alert tab shows its own disposition. The timeline records a **Disposition Submitted** event tagged **Case closed**.

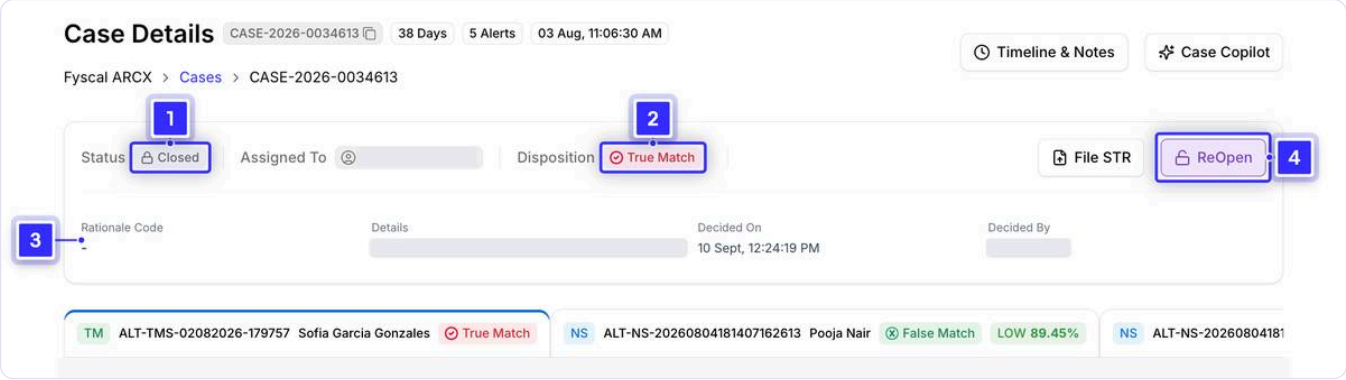


Figure 3.22 A Closed case (CASE-2026-0034613): Status Closed (1), Disposition True Match (2), the decision block (3), and File STR and ReOpen (4)

The case timelines show two ways a case has reached **Closed**:

Path	Timeline events, oldest first	Example
Direct	**Disposition Submitted**, tagged **Case closed** and the number of alerts (for example *1 Alert*)	CASE-2026-0034611
With review	**Review Requested** (tagged **Case closed**, with the disposition True Match and the rationale), then **Disposition Approved** by a second user (tagged **Case closed**, *5 Alerts*)	CASE-2026-0034613

In both paths the closing event names all of the case's alerts, so the case disposition closes the case together with its alerts.

Note

On a Reopened case with six undisposed alerts (CASE-2026-0034617), both **Dispose Alert** and the case **Disposition** are available. The steps in this guide dispose of each alert first.

AML context

Reviewers, auditors and supervisors read the rationale long after the decision. Say what you compared (for example name, date of birth, ID number or transaction pattern), what you found and why the disposition follows from it. The product checks only the minimum length of 10 characters.

Review a case in Pending Review

A case in **Pending Review** shows a **Pending Review** panel under the case bar. Use **Pending Approval** on All Cases to list these cases.

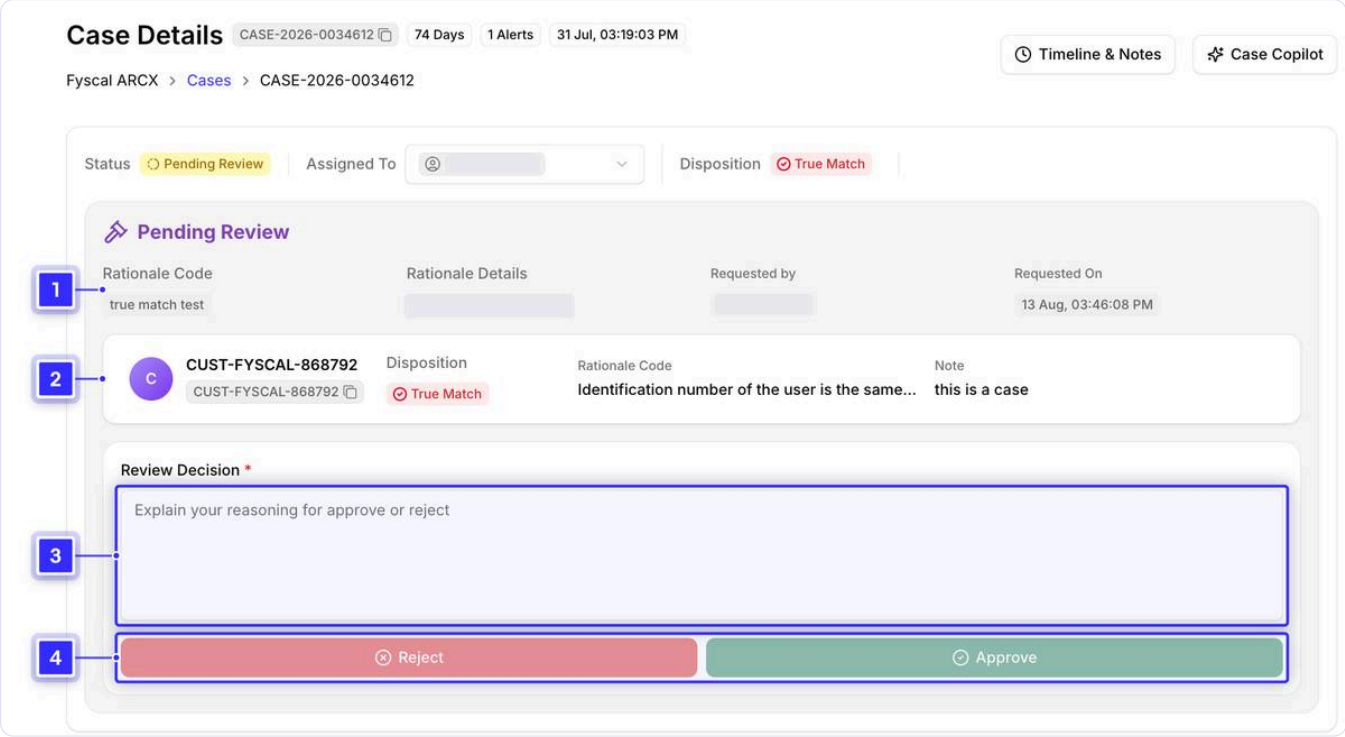


Figure 3.23 The Pending Review panel on CASE-2026-0034612: the request (1), the decision card (2), Review Decision (3), and Reject and Approve (4)

Part of the panel	What it shows
Request (1)	**Rationale Code**, **Rationale Details**, **Requested by** and **Requested On**.
Decision card (2)	The customer, **Disposition** (for example True Match), **Rationale Code** and **Note**.
Review Decision * (3)	A required text box: *Explain your reasoning for approve or reject*.
Reject / Approve (4)	The two decision buttons.

Step 1 **Record the review**

Read the request and the decision card. Type your reasoning in **Review Decision**, then click **Reject** or **Approve**.

AML context

A second review of a disposition (the "four-eyes" principle) is a common control: a different person checks that the evidence supports the decision before it stands. Write the review reasoning so that someone reading the case later can see what was checked.

Reopen a case

Cases in **Closed**, **STR Draft** and **STR Created** show **ReOpen** in the case bar.

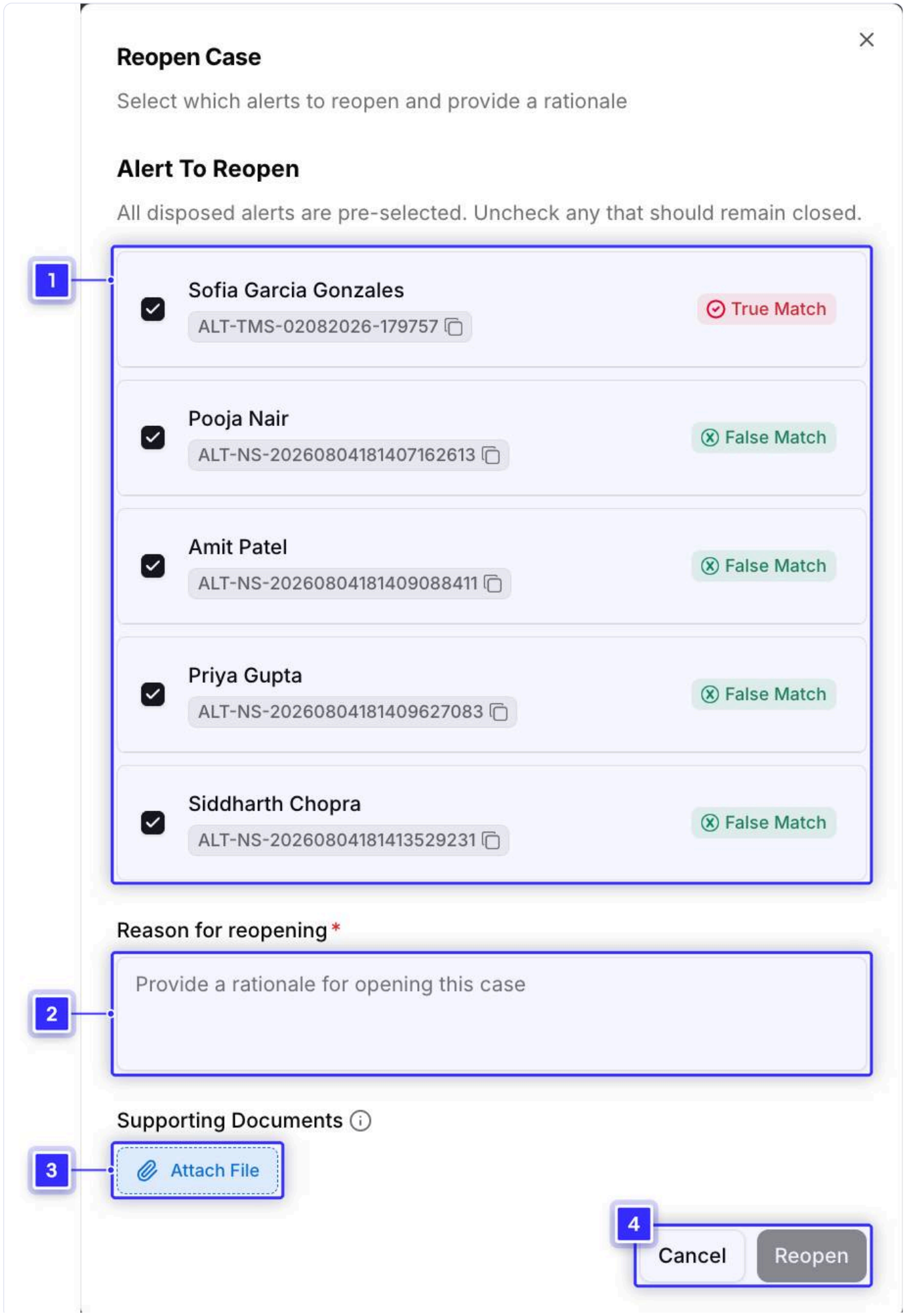

Reopen Case
Select which alerts to reopen and provide a rationale
Alert To Reopen
All disposed alerts are pre-selected. Uncheck any that should remain closed.
1
Sofia Garcia Gonzales
ALT-TMS-02082026-179757
True Match
Pooja Nair
ALT-NS-20260804181407162613
False Match
Amit Patel
ALT-NS-20260804181409088411
False Match
Priya Gupta
ALT-NS-20260804181409627083
False Match
Siddharth Chopra
ALT-NS-20260804181413529231
False Match
Reason for reopening *
2
Provide a rationale for opening this case
Supporting Documents
3
Attach File
4
Cancel
Reopen

Figure 3.24 The Reopen Case dialog: Alert To Reopen with all disposed alerts pre-selected (1), Reason for reopening (2), Supporting Documents (3), Cancel and Reopen (4)

Step 1 **Choose the alerts**

Click **ReOpen**. The **Reopen Case** dialog lists the case's alerts under **Alert To Reopen**, each with its disposition. *All disposed alerts are pre-selected. Uncheck any that should remain closed.*

Step 2 **Give the reason**

Enter **Reason for reopening** (required; *Provide a rationale for opening this case*). Optionally add **Supporting Documents** with **Attach File**. Click **Reopen**, or **Cancel**.

A reopened case has the status **Reopened**, and its timeline shows a **Reopened** event with the previous status, the rationale and the reopened alerts.

File an STR

Fyscal ARCX → Case Manager → Cases → (open a case) → File STR or Preview STR

WHERE	FORMAT	STEPS	AFTERWARDS
Case Details → File STR, or Preview STR for a draft	GoTRACS-compliant STR for the AMLC	Six, from Select Alerts to Narratives	The filed STR is listed in Regulatory Reports

The STR wizard, titled **Suspicious Transaction Report (STR)** with the subtitle *GoTRACS-compliant STR filing for AMLC*, prepares a Suspicious Transaction Report for the AMLC from a case. It opens over Case Details and shows the case ID in its header. The case bar shows the STR button that matches the case status:

Case status	STR button	What it does
Closed (in the examples, with disposition **True Match**)	**File STR**	Opens the wizard to file an STR for the case.
STR Draft	**Preview STR**	Reopens the saved draft at the step where it was left.
STR Created	**Download STR**	Shown once the STR has been filed (see After the STR is filed).

Before you start

- Dispose the case's alerts and close the case first (see Dispose alerts and close a case). **File STR** appears only once the case is closed: open cases (for example Reopened) show **Dispose Alert** and the **Disposition** list instead, and no STR button. In the examples, **File STR** is shown on a **Closed** case with the disposition **True Match**.
- After the STR is created, the timeline records an **STR Created** event and the case bar shows **Download STR** in place of **File STR** (CASE-2026-0034611).
- You need at least one suspicious transaction for step 4. **Select Suspicious Transactions** is required, and **Next Step** stays disabled while no transaction is selected (see Common blocks).
- Have the **Date of determination** ready. On step 2 it sets the **Filing deadline** message shown next to it.

AML context

A Suspicious Transaction Report tells the financial intelligence unit what happened, who was involved and why it is suspicious. Reports are expected within a set time of the point at which suspicion is formed, which is why the wizard asks for the date of determination and shows a filing deadline.

The six steps

The progress bar across the top of the wizard shows the six steps. The current step has a blue number; a step already completed shows a green tick; later steps show a grey number.



Figure 3.25 The STR wizard for CASE-2026-0107624: the title and case ID (1), steps 1 to 3 completed (2), step 4 Transaction current (3), the later steps (4) and the close button (5)

1. The title, **Suspicious Transaction Report (STR)**, with *GoTRACS-compliant STR filing for AMLC* and the case ID.
2. Steps already completed show a green tick (here steps 1 to 3).
3. The current step has a blue number (here step 4, **Transaction**).

4 Later steps show a grey number.
5 The close button (×).

Step	Name	What you do
1	**Select Alerts**	Choose which of the case's alerts the STR covers.
2	**Report Type**	Choose the STR type and fill in the report header, including the date of determination.
3	**Reason for suspicion**	Tick the SC, PC or MC reason codes.
4	**Transaction**	Select the suspicious transactions to report.
5	**Subject parties**	Check the parties derived from the selected transactions.
6	**Narratives**	Write the STR narrative.

Control	Where it appears	What it does
Next Step	Footer, right	Moves to the next step. Greyed out while a required entry on the step is missing (seen on step 4).
Previous Step	Footer, left; not shown on step 1	Moves back one step.
Save as draft	Footer, next to Next Step, while the STR is a draft	Saves your entries as a draft. Not shown when a filed STR is opened read-only from Regulatory Reports.
×	Top right of the wizard	Closes the wizard and returns to Case Details.

The codes after field names, such as *H-3* or *D-SD-2*, are the GoTRACS field codes shown on screen. A red * marks a required field.

Open the STR wizard

Open the wizard from the case: with **File STR** to start an STR, or with **Preview STR** to continue a saved draft.

Step 1 **Start an STR from a closed True Match case**

Open the case in Case Details. Check that **Status** reads **Closed** and **Disposition** reads **True Match**, then click **File STR** in the case bar.

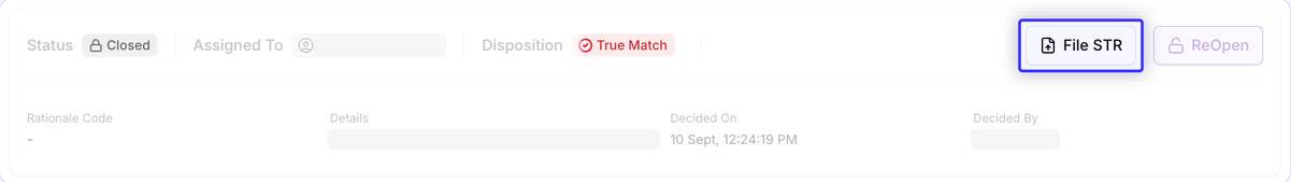


Figure 3.26 File STR in the case bar of a Closed case with disposition True Match (CASE-2026-0034613)

Step 2 **Find a case with a saved draft**

To continue a draft, go to **Cases**, open the **All Cases** tab and type the case ID in *Search by Case Title / ID or Customer Name*. The case shows the status **STR Draft**. Click the row to open the case. To list every draft, set the **Status** filter to **STR Draft** (see Filter and search cases).

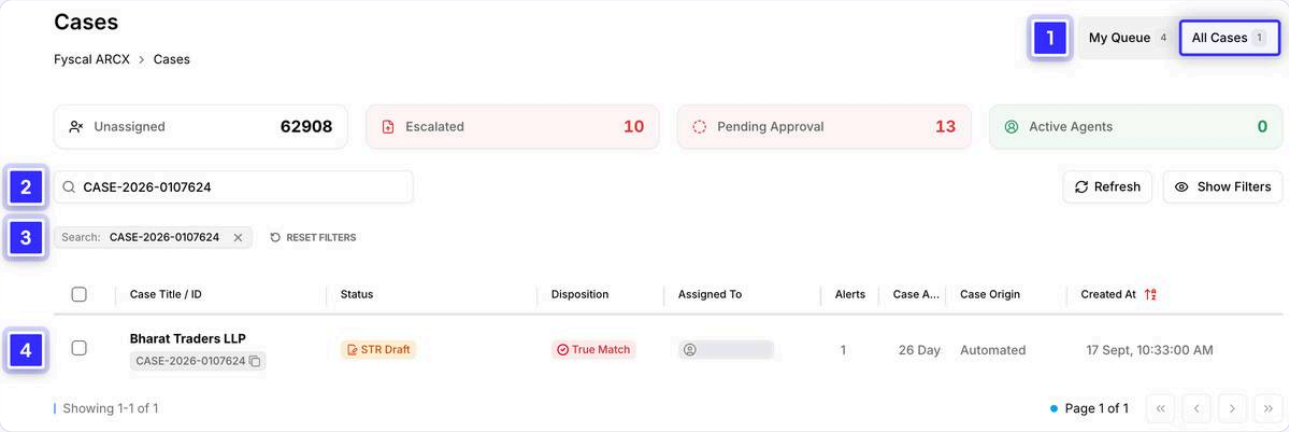


Figure 3.27 All Cases (1) searched for CASE-2026-0107624 (2), with the active-filter tag (3): one case, Bharat Traders LLP, in STR Draft (4)

Step 3 **Reopen the draft**

Click **Preview STR** in the case bar. The wizard opens at the step where the draft was left. In the example it opens at step 4 **Transaction**, with steps 1 to 3 ticked (Figure 3.25). Use **Previous Step** to go back to earlier steps.

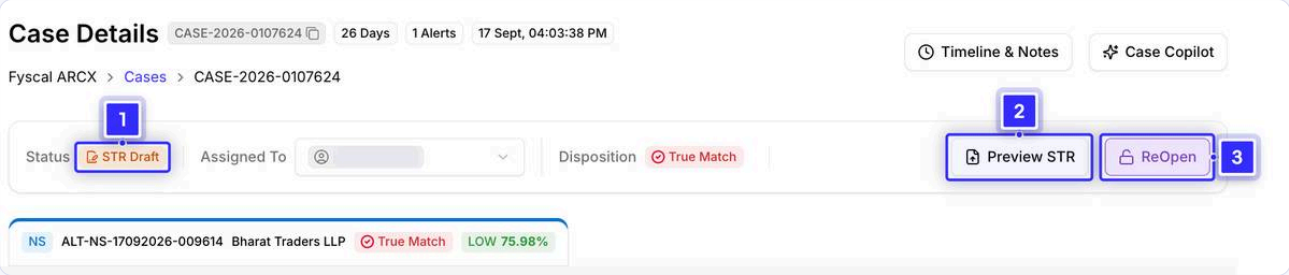


Figure 3.28 An STR Draft case (CASE-2026-0107624, Bharat Traders LLP): the STR Draft status (1), Preview STR (2) and ReOpen (3)

Step 1: Select Alerts

Choose which of the case's alerts the STR covers. The screen states: *Transactions and parties from selected alerts appear in subsequent steps.*

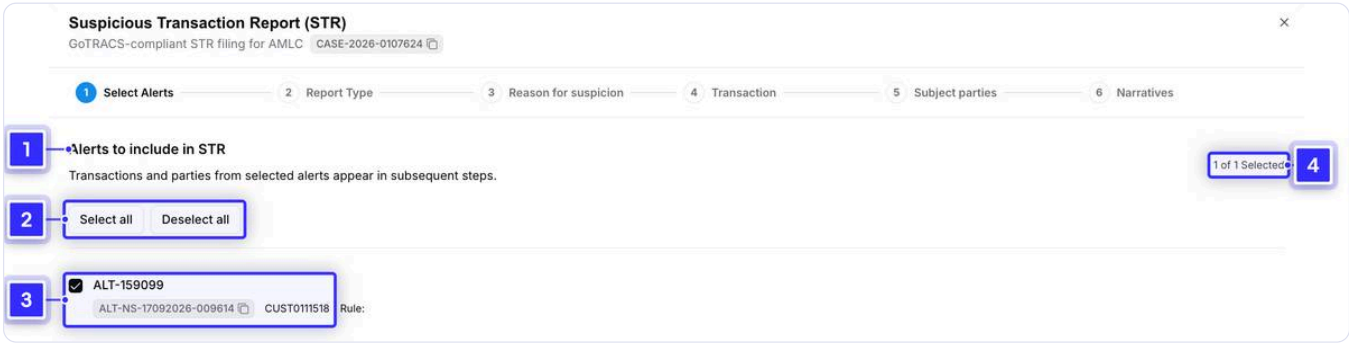


Figure 3.29 Step 1, Select Alerts, for CASE-2026-0107624: the instruction (1), Select all and Deselect all (2), one alert, ALT-159099, selected (3), and the counter (4)

1. **Alerts to include in STR**, with the instruction above.
2. **Select all** and **Deselect all**.
3. An alert row: a checkbox, the alert number (*ALT-159099*), the alert ID (*ALT-NS-17092026-009614*) with a copy icon, the customer ID (*CUST0111518*) and **Rule:**. A Name Screening alert shows **Rule:** with no value; a Transaction Monitoring alert shows its rule and its number of transactions (see Regulatory Reports, step 1).
4. The counter, *1 of 1 Selected*.

The footer of step 1, below the list, holds **Save as draft** and **Next Step**. Step 1 has no **Previous Step**.

Field	Code	Required	What to enter or the options
Alerts to include in STR	None shown	No marker	One checkbox per alert in the case. **Select all** ticks every alert; **Deselect all** clears them. The counter shows how many are selected out of the total.

Step 1 **Tick the alerts to report**

Tick each alert the STR should cover, or click **Select all**. Untick any alert to leave out. Check the counter (for example *1 of 1 Selected*).

Step 2 **Go to step 2**

Click **Next Step**. Step 1 now shows a green tick and step 2 **Report Type** opens.

Step 2: Report Type

Choose the type of STR and complete the report header. The values in the figures are those saved in the draft for CASE-2026-0107624.

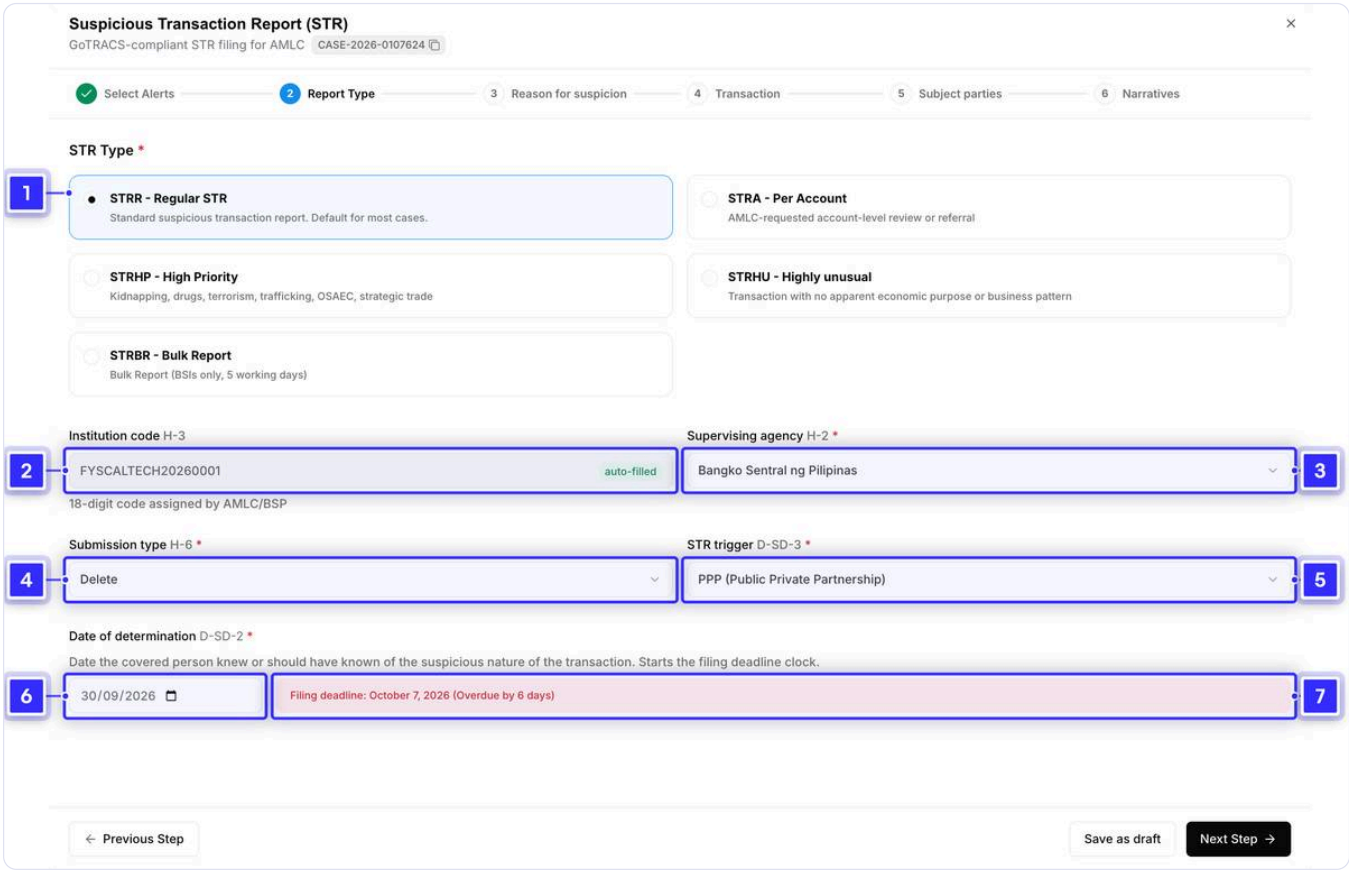


Figure 3.30 Step 2, Report Type: STR Type (1), Institution code (2), Supervising agency (3), Submission type (4), STR trigger (5), Date of determination (6) and the Filing deadline message (7)

#	Field	Code	Required	What to enter or the options
1	STR Type	None shown	Yes (*)	One of five radio-button cards: **STRR - Regular STR**, **STRA - Per Account**, **STRHP - High Priority**, **STRHU - Highly unusual** and **STRBR - Bulk Report**. See STR types compared below.
2	Institution code	H-3	No marker	Greyed out and tagged **auto-filled**; you do not type it. Help text: *18-digit code assigned by AMLC/BSP*. Example: *FYSCALTECH20260001*.
3	Supervising agency	H-2	Yes (*)	Bangko Sentral ng Pilipinas; Securities and Exchange Commission; Insurance Commission; Designated Non-Financial Businesses and Professions; Philippine Amusement and Gaming Corporation; Cagayan Economic Zone Authority; Aurora Pacific Economic Zone and Freeport; People's Bank Supervised by BSP (Figure 3.31).

#	Field	Code	Required	What to enter or the options
4	Submission type	H-6	Yes (*)	New; Edit/Correction; Delete; Test (Figure 3.32).
5	STR trigger	D-SD-3	Yes (*)	CP (proactive/alerts); PPP (Public Private Partnership); KYC Docs requested by AMLC/AMLC Referrals; Shared AMLC Studies; Watch list; Freeze Orders; Targeted Financial Sanctions (TFS) (Figure 3.33).
6	Date of determination	D-SD-2	Yes (*)	A date, dd/mm/yyyy, typed or picked from the calendar icon. Help text: *Date the covered person knew or should have known of the suspicious nature of the transaction. Starts the filing deadline clock.*
7	Filing deadline	None shown	Not an entry	A message beside the date, worked out from it. It changes with the current date. For 30/09/2026 it read *Filing deadline: October 7, 2026 (Due today!)* on 7 October and *Filing deadline: October 7, 2026 (Overdue by 6 days)* on 13 October.

STR types compared

Each **STR Type** card carries a short description. The table sets the five cards side by side, using only what the cards say.

On the card	STRR	STRA	STRHP	STRHU	STRBR
Name	Regular STR	Per Account	High Priority	Highly unusual	Bulk Report
Description	Standard suspicious transaction report. Default for most cases.	AMLC-requested account-level review or referral	Kidnapping, drugs, terrorism, trafficking, OSAEC, strategic trade	Transaction with no apparent economic purpose or business pattern	Bulk Report (BSIs only, 5 working days)
Described as the default	✓ Yes	✗ No	✗ No	✗ No	✗ No
Linked to an AMLC request or referral	✗ No	✓ Yes	✗ No	✗ No	✗ No
Names specific crimes	✗ No	✗ No	✓ Yes	✗ No	✗ No
Limited to some institutions	✗ No	✗ No	✗ No	✗ No	✓ Yes BSIs only
States a time limit	✗ No	✗ No	✗ No	✗ No	✓ Yes 5 working days

AML context

Pick the type from what the investigation found, not from the alert that started it. A transaction that matches none of the listed crimes but has no economic sense fits the "highly unusual" description; a report about one of the serious crimes named on the High Priority card fits that card. If more than one could apply, follow your institution's procedure or ask your compliance officer.

Step 1 **Choose the STR type**

Under **STR Type**, click the card that fits the report. The chosen card has a filled radio button and a blue border.

Step 2 **Check the institution code**

Institution code is filled in for you. Check that it is your institution's code.

Step 3 **Choose the supervising agency**

Click **Supervising agency** and click your institution's supervising agency. The current choice is ticked.

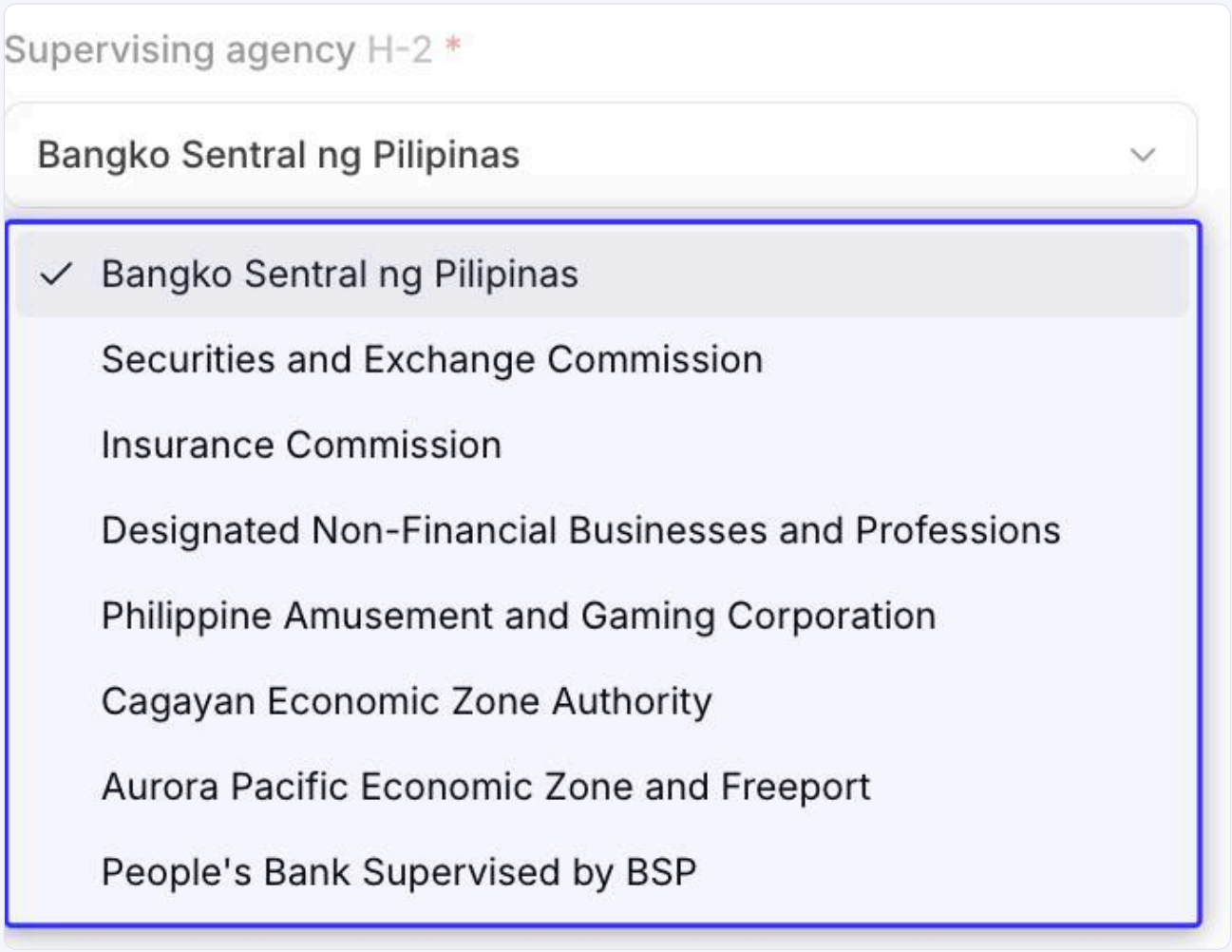


Figure 3.31 The Supervising agency list, with Bangko Sentral ng Pilipinas ticked

Step 4 **Choose the submission type**

Click **Submission type** and choose **New**, **Edit/Correction**, **Delete** or **Test**.

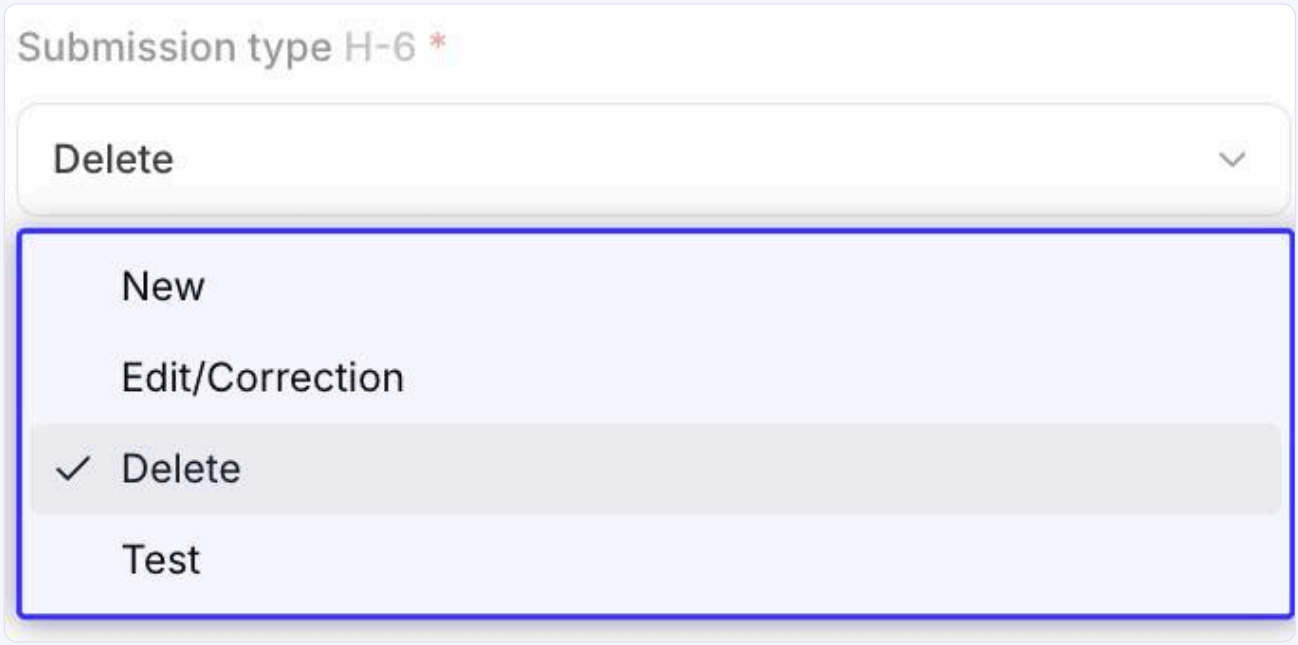


Figure 3.32 The Submission type list, with Delete ticked in the example draft

Step 5 **Choose the STR trigger**

Click **STR trigger** and choose what led to the report.

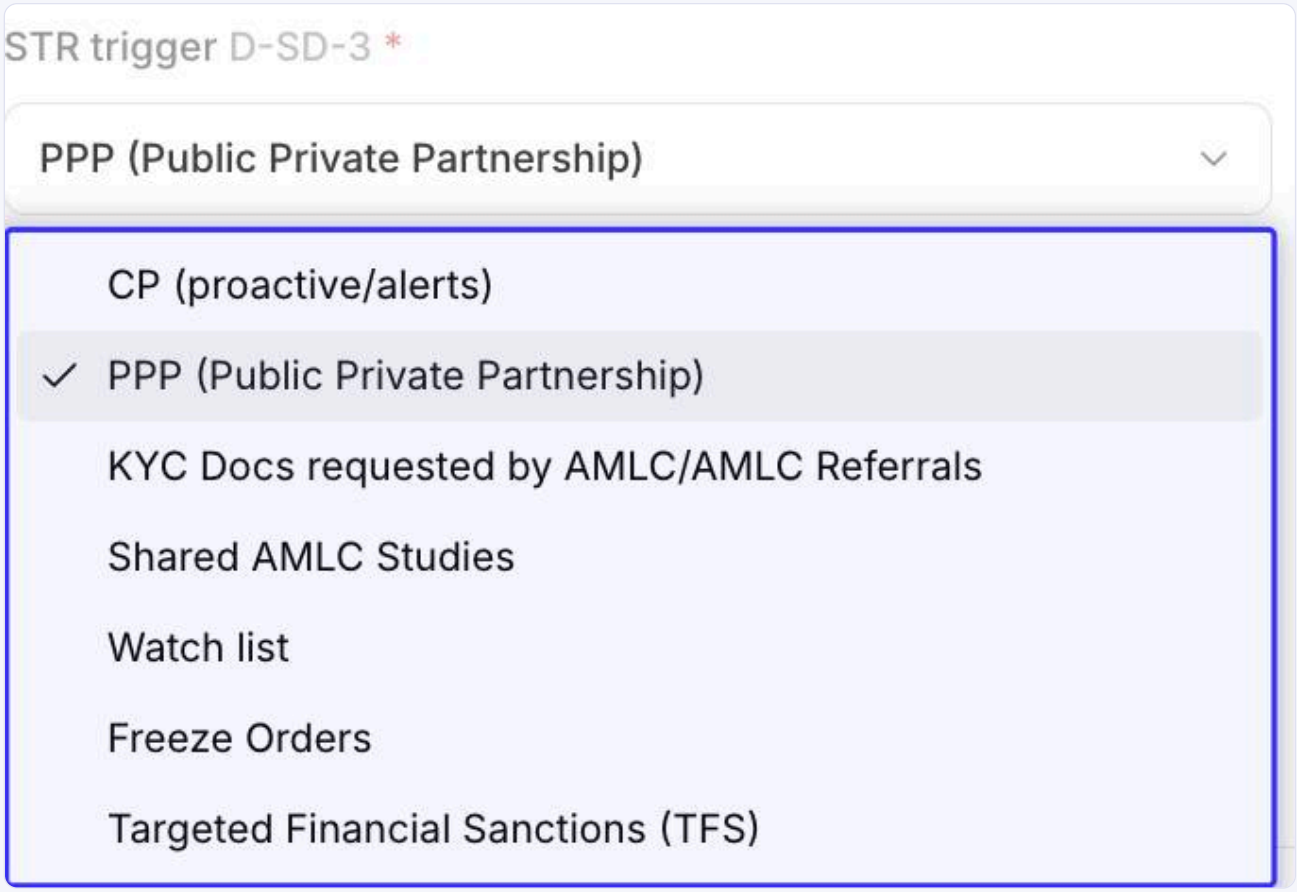


Figure 3.33 The STR trigger list, with PPP (Public Private Partnership) ticked

Step 6 **Enter the date of determination**

In **Date of determination**, enter the date as dd/mm/yyyy or pick it from the calendar icon. Read the **Filing deadline** message that appears beside it (number 7 in Figure 3.30). In the example, 30/09/2026 gives a deadline of October 7, 2026; viewed on 13 October the message reads *Filing deadline: October 7, 2026 (Overdue by 6 days)*, in red.

Step 7 **Go to step 3**

Click **Next Step**. Step 2 now shows a green tick and step 3 **Reason for suspicion** opens.

Step 3: Reason for suspicion

Tick the reason codes that explain why the transactions are suspicious. There are two lists: the required primary codes and optional additional codes. Each list scrolls inside the wizard.

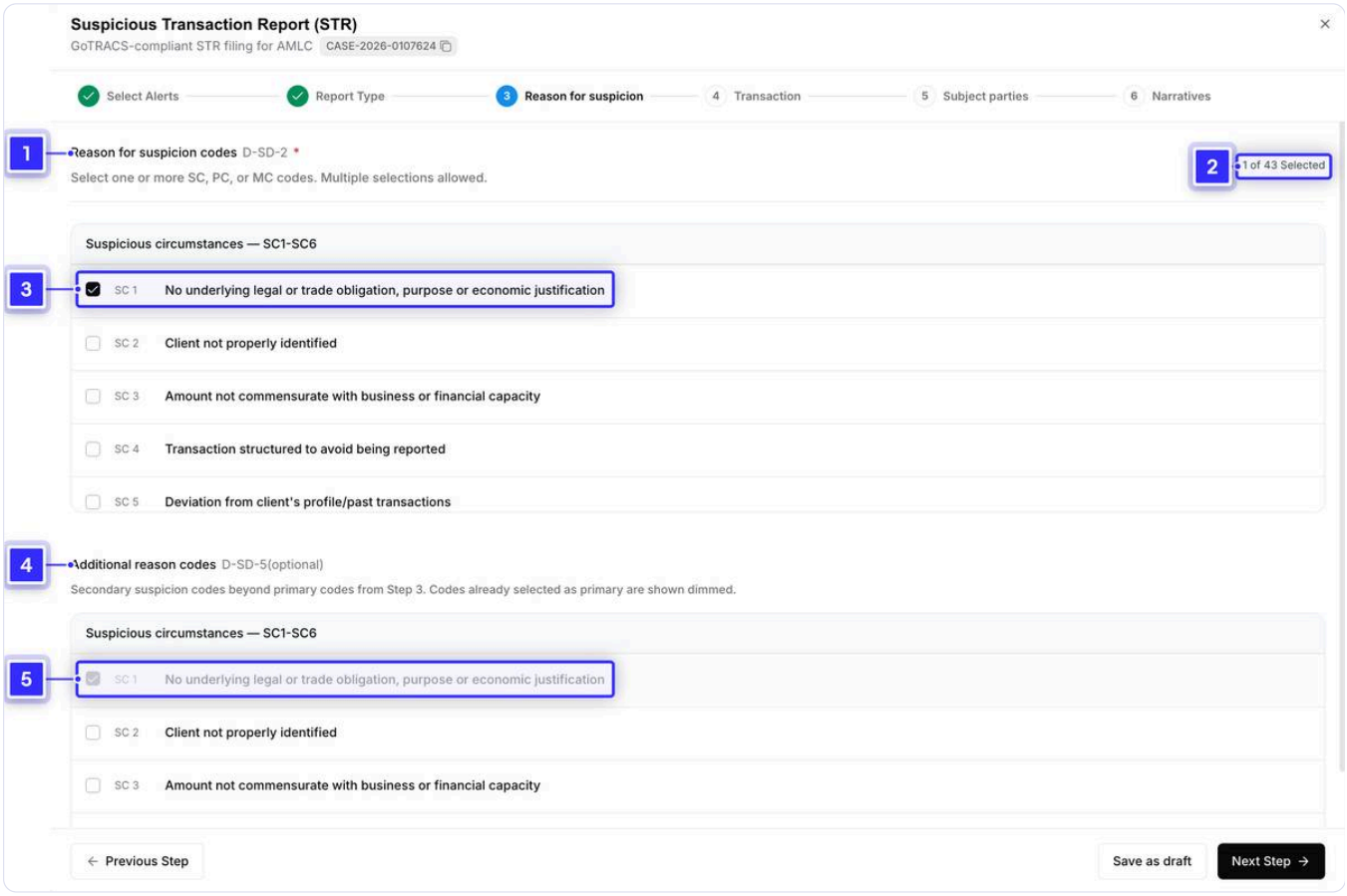


Figure 3.34 Step 3, Reason for suspicion: SC 1 ticked as a primary code and shown dimmed under Additional reason codes

1. **Reason for suspicion codes** D-SD-2 (required): *Select one or more SC, PC, or MC codes. Multiple selections allowed.*
2. The counter, *1 of 43 Selected*. The lists hold 43 codes: SC 1 to SC 6, PC 1 to PC 36 and MC 01.
3. A ticked code (**SC 1** in the example).
4. **Additional reason codes** D-SD-5 (optional): *Secondary suspicion codes beyond primary codes from Step 3. Codes already selected as primary are shown dimmed.*
5. The same code, dimmed in the additional list because it is already a primary code.

Field	Code	Required	What to enter or the options
Reason for suspicion codes	D-SD-2	Yes (*)	One or more codes, in three groups: **Suspicious circumstances — SC1-SC6**, **Predicate crimes — PC1-PC36** and **Transnational organized crime — MC1**. See the code table below.
Additional reason codes	D-SD-5	No (labelled *(optional)*)	The same three groups. Codes already ticked as primary are dimmed.

Step 1 **Tick the primary codes**

Under **Reason for suspicion codes**, scroll the list and tick each code that applies. The counter shows how many are ticked.

Step 2 **Check KYC REQ on predicate crimes**

Scroll to **Predicate crimes — PC1-PC36**. Most predicate-crime codes carry a yellow **KYC REQ** tag at the right; PC 4, PC 5, PC 13 and PC 35 do not.

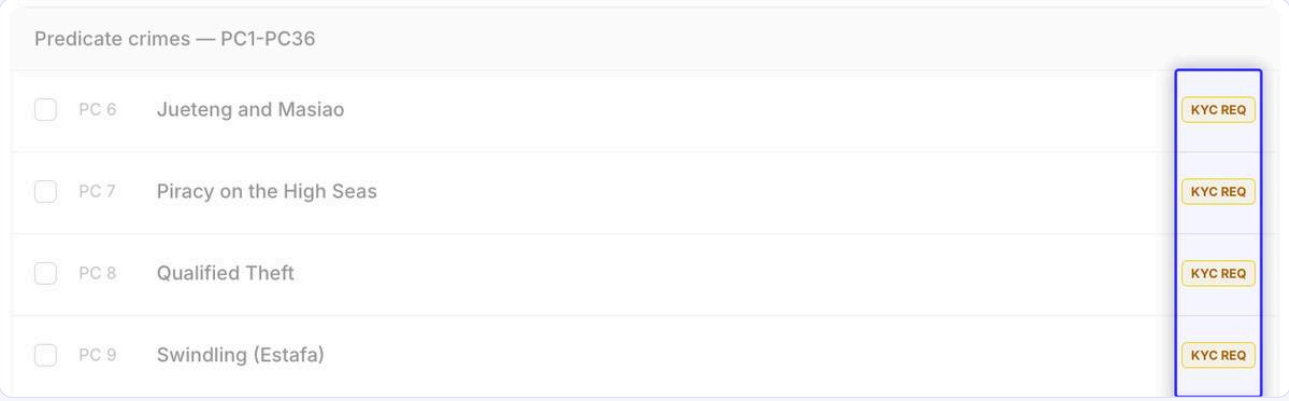


Figure 3.35 Predicate crimes PC 6 to PC 9, each with a KYC REQ tag

Step 3 **Add MC 01 where it applies**

At the end of the list, **Transnational organized crime — MC1** holds one code, **MC 01**: *Transnational Organized Crime (used with another predicate crime).*

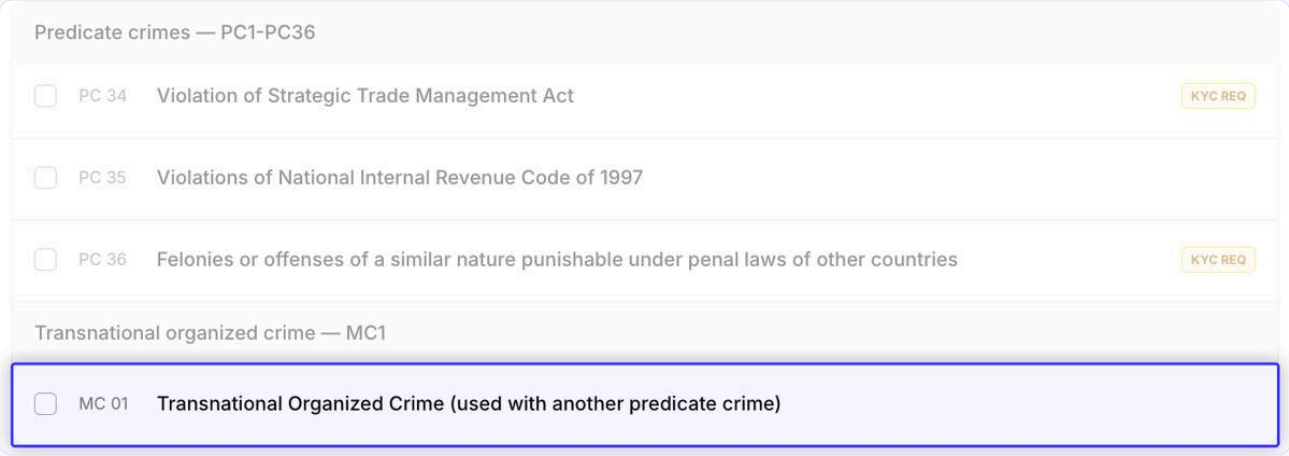


Figure 3.36 The end of the primary list: PC 34 to PC 36 and MC 01

Step 4 **Tick any additional codes**

Under **Additional reason codes**, tick any secondary codes. Codes already ticked above are dimmed here.

Step 5 **Go to step 4**

Click **Next Step**. Step 3 now shows a green tick and step 4 **Transaction** opens.

Code	Description on screen	KYC REQ tag
SC 1	No underlying legal or trade obligation, purpose or economic justification	No
SC 2	Client not properly identified	No
SC 3	Amount not commensurate with business or financial capacity	No
SC 4	Transaction structured to avoid being reported	No
SC 5	Deviation from client's profile/past transactions	No
SC 6	Transaction similar, analogous or identical to any of the foregoing	No

Code	Description on screen	KYC REQ tag
PC 1	Kidnapping for Ransom	Yes
PC 2	Drug Trafficking and Related Offenses	Yes
PC 3	Graft and Corrupt Practices	Yes
PC 4	Plunder	No
PC 5	Robbery and Extortion	No
PC 6	Jueteng and Masiao	Yes
PC 7	Piracy on the High Seas	Yes
PC 8	Qualified Theft	Yes
PC 9	Swindling (Estafa)	Yes
PC 10	Smuggling	Yes
PC 11	Violations under the Electronic Commerce Act of 2000	Yes
PC 12	Hijacking; Destructive Arson; and Murder	Yes
PC 13	Terrorism and Conspiracy to Commit Terrorism	No
PC 14	Financing of Terrorism	Yes
PC 15	Bribery	Yes
PC 16	Frauds and Illegal Exactions and Transactions	Yes
PC 17	Malversation of Public Funds and Property	Yes
PC 18	Forgeries and Counterfeiting	Yes
PC 19	Violations of Anti-Trafficking in Persons Act of 2003	Yes
PC 20	Violations of Revised Forestry Code of the Philippines	Yes
PC 21	Violations of Fisheries Code of 1998	Yes
PC 22	Violations of Philippine Mining Act of 1995	Yes
PC 23	Violations of Wildlife Resources Conservation and Protection Act	Yes
PC 24	Violation of National Caves and Cave Resources Management and Protection Act	Yes
PC 25	Violation of Anti-Carnapping Act of 2002	Yes
PC 26	Violations of Illegal Possession of Firearms, Ammunition or Explosives	Yes
PC 27	Violation of Anti-Fencing Law	Yes
PC 28	Violation of Migrant Workers and Overseas Filipinos Act of 1995	Yes
PC 29	Violation of Intellectual Property Code	Yes
PC 30	Violation of Anti-Photo and Video Voyeurism Act of 2009	Yes
PC 31	Violation of Anti-OSAEC and Anti-CSAEM Act	Yes
PC 32	Violations of RA 7610, Special Protection of Children Against Abuse	Yes
PC 33	Fraudulent Practices under Securities Regulation Code of 2000	Yes
PC 34	Violation of Strategic Trade Management Act	Yes

Code	Description on screen	KYC REQ tag
PC 35	Violations of National Internal Revenue Code of 1997	No
PC 36	Felonies or offenses of a similar nature punishable under penal laws of other countries	Yes
MC 01	Transnational Organized Crime (used with another predicate crime)	No

Note
On screen, **Reason for suspicion codes** and **Date of determination** (step 2) both carry the code D-SD-2.

Step 4: Transaction

Select the suspicious transactions to include in the STR. The list holds the triggered transactions of the alerts selected in step 1. In the example below, the case's only alert is a Name Screening alert, the list is empty and **Next Step** is greyed out.

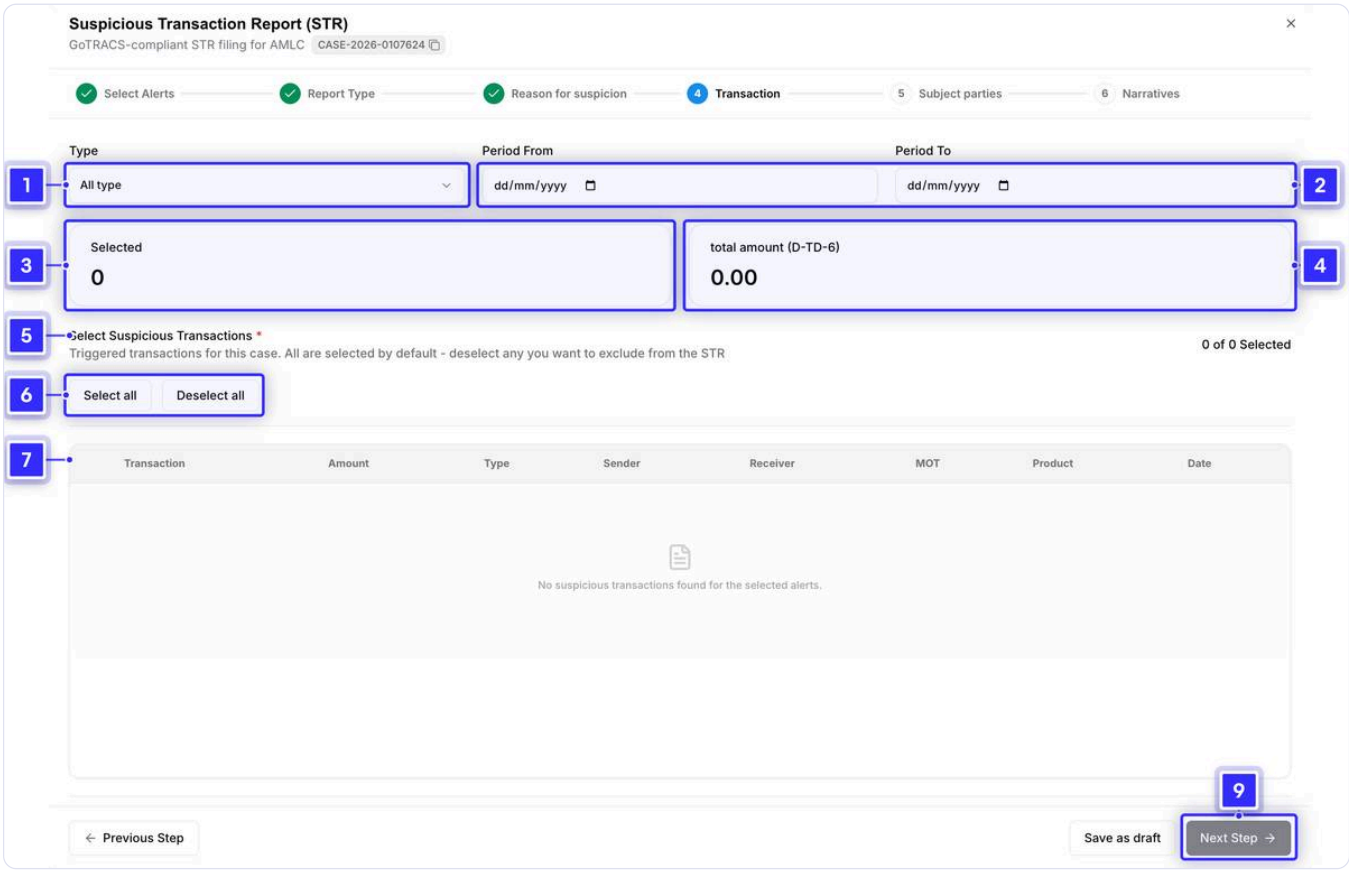


Figure 3.37 Step 4, Transaction, for CASE-2026-0107624: no suspicious transactions found, and Next Step greyed out (9); the numbers follow the list below

1. **Type** filter.
2. **Period From** and **Period To** date filters.
3. **Selected**: the number of transactions selected.
4. **total amount (D-TD-6)**: the total of the selected transactions. When they are in different currencies it is labelled **Mixed** (see Regulatory Reports, step 4).
5. **Select Suspicious Transactions** (required): *Triggered transactions for this case. All are selected by default - deselect any you want to exclude from the STR*. The counter at the right reads, for example, *0 of 0 Selected.*
6. **Select all** and **Deselect all**.
7. The transaction table, with the columns Transaction, Amount, Type, Sender, Receiver, MOT, Product and Date. With no transactions it reads *No suspicious transactions found for the selected alerts.*
8. **Party Role** legend for the letters shown next to each sender and receiver.
9. **Next Step**, greyed out while no transaction is selected.

Field	Code	Required	What to enter or the options
Type	None shown	No marker	A list with one option, **All type** (Figure 3.38).
Period From	None shown	No marker	A date, dd/mm/yyyy.
Period To	None shown	No marker	A date, dd/mm/yyyy.
Selected	None shown	Not an entry	The count of selected transactions.
total amount	D-TD-6	Not an entry	The total of the selected transactions.
Select Suspicious Transactions	None shown	Yes (*)	One checkbox per transaction. All are selected by default.

Party Role letter	Meaning
S	Subject of Suspicion
B	Beneficiary
C	Counterparty
T	Transactor
O	Other participant

Step 1 **Narrow the list if needed**

Set **Period From** and **Period To** to limit the list to a date range. **Type** offers only **All type**.



Figure 3.38 The Type filter open, with its only option, All type

Step 2 **Choose the transactions**

All triggered transactions are selected by default. Untick any transaction to leave out of the STR, or use **Select all** and **Deselect all**. Check **Selected** and **total amount (D-TD-6)**.

Step 3 **Read the note and go to step 5**

Scroll to the bottom of the step. The note reads: *MOT, Product Type, Purpose of Remittance, and Transaction Code are sourced from ingested data and included automatically in the Format X CSV per selected transaction. Total amount can be manually overridden below.* Click **Next Step**. It is greyed out while no transaction is selected.

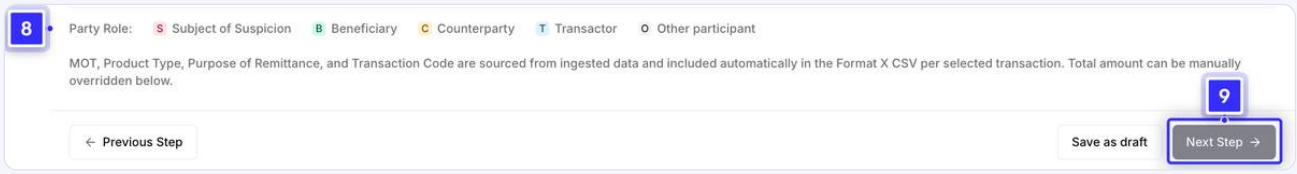


Figure 3.39 The bottom of step 4: the Party Role legend (8), the note on ingested data, and Next Step greyed out (9)

Note

The note says the total amount can be overridden below, but no field for overriding it is shown on this step.

Step 5: Subject parties

Check the parties named in the STR. The screen states: *Auto-derived from selected transactions. Click a row to expand and edit.* Each party row shows an **AH** tag, the name as *Last, First* (or *Last, First, Middle*) and the customer ID.

The figure comes from a filed STR (STR 694, CASE-2026-0000075) opened read-only from Regulatory Reports, so its fields appear greyed.

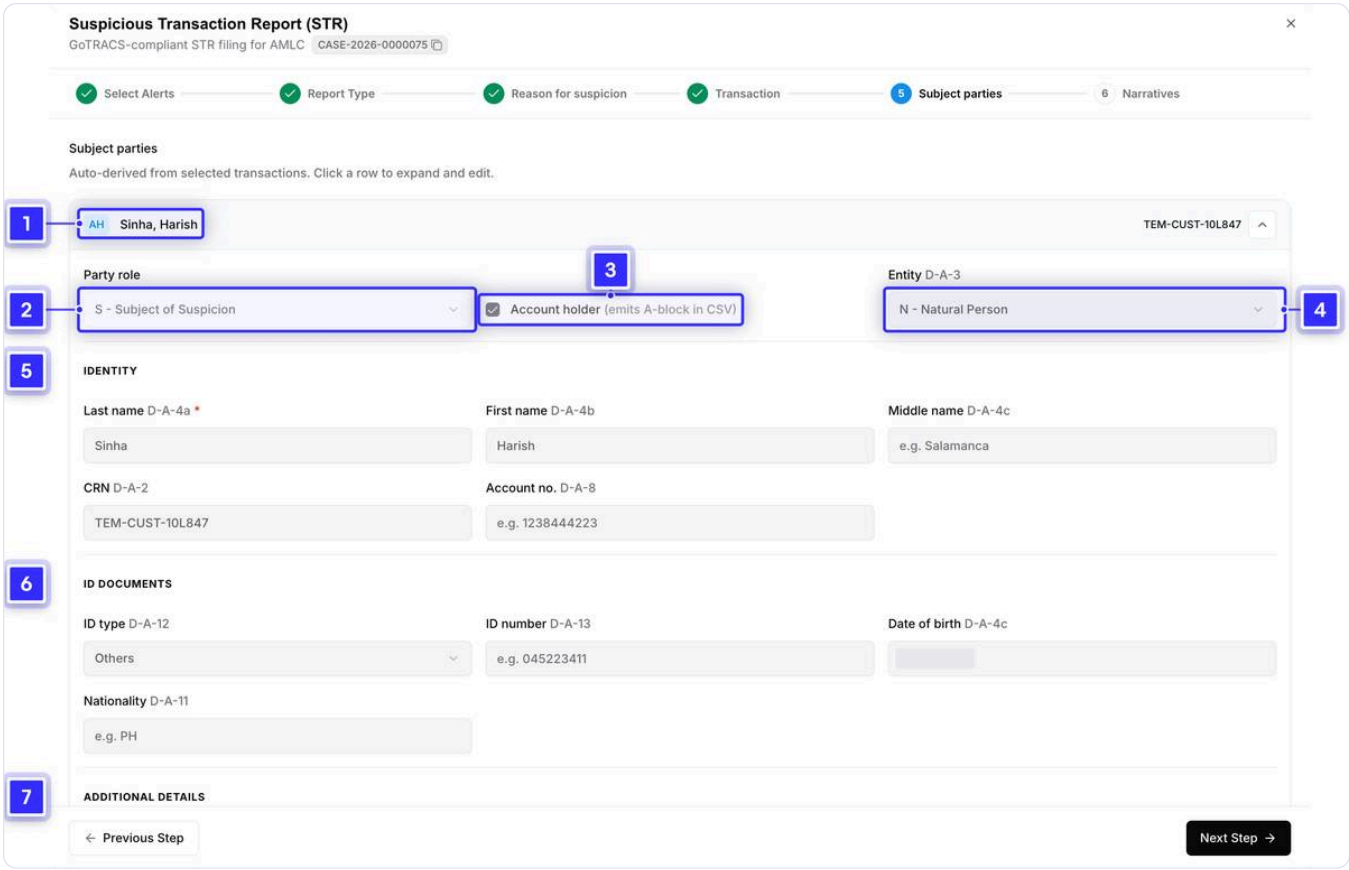


Figure 3.40 Step 5, Subject parties, in a filed STR viewed read-only: the party Sinha, Harish expanded (1), Party role (2), Account holder (3), Entity (4), IDENTITY (5), ID DOCUMENTS (6) and ADDITIONAL DETAILS (7)

1. The party row (**Sinha, Harish**). The customer ID (*TEM-CUST-10L847*) is at the right; the arrow collapses the row.
2. **Party role**.
3. **Account holder** checkbox, labelled *(emits A-block in CSV)*.
4. **Entity** D-A-3.
5. **IDENTITY** fields.
6. **ID DOCUMENTS** fields.
7. **ADDITIONAL DETAILS** fields, further down (scroll the wizard).

Field	Code	Required	What to enter or the options
Party role	None shown	No marker	A list. Example value: *S - Subject of Suspicion*.
Account holder	None shown	No marker	Checkbox, labelled *(emits A-block in CSV)*.
Entity	D-A-3	No marker	A list. Example value: *N - Natural Person*.
IDENTITY			
Last name	D-A-4a	Yes (*)	The party's last name.
First name	D-A-4b	No marker	The party's first name.
Middle name	D-A-4c	No marker	Placeholder *e.g. Salamanca*.
CRN	D-A-2	No marker	The customer ID, for example *TEM-CUST-10L847*.
Account no.	D-A-8	No marker	Placeholder *e.g. 1238444223*.
ID DOCUMENTS			
ID type	D-A-12	No marker	A list. Example value: *Others*.
ID number	D-A-13	No marker	Placeholder *e.g. 045223411*.
Date of birth	D-A-4c	No marker	A date (hidden in the figure).
Nationality	D-A-11	No marker	Placeholder *e.g. PH*.
ADDITIONAL DETAILS			
Complete address	D-A-5	No marker	The party's address.
Country code	D-A-6	No marker	Example value: *PH - Philippines*.
ID City code — PSGC	D-A-7	Labelled *Required for PH*	The PSGC city code.
Place of birth	D-A-10	No marker	The party's place of birth.
Source of fund	D-A-6	No marker	Example value: *Employed*.
Contact no.	D-A-15	No marker	The party's contact number.
Old account no.	D-A-16	No marker	A previous account number.

Step 1 **Expand a party**

Click a party row. It expands to show **Party role**, **Account holder**, **Entity** and the **IDENTITY**, **ID DOCUMENTS** and **ADDITIONAL DETAILS** fields.

Step 2 **Check and complete the fields**

Check **Party role** and **Entity**, and whether **Account holder** should be ticked. Make sure **Last name** is filled in, then complete the other fields you hold for the party. For a party in the Philippines, fill in **ID City code — PSGC**.

Step 3 **Repeat for each party and go to step 6**

Collapse the row with the arrow at its right and repeat for each party in the list. Then click **Next Step**.

Step 6: Narratives

Write the narrative of the STR. The figure comes from the same filed STR (STR 694) opened read-only from Regulatory Reports, so the text box appears greyed; the narrative text is hidden.

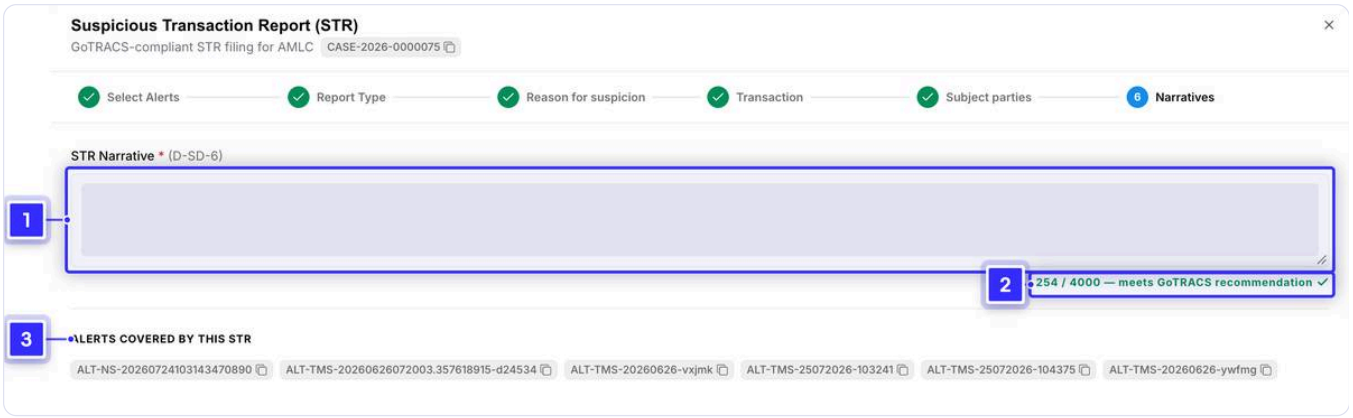


Figure 3.41 Step 6, Narratives, in a filed STR viewed read-only: the STR Narrative, text hidden (1), its counter (2) and the alerts covered (3)

1. **STR Narrative** (D-SD-6, required).
2. The character counter, for example *254 / 4000 — meets GoTRACS recommendation*, in green with a tick.
3. **ALERTS COVERED BY THIS STR**: the IDs of the alerts selected in step 1, each with a copy icon.

The footer of step 6 holds only **Previous Step**. This is the last step, so there is no **Next Step**.

Field	Code	Required	What to enter or the options
STR Narrative	D-SD-6	Yes (*)	Free text. The counter shows the length against a maximum of 4000 characters.
ALERTS COVERED BY THIS STR	None shown	Not an entry	The alerts selected in step 1.

Step 1 **Write the narrative**

Type the narrative in **STR Narrative**. Watch the counter below the box: it shows the number of characters out of 4000 and reads *meets GoTRACS recommendation* when the text meets it.

Step 2 **Check the alerts covered**

Read **ALERTS COVERED BY THIS STR**. If an alert is missing or should not be there, click **Previous Step** back to step 1 and change the selection.

AML context

The narrative is the part of an STR that an analyst at the financial intelligence unit reads first. A useful narrative says who is involved, what happened and when, which accounts and amounts were used, why the activity is suspicious (with reference to the customer's profile and the reason codes chosen), and what the institution has done about it.

After the STR is filed

A case whose STR has been filed has the status **STR Created**. Its case bar shows **Download STR** and **ReOpen**. The filed STR is listed in Regulatory Reports, where you can open it read-only and download its CSV.

Not covered in this edition

The final action on the Narratives step that completes the filing is not shown in this guide; this edition documents the wizard up to Narratives and the case after filing. If you are unsure how to complete a filing, ask your compliance lead or contact support at hello@fyscaltech.com.

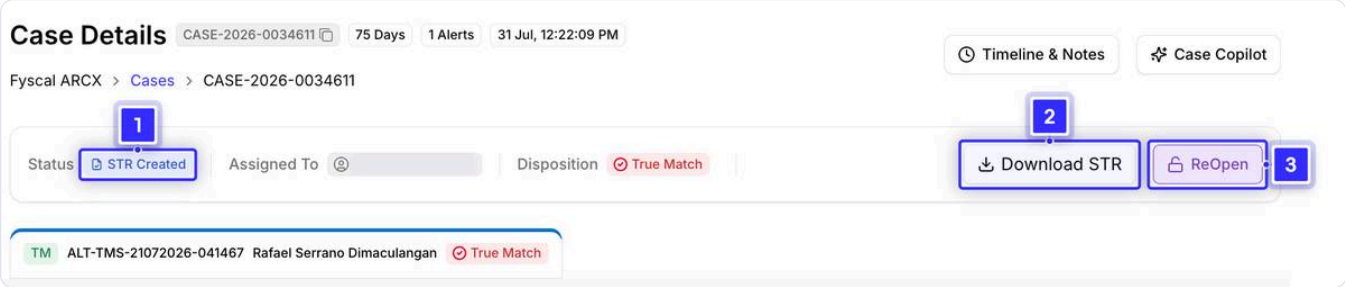


Figure 3.42 An STR Created case (CASE-2026-0034611, Rafael Serrano Dimaculangan): the STR Created status (1), Download STR (2) and ReOpen (3)

If you close the wizard with **×** before the STR is filed, you return to Case Details. A case that already had a saved draft keeps the status **STR Draft** and its **Preview STR** button.

Common blocks

- **Next Step is greyed out on step 4. Select Suspicious Transactions** is required. When the alerts selected in step 1 have no transactions, the table reads *No suspicious transactions found for the selected alerts.*, **Selected** shows 0 and **Next Step** stays greyed out. No other message is shown. Click **Previous Step** back to step 1 and check that the selected alerts include ones with transactions; a Transaction Monitoring alert row shows its number of transactions (Figures 3.37 and 3.39).
- **The filing deadline is shown in red.** The **Filing deadline** message beside **Date of determination** is shown in red in both examples captured: *Filing deadline: October 7, 2026 (Overdue by 6 days)* in a draft viewed on 13 October and *Filing deadline: August 31, 2026 (Overdue by 44 days)* on a filed STR viewed on 14 October (see Regulatory Reports, step 2). On a filed STR the message alone does not show whether the STR was filed late. Check that the date of determination is correct (Figure 3.30).

Alerts list

Fyscal ARCX → Case Manager → Alerts

The **Alerts** screen lists alerts raised by Name Screening and Transaction Monitoring. **My Queue** shows the alerts assigned to you; **All Alerts** shows all alerts, with summary chips and row checkboxes.

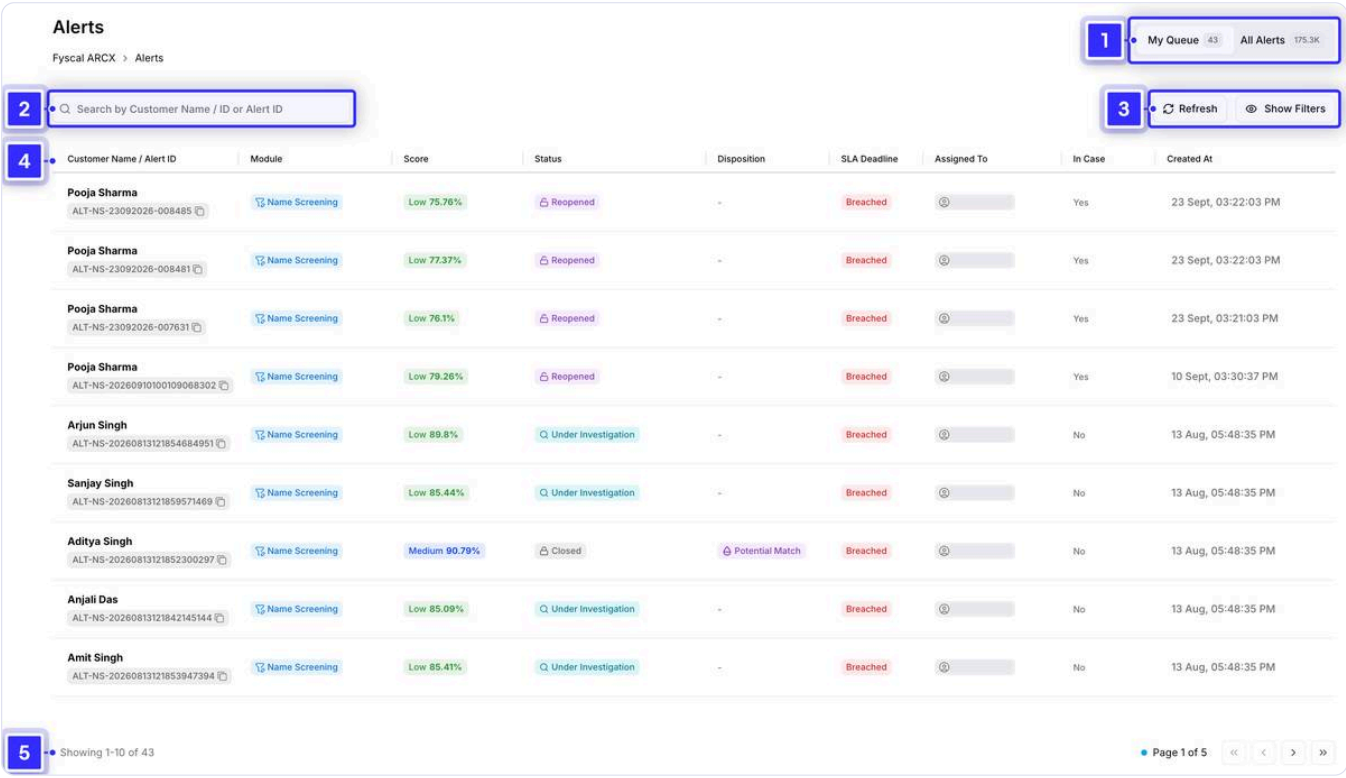


Figure 3.43 The Alerts screen on My Queue: the tabs (1), search (2), Refresh and Show Filters (3), the alert list (4) and pagination (5)

1. **My Queue** and **All Alerts** tabs, each with a count (43 and 175.3K in the example).
2. Search box: *Search by Customer Name / ID or Alert ID*.

3. **Refresh** and **Show Filters**.
4. The alert list.
5. Pagination: *Showing 1-10 of 43* and *Page 1 of 5* with first, previous, next and last page buttons.

Column	What it shows
Customer Name / Alert ID	The customer name and the alert ID (for example *ALT-NS-23092026-008485*), with a copy icon. Name Screening IDs start with *ALT-NS*, Transaction Monitoring IDs with *ALT-TMS*.
Module	**Name Screening** or **Transaction Monitoring**.
Score	The score band and percentage, for example *Low 75.76%* or *Medium 90.79%*.
Status	Not Started, Under Investigation, Pending Review, Escalated, Closed or Reopened.
Disposition	True Match, False Match, Potential Match, or **-**.
SLA Deadline	**On Track** (green) or **Breached** (red).
Assigned To	The assigned user, or **-** when unassigned.
In Case	**Yes** when the alert belongs to a case, **No** when it does not.
Created At	Creation date and time.

All Alerts chips and filters

On **All Alerts**, chips above the list (1) show **Unassigned**, **Escalated**, **SLA Breached** and **Active Agents**, each with a count. Click **Show Filters** to open the filter bar (2); the button then reads **Hide Filters**.

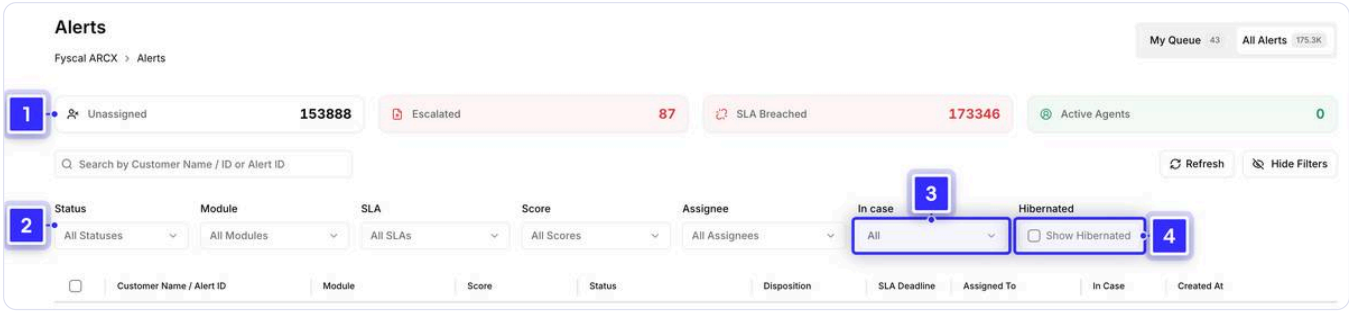


Figure 3.44 All Alerts with the filters shown: the summary chips (1), the filter bar (2), In case (3) and Show Hibernated (4)

Filter	Default	Options
Status	All Statuses	All Statuses, Not Started, Under Investigation, Pending Review, Escalated, Closed, Reopened
Module	All Modules	All Modules, Name Screening, Transaction Monitoring
SLA	All SLAs	All SLAs, Breached, On Track
Score	All Scores	All Scores, Low, Medium, HIGH
Assignee	All Assignees	A list of users. The signed-in user is labelled *(You)*.
In case (3)	All	All, Yes, No
Hibernated (4)	Unticked	**Show Hibernated** checkbox

Alert Details: Name Screening

Fyscal ARCX → Case Manager → Alerts → (click an alert)

Alert Details shows one alert. The example is ALT-NS-05102026-000115 for Ramon Michael Castillo Tan: a Name Screening alert with two watchlist candidates that is assigned but not yet started.

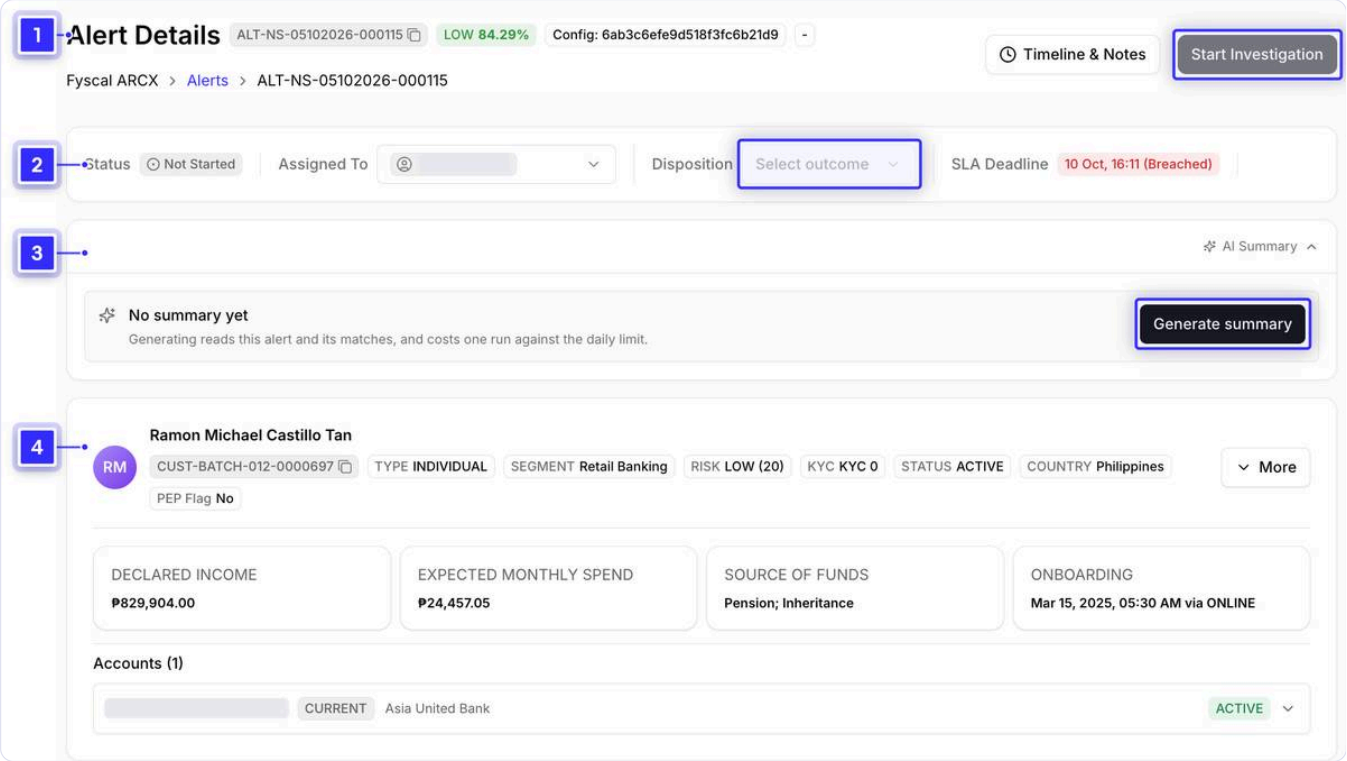


Figure 3.45 Alert Details for a Name Screening alert that is Not Started: the header (1), the alert bar (2), the AI Summary card (3) and the customer card (4)

1. Header: **Alert Details**, the alert ID, the score band and percentage (*LOW 84.29%*), *Config:* followed by the configuration version ID, and the creation date (shown as **-** on this alert). At the right: **Timeline & Notes** and, on this Not Started alert, **Start Investigation**, shown in grey.
2. Alert bar: **Status**, **Assigned To** (the assigned user, hidden in the figure), **Disposition** (*Select outcome*; greyed out on this alert) and **SLA Deadline** (date and time; red with *(Breached)* once missed).
3. **AI Summary** card (see below).
4. Customer card and **Accounts**, as in Customer, accounts and matches.

Below these, **Matches** shows each watchlist candidate side by side with the customer (1). Here MICHAEL TAN (2) is selected and RAMON TAN (3) is the second candidate. The highlighted candidate's record opens in the **Selected** panel (4) with the **Identity** and **Additional Information** tabs. All fields are described in Customer, accounts and matches.

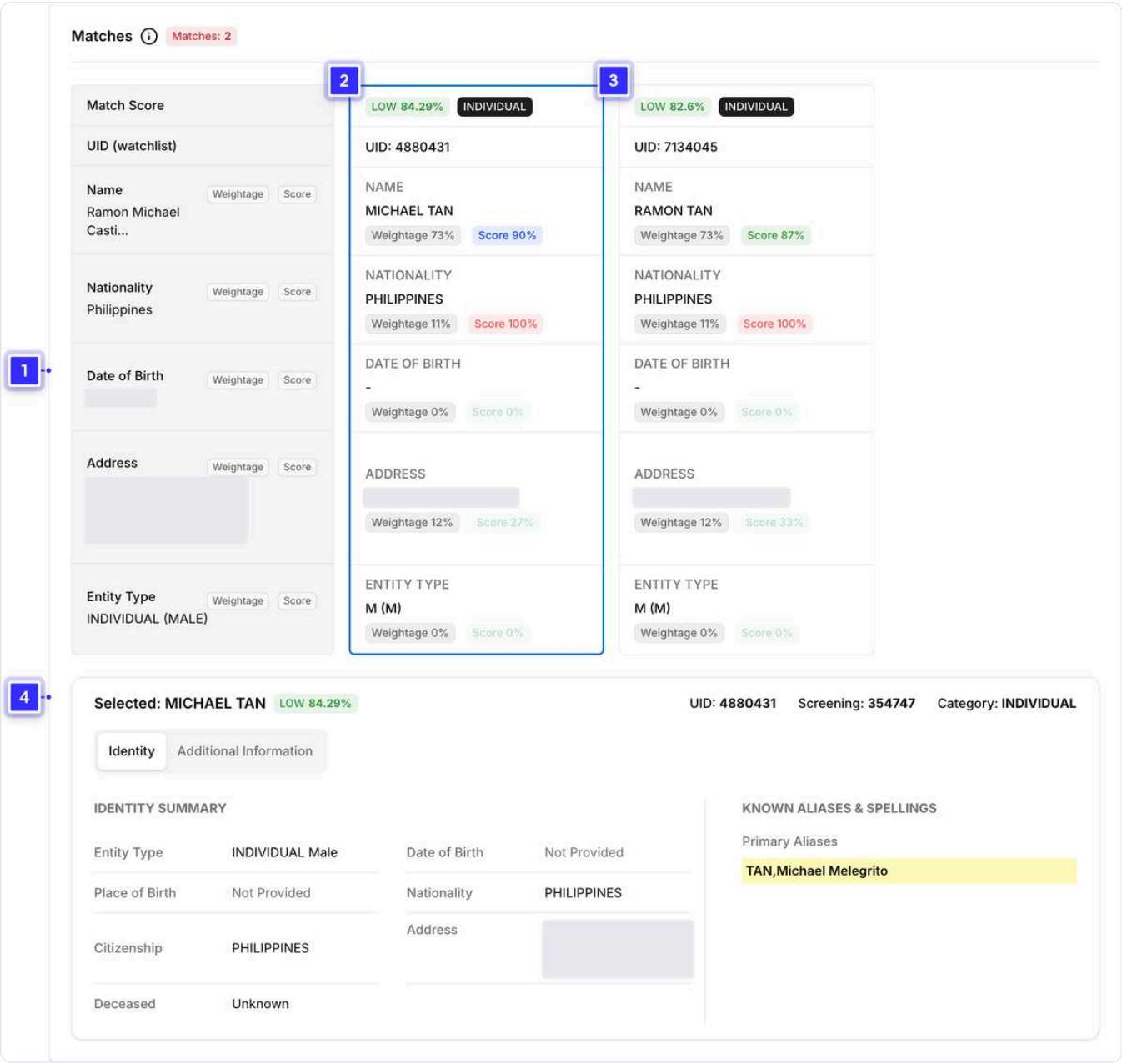


Figure 3.46 Matches for ALT-NS-05102026-000115: the customer (1), MICHAEL TAN, LOW 84.29%, selected (2), RAMON TAN, LOW 82.6% (3) and the Selected panel (4)

AI Summary

Until a summary is generated, the card reads *No summary yet* and *Generating reads this alert and its matches, and costs one run against the daily limit.* Click **Generate summary** to create one. The **AI Summary** control at the top right of the card collapses and expands it. The prompts behind the summary are managed in Agentic Workflows (see Case Manager Config).

A generated summary, as on the Transaction Monitoring alert in Figure 3.48, has:

- a verdict tag with a one-line reason (for example **Insufficient Data**: *Insufficient data; transaction details unavailable*);
- **RATIONALE**, with a copy icon;
- sections with an item count, for example **KEY FINDINGS (4)**, **TRANSACTION PATTERN ANALYSIS (3)**, **RULE TRIGGER ANALYSIS (2)** and **RISKS & DATA GAPS (3)**;
- **RECOMMENDED ACTION**;
- a footer with the prompt version, the model and the generation time, for example *Prompt v3 · Model openai/gpt-oss-120b · 28 Sept, 05:28 PM*.

> **Note**
> The AI Summary is generated text. Read it alongside the alert evidence; the disposition is recorded by the analyst.

Alert timeline

Timeline & Notes opens the **Activity Timeline** for the alert, headed with the alert number. It has the same **ADD A NOTE**, **Attach File** and **Add note** controls as the case timeline (1). Events are listed newest first, each with its date and time:

- **Assigned** (2): who made the change, and the owner before and after it (here *Unassigned* » the new owner).
- **Created** (3): an alert raised by screening starts with a Created event by *System*.

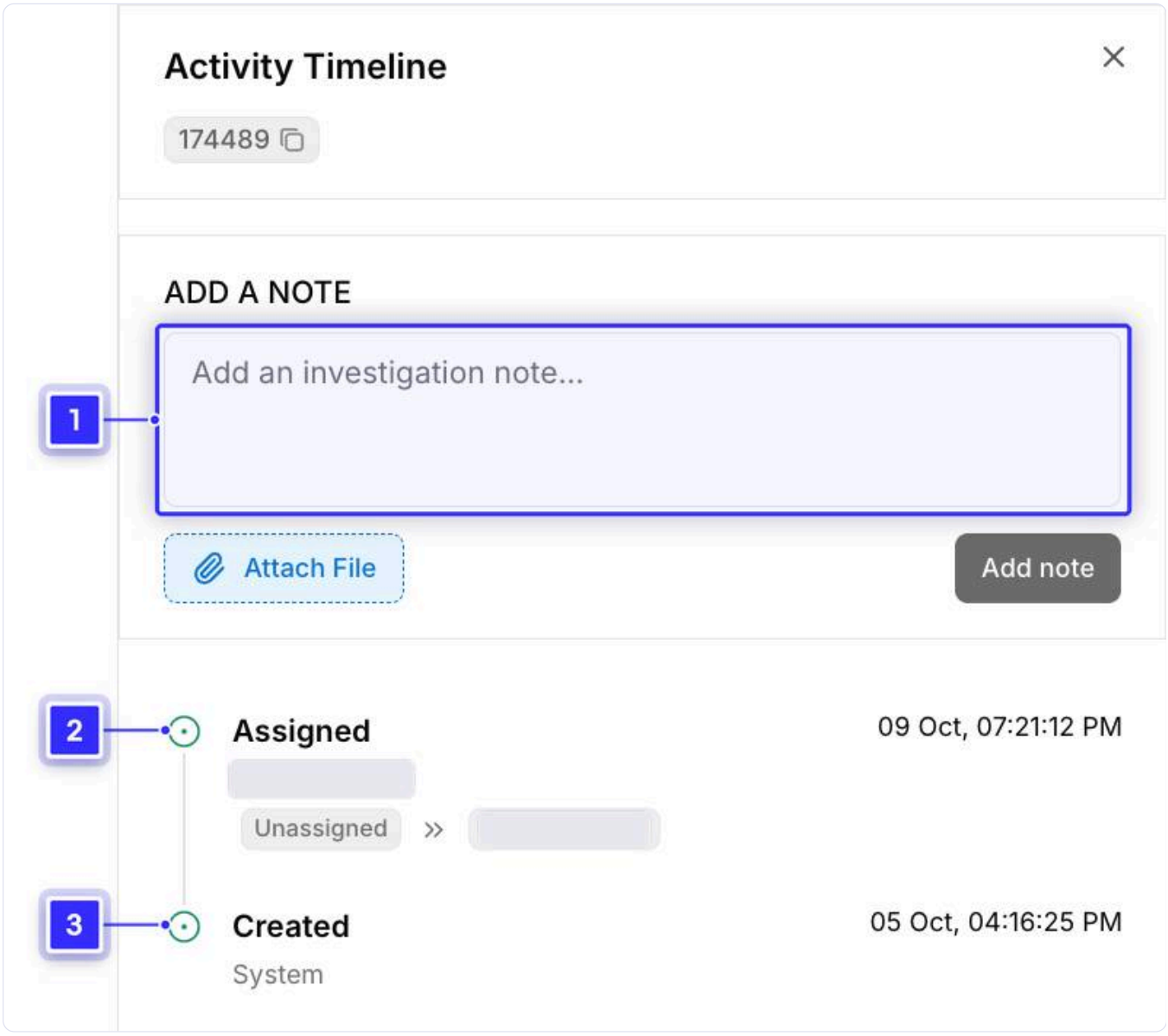


Figure 3.47 Activity Timeline for alert 174489: the note controls (1), the Assigned event (2) and the Created event by System (3)

Alert Details: Transaction Monitoring

A Transaction Monitoring alert has the same layout, with the evidence tabs **Analytics**, **Transactions**, **Other Cases / Alerts** and **Rule Analysis** in place of Matches (see Transaction Monitoring evidence tabs). The example is ALT-TMS-13092026-187809 for Margarita Ong Abalos: a Closed alert that belongs to a case. Its decision was recorded again on 13 Oct 2026, and the new decision leaves **Disposition**, **Rationale Code** and **Details** blank.

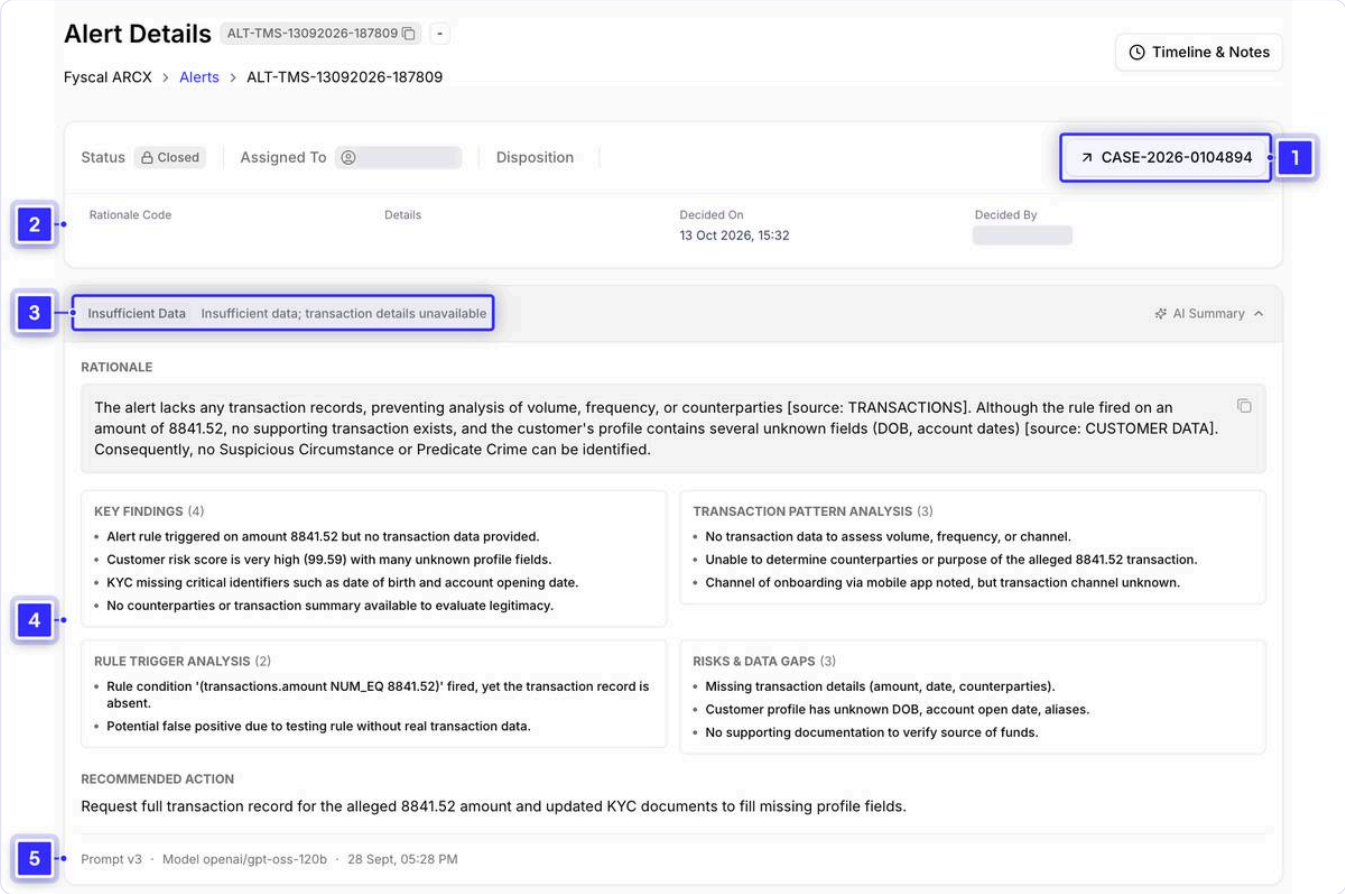


Figure 3.48 A closed Transaction Monitoring alert: the case button (1), the decision block (2), the AI Summary verdict (3), its sections (4) and the footer (5)

- An alert that belongs to a case shows a button with the case ID (1) (here **CASE-2026-0104894**) at the right of the alert bar. Click it to open the case.
- A decided alert shows a decision block (2): **Rationale Code**, **Details**, **Decided On** and **Decided By**. A field with no value is left blank.
- The AI Summary opens with its verdict (3). For monitoring alerts its sections (4) include **TRANSACTION PATTERN ANALYSIS** and **RULE TRIGGER ANALYSIS**, and the footer (5) gives the prompt version, model and time.

Work an alert

These are the controls on Alert Details as an alert moves from Not Started to a decision. Which controls appear depends on the alert's status and on whether it is assigned and grouped; the table records what the example alerts show.

Alert Details control	Not Started	Under Investigation, assigned, not in a case	Closed, in a case
Start Investigation	◑ Partial Shown in grey	✕ No	✕ No
Disposition reads *Select outcome*	✓ Yes Greyed out	✓ Yes Opens the list	✕ No Shows the recorded outcome; blank on the example
Group into Case	✕ No	✓ Yes	✕ No
Button with the case ID	✕ No	✕ No	✓ Yes
Decision block (Rationale Code, Details, Decided On, Decided By)	✕ No	✕ No	✓ Yes

Examples: ALT-NS-05102026-000115 (Figure 3.45), ALT-NS-20260813121854684951 (Figure 3.49) and ALT-TMS-13092026-187809 (Figure 3.48).

Step 1 **Check the alert's status and owner**

Read **Status** and **Assigned To** in the alert bar. On the **Not Started** example, **Start Investigation** is shown in grey next to Timeline & Notes and **Disposition** is greyed out (Figure 3.45). On an alert that is **Under Investigation** and assigned (1 in Figure 3.49), **Start Investigation** is not shown and **Disposition** can be opened.

Step 2 **Choose a disposition**

Open **Disposition** (*Select outcome*) (2) and choose **True Match**, **False Match** or **Potential Match**. What happens after you choose is not covered in this edition.

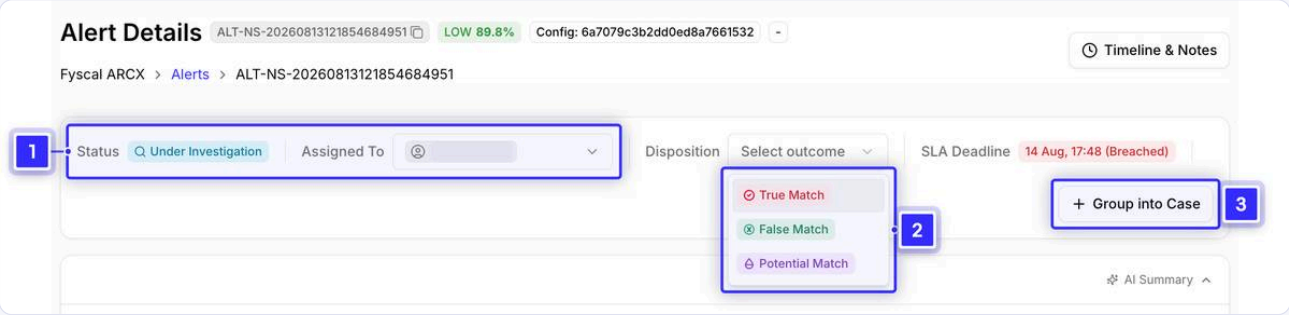


Figure 3.49 An alert Under Investigation: Status and Assigned To (1), the open Disposition list (2) and Group into Case (3)

Step 3 **Group the alert into a case**

An alert that is Under Investigation and not in a case shows **Group into Case** (3) at the right of the alert bar. From a case, you can also bring ungrouped alerts in with Add Alerts. The result of Group into Case is not covered in this edition.

Alert status changes recorded on screen

Reopening a case reopens the alerts you leave selected. The **Reopen Case** dialog pre-selects every disposed alert (*Uncheck any that should remain closed*), and the case timeline then records *n alert(s) Reopened* with a link to each alert (see Reopen a case). The alert statuses offered by the **Status** filter are Not Started, Under Investigation, Pending Review, Escalated, Closed and Reopened.

RELATED IN CORE WORKFLOW

Case Manager Configuration | Customer 360 | Regulatory Reports

CORE WORKFLOW

4 Case Manager Configuration

Fyscal ARCX → Case Manager → Config

The four **Config** pages under Case Manager hold the settings behind case work. Administrators use them to choose which alert types are merged into cases and who the cases go to, set up alert assignment, maintain the prompts and model used by Agentic Workflows, and arrange teams into hierarchies. This chapter describes each page, field by field, as it appears on screen.

FOR	IN THE MENU	READING TIME
Administrators	Fyscal ARCX → Case Manager → Config	About 26 min

Case Creation & Assignment: Active Configuration: check how alerts are currently merged into cases and who receives them.

Edit the case creation configuration: change alert types, groups and case assignment mappings.

Configuration History: review earlier case creation configurations.

Alert Assignment: set up how alerts are assigned to people.

Agentic Workflows: Prompt Config: read the prompts and their revisions.

Edit and publish a prompt: change a prompt and publish it as a new version.

Agentic Workflows: Model Config: check, update or restore the model configuration.

Team Management: the hierarchy list: find, filter and open hierarchy templates.

Add a hierarchy: create a new hierarchy template.

View a hierarchy's details: check a hierarchy's IDs, status and dates.

The hierarchy builder: Template Builder tab: see the roles at each level of a hierarchy.

The hierarchy builder: Hierarchy Builder tab: see the members at each depth as a chart.

Open **Fyscal ARCX** in the sidebar, then **Case Manager**, then **Config**. Config lists four pages: **Case Creation & Assignment**, **Alert Assignment**, **Agentic Workflows** and **Team Management**. The sidebar shortens long names (for example *Case Creation …*, *Team Manage…*).

> **Note**
> The breadcrumb under each page title differs from the sidebar path. Case Creation & Assignment and Alert Assignment show **Fyscal ARCX › Config › …**, Agentic Workflows shows **Fyscal ARCX › Agentic Workflows**, and Team Management shows **Fyscal ARCX › Case Manager › Config › Team Management**.

Case Creation & Assignment: Active Configuration

Fyscal ARCX → Case Manager → Config → Case Creation & Assignment

CONTROLS	GROUPING KEY	EXAMPLE	VERSIONS
Which alert types become cases, how they are grouped, who receives the cases	Customer ID, case age and status (on-screen banner)	Transaction Monitoring only; Group 1; Method Sequential	One ACTIVE configuration; earlier ones INACTIVE in Configuration History

Check this page to see which alert types are turned into cases, how they are grouped and who the cases are assigned to. It shows the configuration that is currently **ACTIVE** for turning alerts into cases. It has three panels: **Merge Alerts to a Case**, **Alert Type Grouping** and **Auto Assignment of Cases**. The page opens on the **Active Configuration** tab, read-only, with an **Edit** button.

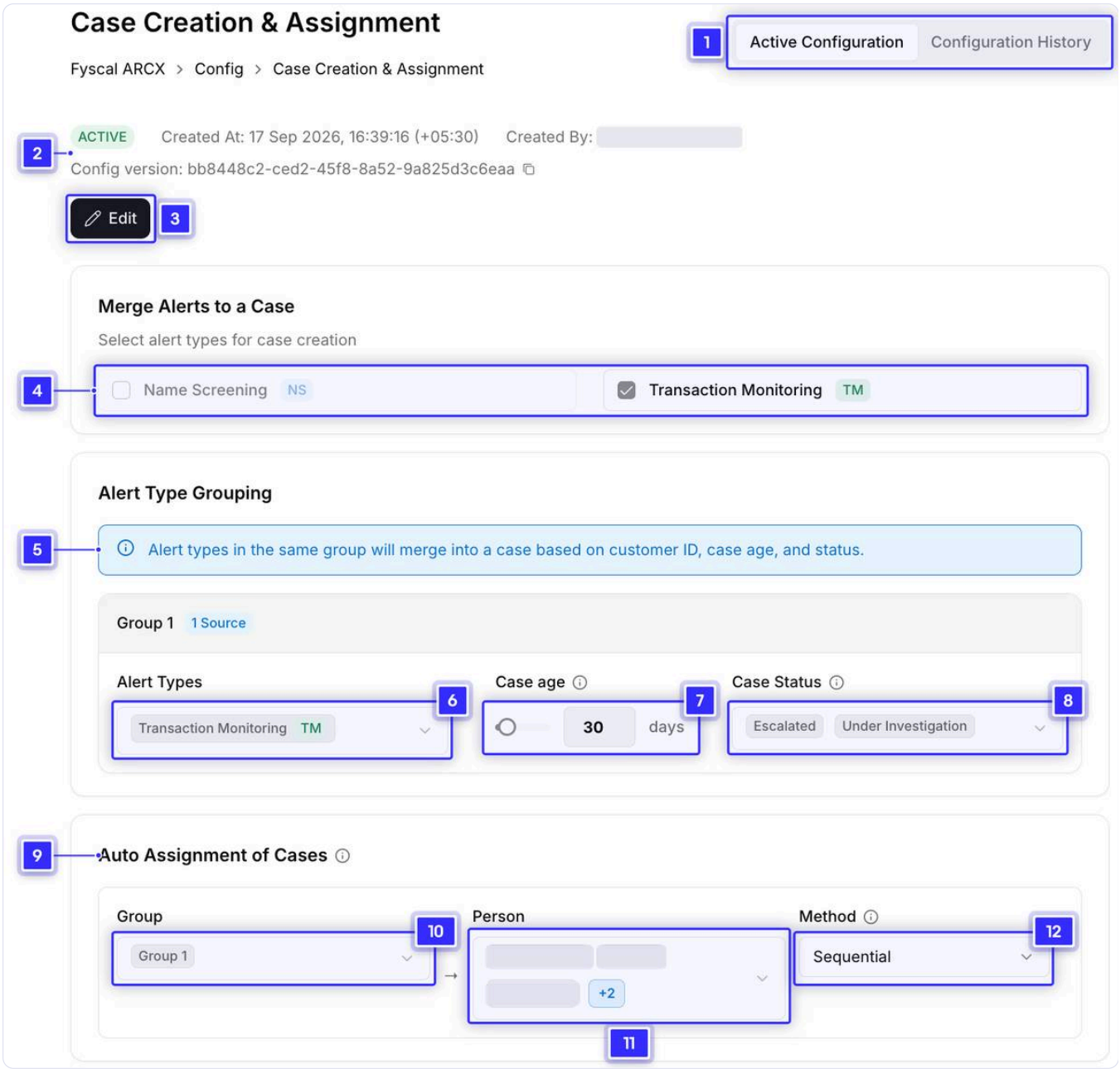


Figure 4.1 Case Creation & Assignment, Active Configuration tab: the active configuration's header, Merge Alerts to a Case, Alert Type Grouping (Group 1) and Auto Assignment of Cases.

1. **Active Configuration** and **Configuration History** tabs. History is described in Configuration History.
2. The configuration header: the **ACTIVE** status, **Created At** (17 Sep 2026, 16:39:16 (+05:30) in the example), **Created By** (a staff member's name), and **Config version**, a unique ID (bb8448c2-ced2-45f8-8a52-9a825d3c6eaa) with a copy icon.
3. **Edit** opens the configuration for changes (see Edit the case creation configuration).
4. **Merge Alerts to a Case**: the helper text reads "Select alert types for case creation". Two checkboxes: **Name Screening** (tag **NS**) and **Transaction Monitoring** (tag **TM**). In the example only Transaction Monitoring is ticked.
5. **Alert Type Grouping**: the information banner reads "Alert types in the same group will merge into a case based on customer ID, case age, and status." Each group is a card headed with its name (**Group 1**) and a tag (**1 Source**).
6. **Alert Types**: the alert types in the group. Group 1 holds **Transaction Monitoring TM**.
7. **Case age**: a slider with the value in a box to its right, in **days** (30 in the example). The label has an information icon.
8. **Case Status**: the case statuses set for the group, here **Escalated** and **Under Investigation**. The label has an information icon.
9. **Auto Assignment of Cases**: maps a group to people. The heading has an information icon.
10. **Group**: the group the mapping applies to (**Group 1**), followed by an arrow (→).
11. **Person**: the people the group maps to. Three names are shown as tags and the rest are counted in a **+2** tag.
12. **Method**: the assignment method, here **Sequential**. The label has an information icon.

Field	What it shows	Options or format seen
Status	Whether this configuration is the one in effect	**ACTIVE** on this tab; past versions show **INACTIVE** in Configuration History
Created At	When the configuration was saved	17 Sep 2026, 16:39:16 (+05:30)
Created By	The staff member shown as creator	A staff member's name
Config version	Unique ID of this configuration	A 36-character ID, with a copy icon
Merge Alerts to a Case	The alert types selected "for case creation"	Name Screening (NS), Transaction Monitoring (TM)
Alert Types (per group)	The alert types in the group	Name Screening NS, Transaction Monitoring TM
Case age (per group)	A number of days	Slider and value box, e.g. 30 days
Case Status (per group)	The case statuses set for the group	Escalated, Under Investigation in the example
Group (Auto Assignment)	The group a mapping applies to	Group 1
Person (Auto Assignment)	The people the group is mapped to	Name tags, with a +N tag when more people are selected than are shown
Method (Auto Assignment)	How cases are distributed among the people	Sequential in the example

Note
The banner states what grouping is based on: customer ID, case age and status. The information icons beside **Case age**, **Case Status**, **Auto Assignment of Cases** and **Method** hold further help text. Hover over them to read it.

How the three panels fit together

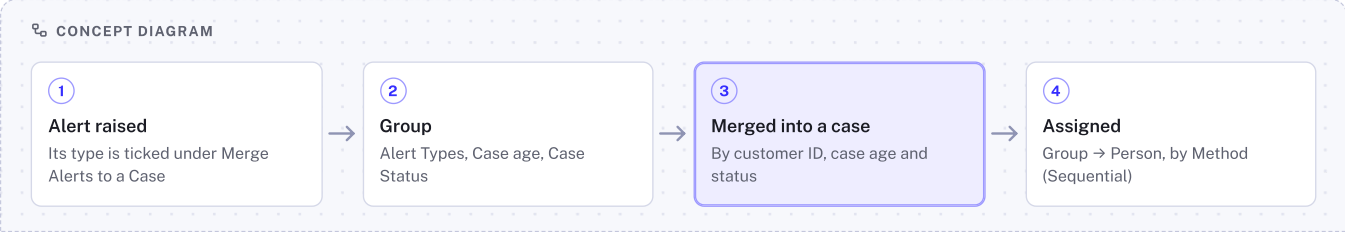


Diagram 4.1 — From alert to assigned case, as set on this page

Read the page from top to bottom. **Merge Alerts to a Case** picks the alert types that are turned into cases. Each **Alert Type Grouping** card says which of those types are merged together. **Auto Assignment of Cases** then maps each group to one or more people, with a **Method** for sharing the cases among them.

AML context
Automatic grouping and assignment decide who sees an alert and when. Institutions usually document these rules, review changes to them, and check that work is shared so that no one reviews their own decisions.

Edit the case creation configuration

Fyscal ARCX → Case Manager → Config → Case Creation & Assignment → Edit

Use edit mode when you need to change which alerts become cases, how they are grouped or who receives the cases. Edit mode shows the same three panels with editable controls. The header line (status, Created At, Created By, Config version) stays at the top, and **Cancel** and **Save** appear at the bottom of the page.

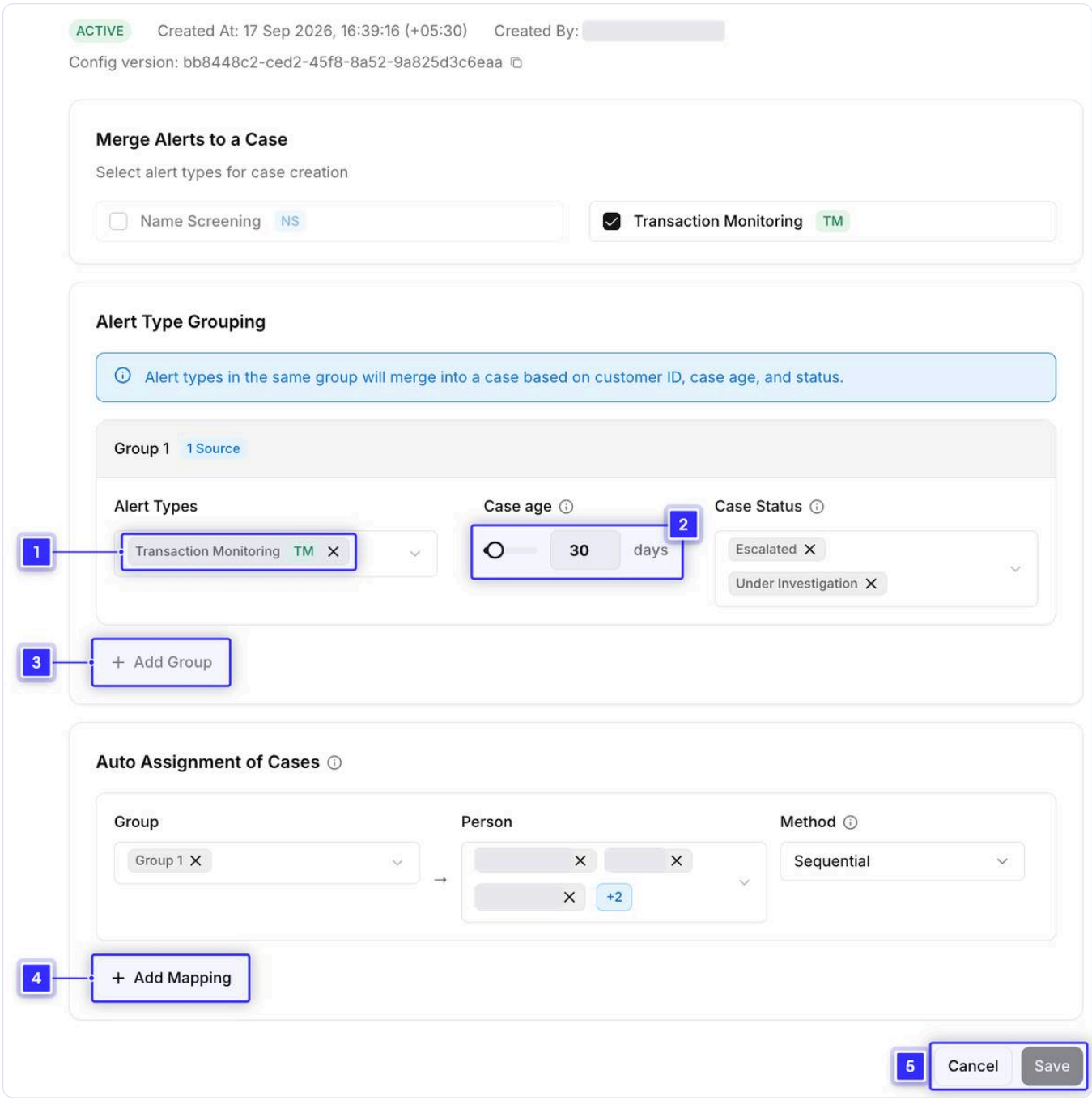


Figure 4.2 Edit mode: removable tags, the Case age slider, Add Group, Add Mapping, and Cancel and Save at the bottom.

1. Selected values are tags with a remove (×) mark: the group's Alert Types, Case Status values, the mapping's Group and each Person.
2. **Case age**: the slider and its value box (30 **days**).
3. **Add Group**, below the last group card. It is shown greyed out in Figure 4.2.
4. **Add Mapping**, below the last Auto Assignment mapping.
5. **Cancel** and **Save**. **Save** is greyed out when edit mode opens.

Tip

Before you change the configuration:

- copy the **Config version** of the active configuration (copy icon in the header), so you can find it later in Configuration History;
- read the help behind the information icons beside **Case age**, **Case Status**, **Auto Assignment of Cases** and **Method**;
- change one thing at a time, then check the next cases created in Case Manager → Cases.

Step 1 **Open edit mode**

On the **Active Configuration** tab, click **Edit** at the top right. The controls become editable and **Cancel** and **Save** appear at the bottom of the page.

Step 2 **Choose the alert types for case creation**

Under **Merge Alerts to a Case**, tick or clear **Name Screening** and **Transaction Monitoring**.

Step 3 **Set up each group**

In each group card, set **Alert Types** (click × on a tag to remove it, or open the field's list with the arrow at its right), move the **Case age** slider to the number of days you need, and set **Case Status** in the same way as Alert Types.

Step 4 **Add a group if needed**

Click **Add Group** below the last group card to add a group.

Step 5 **Map groups to people**

Under **Auto Assignment of Cases**, choose the **Group**, the **Person** or people, and the **Method**. Click **Add Mapping** to add another mapping.

Step 6 **Save or cancel**

Click **Save** to keep your changes, or **Cancel** to leave edit mode without saving.

Configuration History

Fyscal ARCX → Case Manager → Config → Case Creation & Assignment → Configuration History

Use Configuration History to look back at earlier case creation configurations and open any of them read-only. The **Configuration History** tab lists the case creation configurations, newest first: the one that is **ACTIVE** and the earlier ones, which are **INACTIVE**. The example lists 72 configurations over 4 pages.

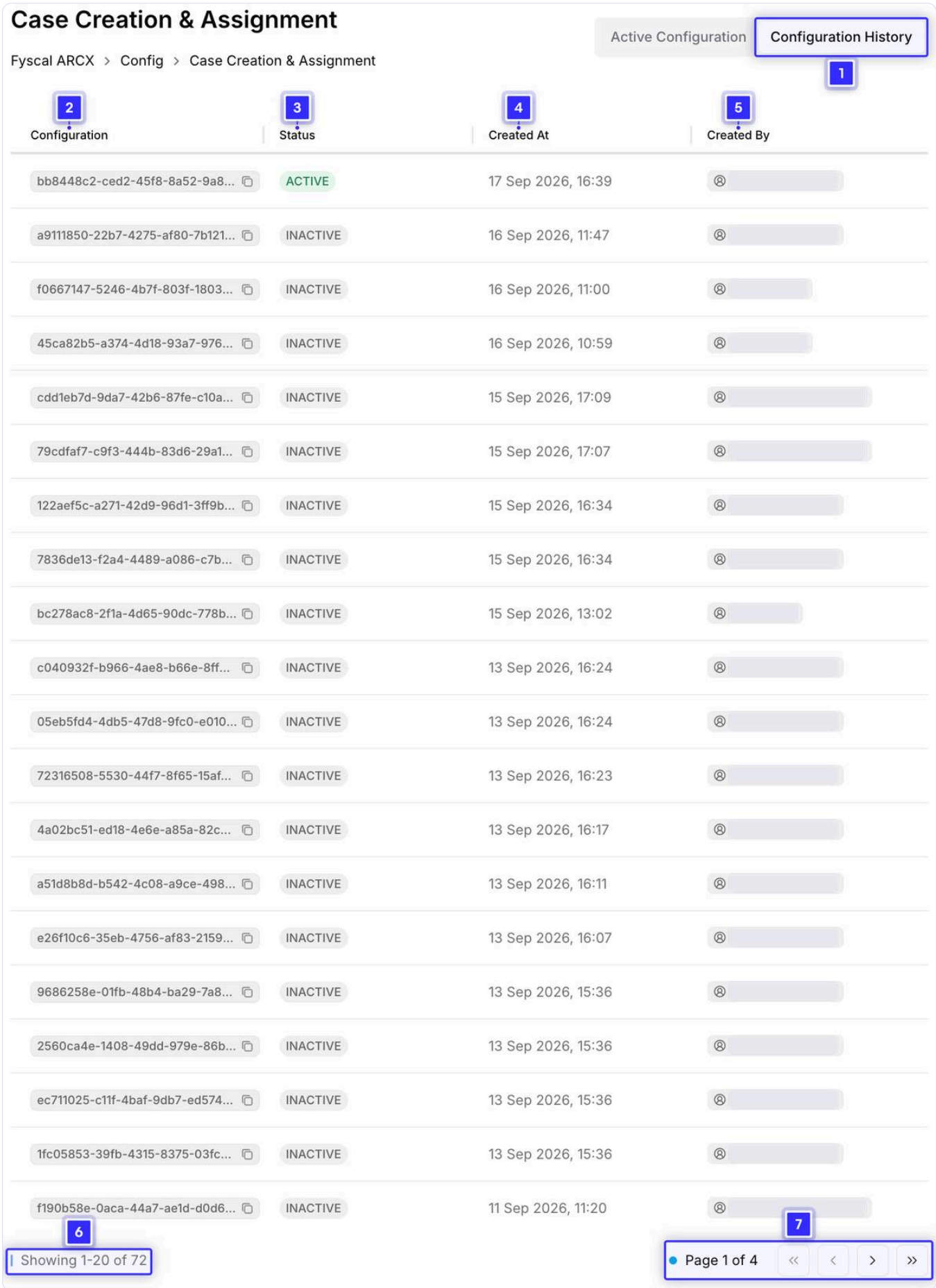


Figure 4.3 Configuration History: version IDs, ACTIVE and INACTIVE statuses, creation times, and pagination (Showing 1-20 of 72).

1 The **Configuration History** tab.

2. **Configuration**: the configuration's version ID, with a copy icon.
3. **Status**: **ACTIVE** or **INACTIVE**.
4. **Created At**: date and time, e.g. 17 Sep 2026, 16:39.
5. **Created By**: a staff member's name.
6. The row count, e.g. **Showing 1-20 of 72**.
7. The page indicator (**Page 1 of 4**) with first, previous, next and last page buttons.

Status	Meaning as shown on screen
ACTIVE	The configuration shown on the Active Configuration tab. One row has this status.
INACTIVE	Every other configuration in the list.

Step 1 **Open an earlier configuration**

Click a row. The **Configuration Details** dialog opens with the row's status (for example **INACTIVE**), **Config Version ID**, **Created At** (with seconds and time zone offset) and **Created By**, followed by the same three panels as the Active Configuration tab, read-only. Figure 4.4 shows configuration a9111850-22b7-4275-af80-7b12123ebeaa: Name Screening is ticked under Merge Alerts to a Case, and Group 1 holds Name Screening NS, with a Case age of 30 days and Case Status Escalated and Under Investigation.

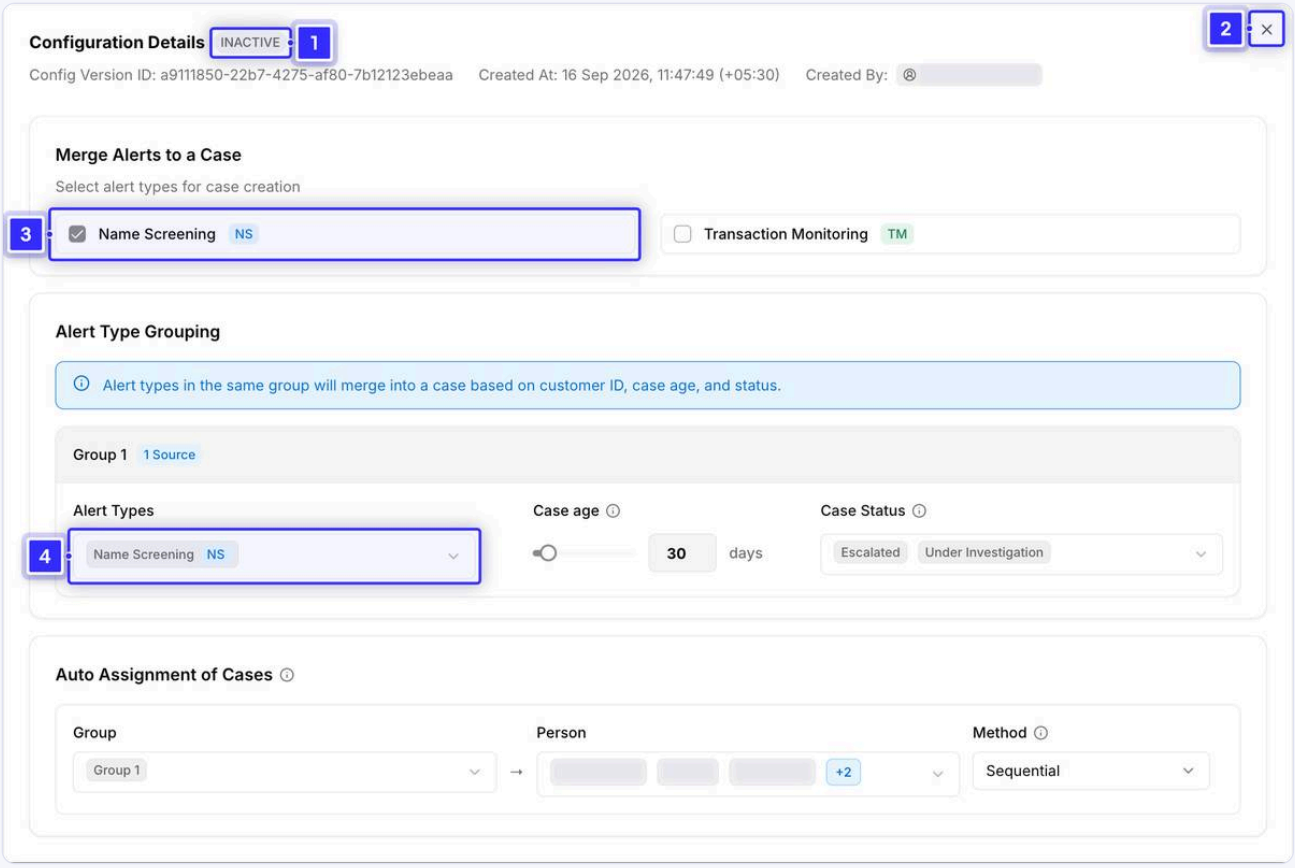


Figure 4.4 Configuration Details for INACTIVE configuration a9111850: the status (1), the close button (2), Name Screening ticked (3) and Group 1 holding Name Screening NS (4)

Step 2 **Close the dialog**

Click × at the top right of the dialog.

Alert Assignment

Fyscal ARCX → Case Manager → Config → Alert Assignment

Alert Assignment holds the settings for assigning alerts to people: the alert types it applies to, and for each mapping the people who receive the alerts and the method used to share them out. It works like Case Creation & Assignment: the page opens on the **Active Configuration** tab, read-only, with an **Edit** button, and earlier versions are listed on the **Configuration History** tab.

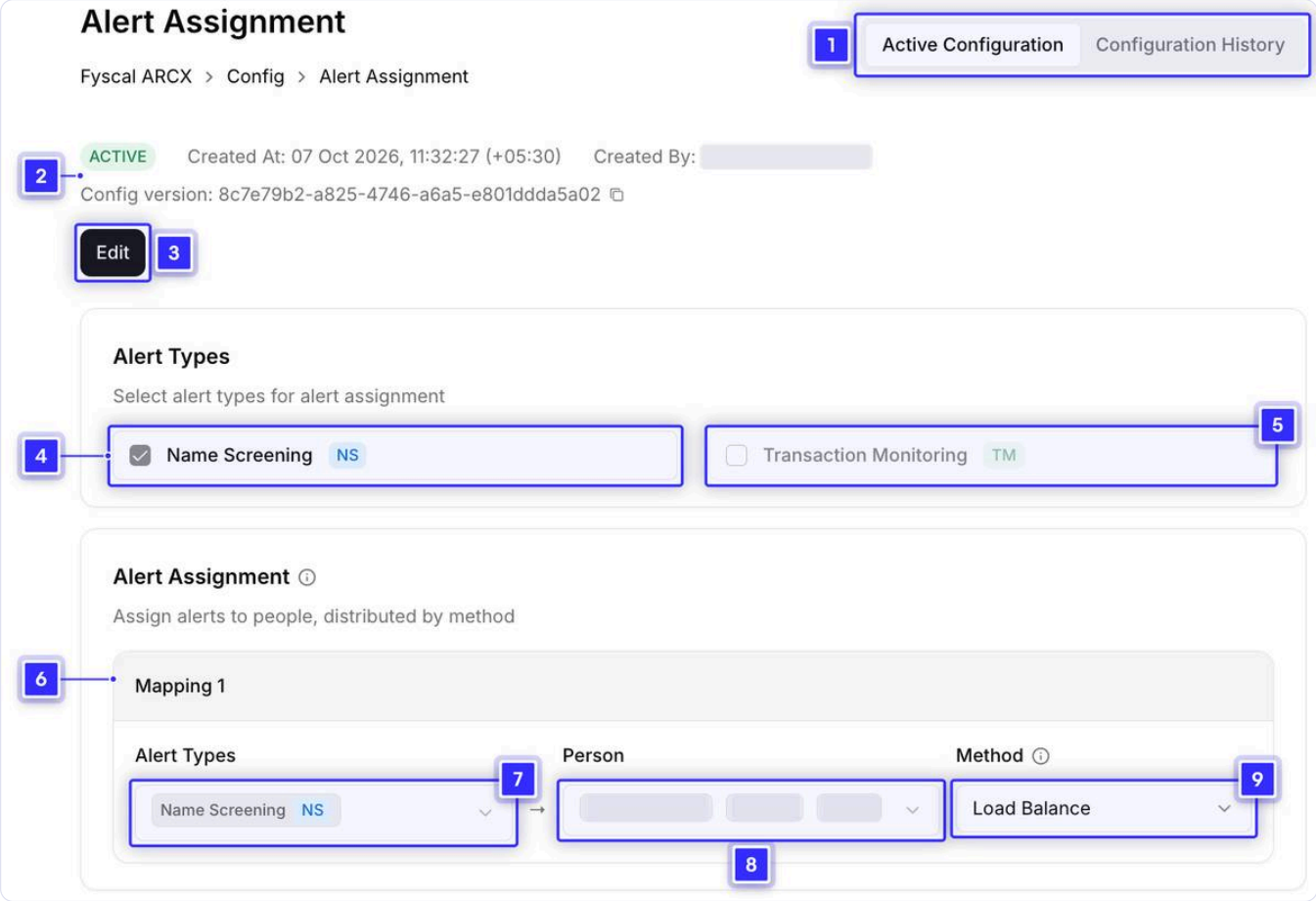


Figure 4.5 Alert Assignment, Active Configuration tab: the tabs (1), the configuration header (2), Edit (3), the Name Screening (4) and Transaction Monitoring (5) alert types, and Mapping 1 (6) with its Alert Types (7), Person (8) and Method (9)

1. **Active Configuration** and **Configuration History** tabs.
2. The configuration header: **ACTIVE**, **Created At** (07 Oct 2026, 11:32:27 (+05:30) in the example), **Created By** (a staff member's name) and **Config version** (8c7e79b2-a825-4746-a6a5-e801ddda5a02) with a copy icon.
3. **Edit** opens the configuration for changes (Figure 4.6).
4. **Alert Types** ("Select alert types for alert assignment"): **Name Screening NS**, ticked in the example.
5. **Transaction Monitoring TM**, shown greyed out.
6. **Alert Assignment** ("Assign alerts to people, distributed by method", with an information icon) holds one card per mapping, here **Mapping 1**.
7. **Alert Types**: the alert types the mapping covers (**Name Screening NS**), followed by an arrow (→).
8. **Person**: the people who receive the alerts, shown as name tags (three in the example; names hidden in the figure).
9. **Method**: how alerts are shared among the people, here **Load Balance**. The label has an information icon.

Field	What it shows	Options or state seen
Alert Types	The alert types the assignment applies to	Name Screening (NS); Transaction Monitoring (TM), greyed out
Alert Types (per mapping)	The alert types a mapping covers	Name Screening NS in the example
Person (per mapping)	The people who receive the alerts	Name tags
Method (per mapping)	How alerts are shared among the people	Load Balance in the example (Case Creation & Assignment shows Sequential)

The **Configuration History** tab has the same columns as in Configuration History (Figure 4.3): **Configuration**, **Status**, **Created At** and **Created By**. The example lists 8 configurations: one **ACTIVE** and seven **INACTIVE**.

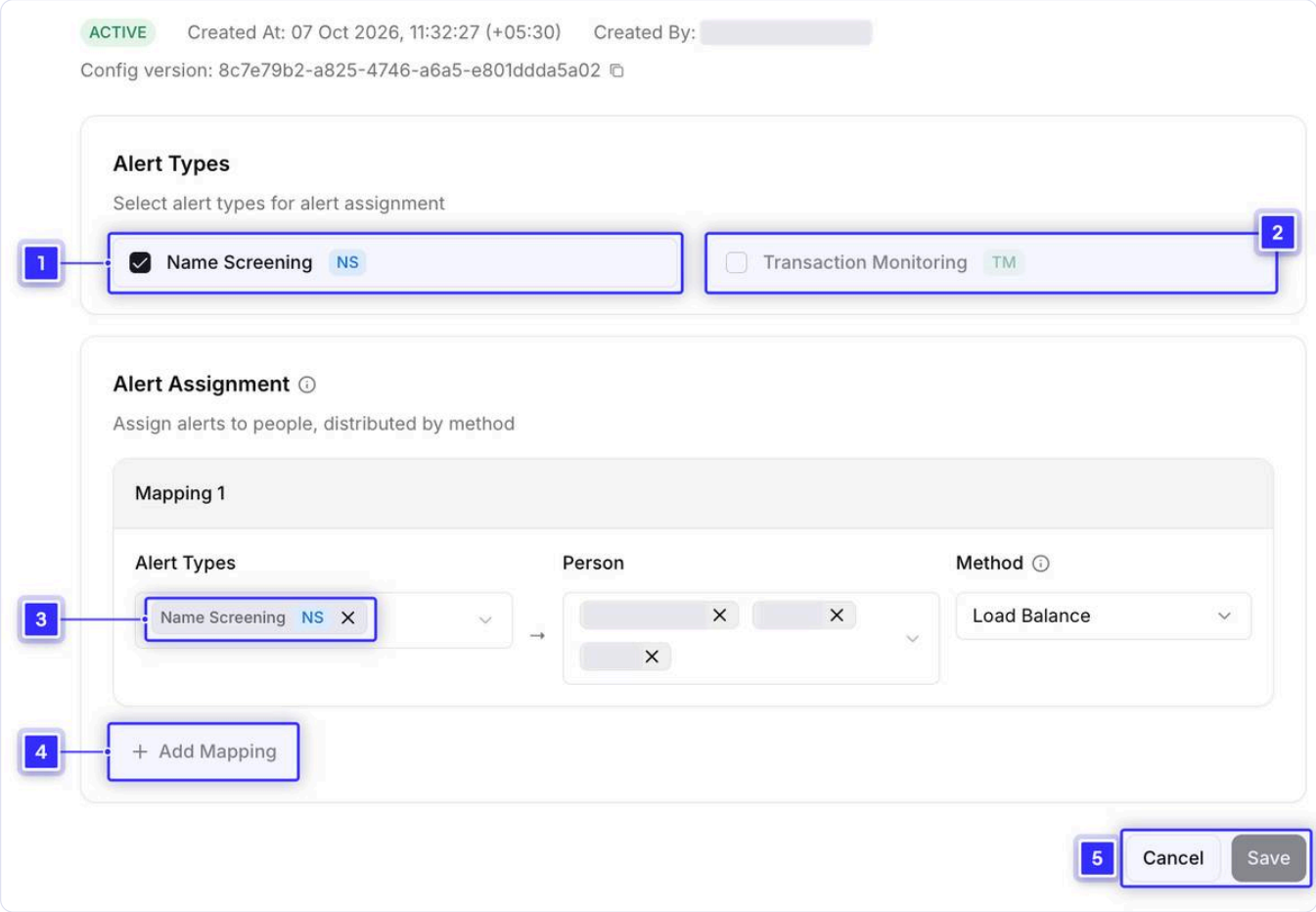


Figure 4.6 Alert Assignment in edit mode: the Name Screening checkbox (1), Transaction Monitoring greyed out (2), a removable tag (3), Add Mapping (4), and Cancel and Save (5)

1. **Name Screening NS** can be ticked or cleared.
2. **Transaction Monitoring TM** stays greyed out in edit mode.
3. Selected values are tags with a remove (×) mark: the mapping's Alert Types and each Person.
4. **Add Mapping**, below the last mapping. It is shown greyed out in Figure 4.6.
5. **Cancel** and **Save**. **Save** is greyed out when edit mode opens.

Step 1 **Open edit mode**

On the **Active Configuration** tab, click **Edit**. The controls become editable and **Cancel** and **Save** appear at the bottom of the page.

Step 2 **Select the alert types**

Under **Alert Types**, tick the alert types the assignment is for.

Step 3 **Set up each mapping**

In each mapping card, set **Alert Types**, the **Person** or people (click × on a tag to remove it, or open the field's list with the arrow at its right) and the **Method**.

Step 4 **Save or cancel**

Click **Save** to keep your changes, or **Cancel** to leave edit mode without saving.

Agentic Workflows: Prompt Config

Fyscal ARCX → Case Manager → Config → Agentic Workflows → Prompt Config

PROMPTS	ACTIVE MODEL	EDITING
Case Copilot, Name Screening Alert Summary, Transaction Monitoring Alert Summary	openai/gpt-oss-120b, version v3 (Model Config)	Publishing a prompt creates a new version

Use Prompt Config to read the prompts behind Case Copilot and the alert summaries, and to compare their revisions. Agentic Workflows has two tabs: **Prompt Config**, which holds the prompts, and **Model Config**, which holds the model configuration (see Agentic Workflows: Model Config). Prompt Config shows one card per prompt.

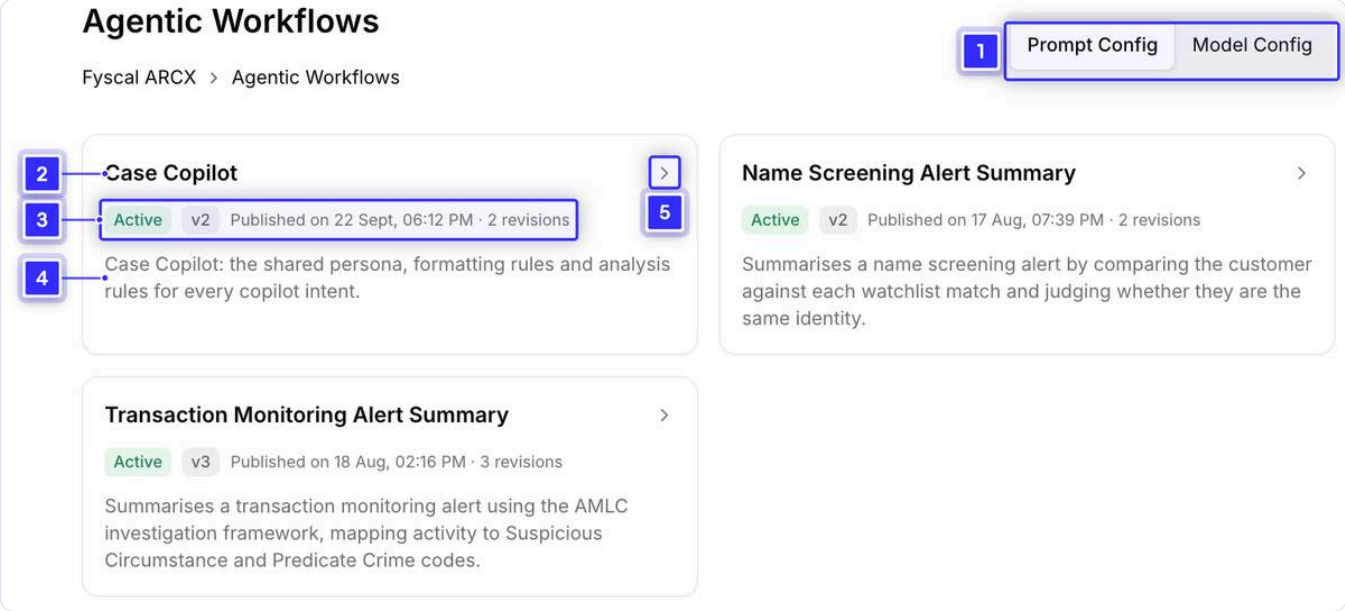


Figure 4.7 Prompt Config: cards for Case Copilot, Name Screening Alert Summary and Transaction Monitoring Alert Summary.

1. **Prompt Config** and **Model Config** tabs.
2. The prompt name.
3. The status (**Active**), the current version (e.g. **v2**), when it was published and how many revisions it has.
4. The prompt's description.
5. The arrow that opens the prompt.

Prompt	Status	Version	Published	Description shown on the card	Where its output appears
Case Copilot	Active	v2	22 Sept, 06:12 PM · 2 revisions	"Case Copilot: the shared persona, formatting rules and analysis rules for every copilot intent."	The **Case Copilot** panel on Case Details (Case Copilot)
Name Screening Alert Summary	Active	v2	17 Aug, 07:39 PM · 2 revisions	"Summarises a name screening alert by comparing the customer against each watchlist match and judging whether they are the same identity."	The **AI Summary** card on a Name Screening alert (Alert Details: Name Screening)
Transaction Monitoring Alert Summary	Active	v3	18 Aug, 02:16 PM · 3 revisions	"Summarises a transaction monitoring alert using the AMLC investigation framework, mapping activity to Suspicious Circumstance and Predicate Crime codes."	The **AI Summary** card on a Transaction Monitoring alert (Alert Details: Transaction Monitoring); its footer reads *Prompt v3 · Model openai/gpt-oss-120b*

Step 1 **Open a prompt**

Click a card. A panel opens on the right with the prompt's name, **Edit**, a close button (×), the revision navigator and the prompt sections. Figure 4.8 shows **Name Screening Alert Summary**.

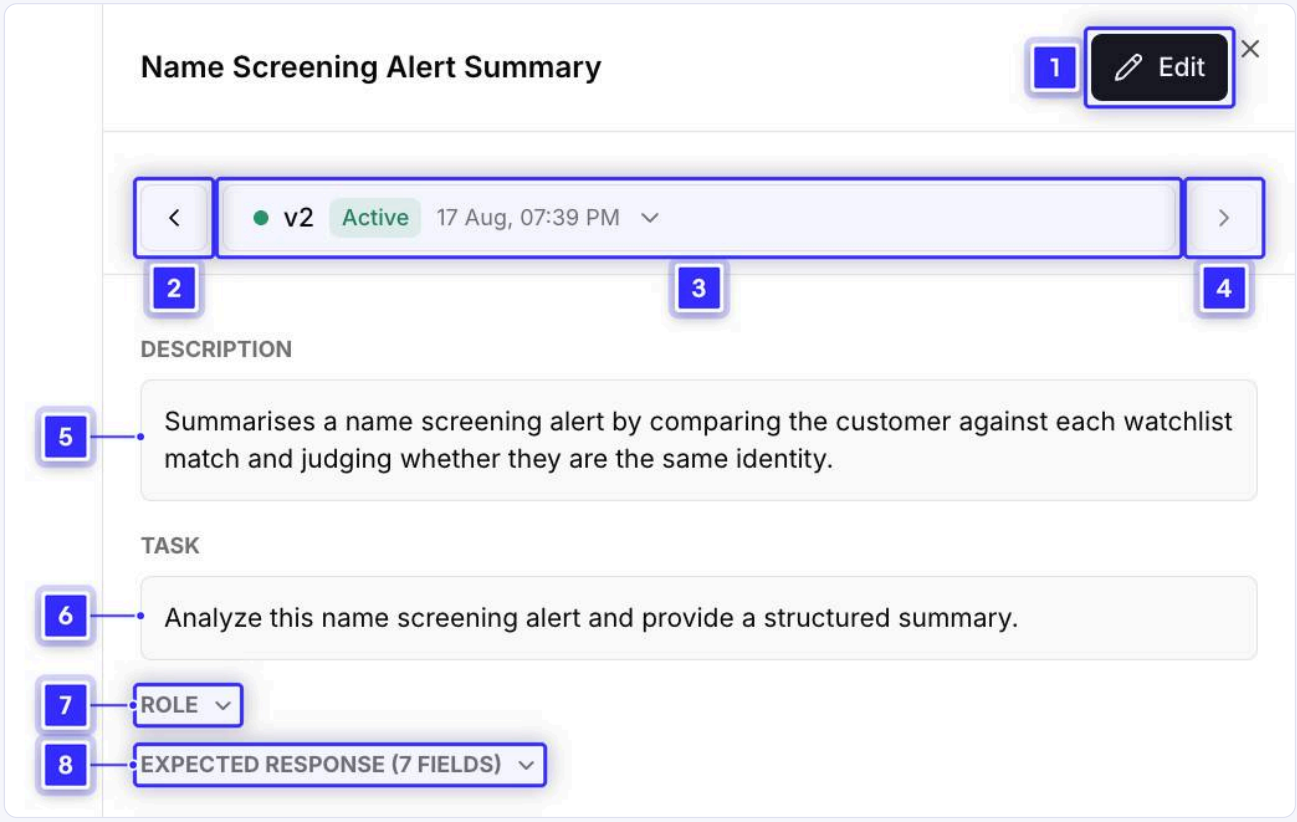


Figure 4.8 The Name Screening Alert Summary panel: Edit, the revision navigator at v2 Active, Description, Task, and the collapsed Role and Expected Response (7 fields).

1. **Edit** opens the prompt for editing (see Edit and publish a prompt).
2. Previous revision.
3. The revision shown: version (**v2**), status (**Active**) and publish time (17 Aug, 07:39 PM). Click it to open the revision picker.
4. Next revision.
5. **DESCRIPTION**: what the prompt is for.
6. **TASK**: "Analyze this name screening alert and provide a structured summary."
7. **ROLE**, collapsed. Click to expand.
8. **EXPECTED RESPONSE (7 FIELDS)**, collapsed. Click to expand.

:::

Step 2 **Pick a revision**

Click the revision in the navigator. A list opens with a search box (1) (*Find a version, e.g. 7*) and one row per version: **v2** (2) (marked **Active**, 17 Aug, 07:39 PM) and **v1** (3) (13 Aug, 03:02 PM). The footer (4) reads **7 of 7 loaded**. The arrows either side of the navigator are labelled **Previous revision** and **Next revision**.

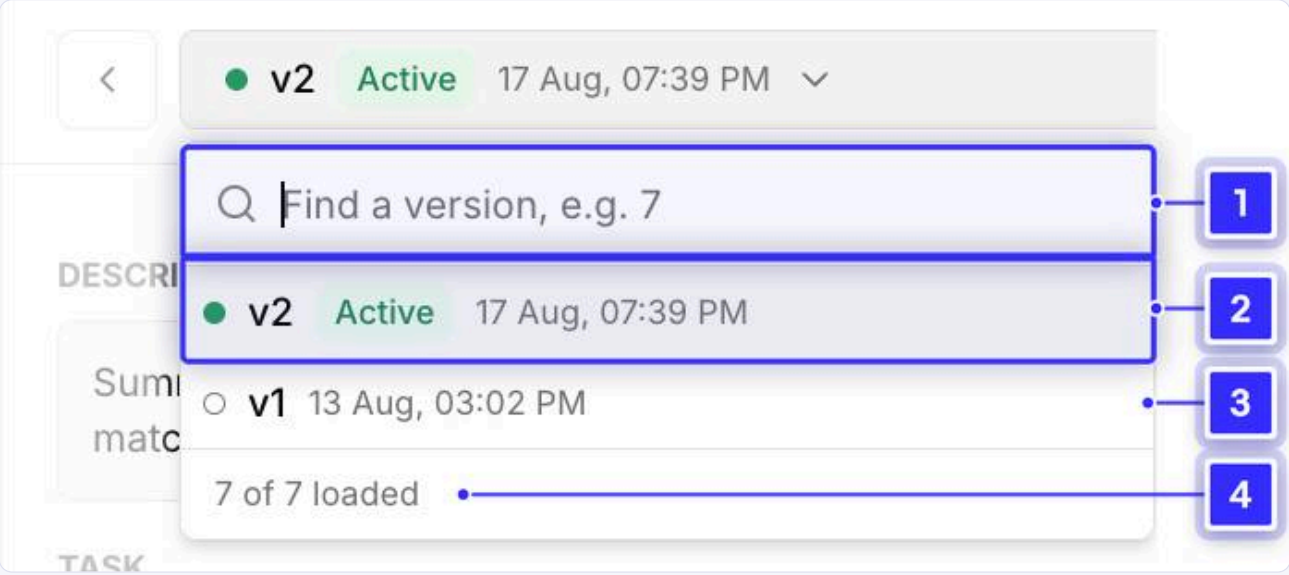


Figure 4.9 The revision picker: the Find a version search (1), v2 Active (2), v1 (3) and the 7 of 7 loaded footer (4)

Step 3 **Read the Role**

Click **ROLE** (1). For Name Screening Alert Summary v2, the Role opens with "You are a expert AML compliance analyst assistant." and then two lists. **INVESTIGATION RULES** (2) has eleven rules, starting with the tie-breaker priority "Name > Date of Birth > Nationality > Government ID > Place of Birth > Gender > Address". **DATA INTEGRITY RULES** (3) has two rules: "Use only supplied data. Never invent identifiers, allegations, or sources. If unknown, say "Unknown"" and "Every substantive claim must cite its source (watchlist record or customer data); output [source: <field_name>] tags".

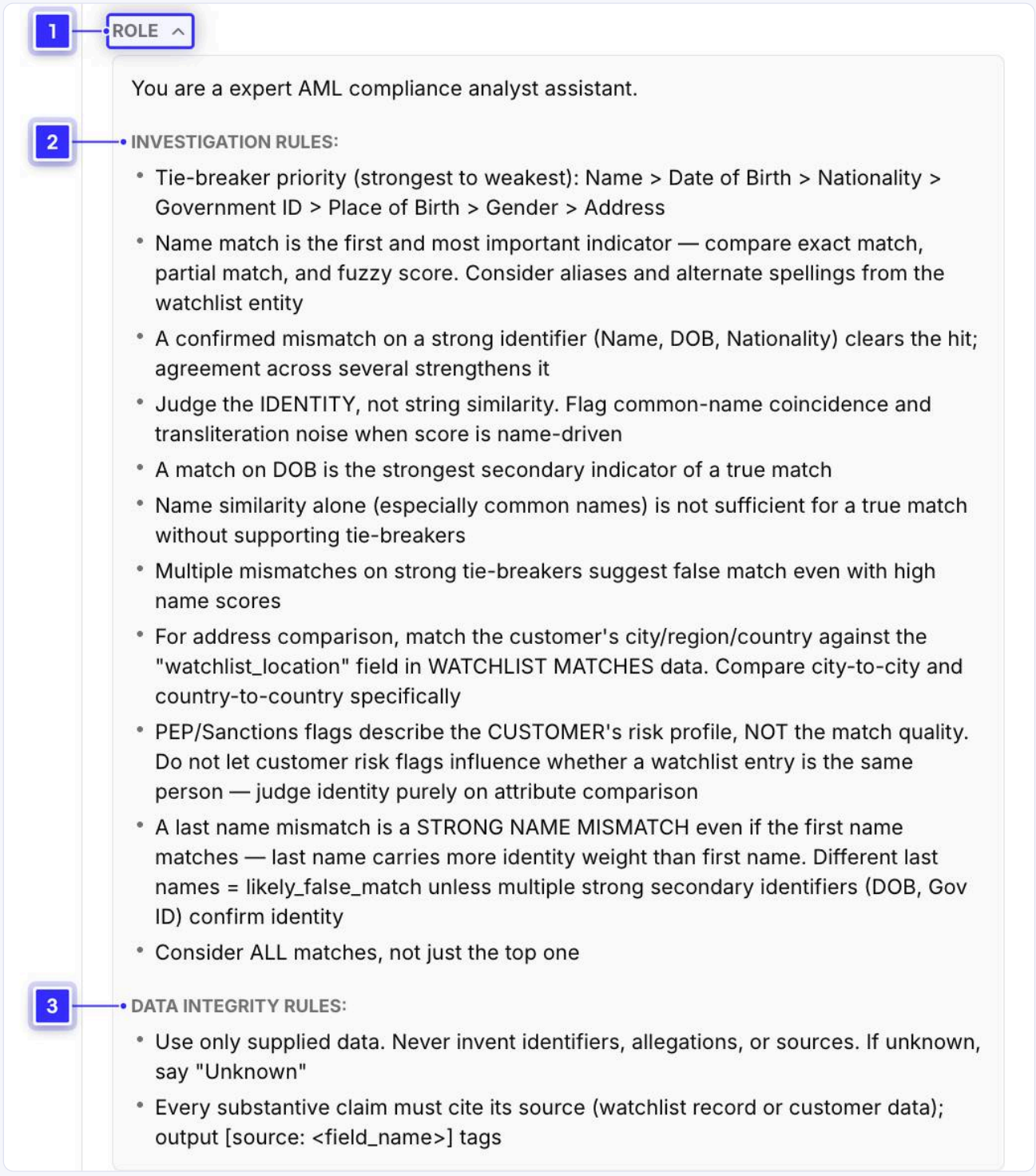


Figure 4.10 ROLE expanded (1) for Name Screening Alert Summary v2: Investigation Rules (2) and Data Integrity Rules (3)

Step 4 **Read the Expected Response**

Click **EXPECTED RESPONSE (7 FIELDS)**, below the Role. It lists the fields of the response, with a **list** label on list fields, the allowed values where there are any, and a short description. For Name Screening Alert Summary v2 the fields are:

Field	Type shown	Values or description shown
verdict	(none shown)	likely_true_match, likely_false_match, inconclusive, insufficient_data
one_line_summary	(none shown)	"max 10 words, very short verdict reason"
rationale	(none shown)	"2-3 sentence justification suitable for audit trail"
key_findings	list	"3-5 bullet points of the most important findings across all matches"
identity_comparison	list	"bullet points comparing key attributes: name, DOB, nationality, gender, address, ID — state customer vs watchlist values"
risks_and_gaps	list	"bullet points combining active risk flags (PEP, sanctions, adverse categories) AND missing data that limits analysis — keep concise"
recommended_action	(none shown)	"specific recommended next step for the analyst"

Step 5 **Close the panel**

Click × at the top right of the panel.

AML context

Prompts and models shape what the AI features tell analysts. Treat a prompt or model change like any other change to a control: record why it was made, keep the earlier versions, and check the output on a few alerts before relying on it. The analyst still records the disposition.

Edit and publish a prompt

Fyscal ARCX → Case Manager → Config → Agentic Workflows → Prompt Config → (prompt) → Edit

Edit a prompt when you need to change its Description, Task or Role; publishing creates a new version. Clicking **Edit** in a prompt panel switches the panel to an edit form. A banner states which version you are editing from and which version publishing creates, for example "Editing from v2 · publishing creates v3".

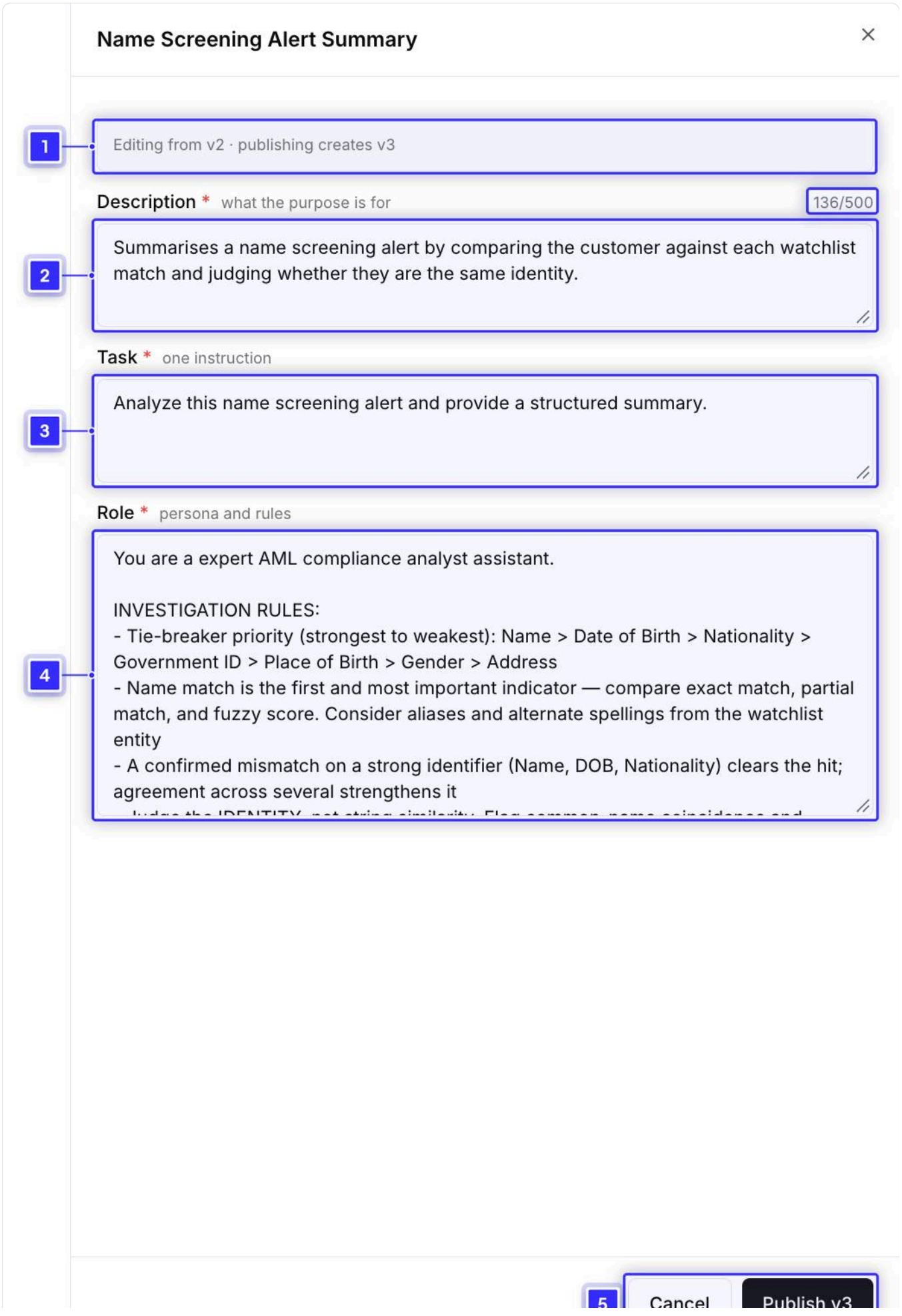

Name Screening Alert Summary
1
Editing from v2 · publishing creates v3
Description * what the purpose is for
136/500
2
Summarises a name screening alert by comparing the customer against each watchlist match and judging whether they are the same identity.
Task * one instruction
3
Analyze this name screening alert and provide a structured summary.
Role * persona and rules
4
You are a expert AML compliance analyst assistant.
INVESTIGATION RULES:
- Tie-breaker priority (strongest to weakest): Name > Date of Birth > Nationality > Government ID > Place of Birth > Gender > Address
- Name match is the first and most important indicator — compare exact match, partial match, and fuzzy score. Consider aliases and alternate spellings from the watchlist entity
- A confirmed mismatch on a strong identifier (Name, DOB, Nationality) clears the hit; agreement across several strengthens it
5
Cancel
Publish v3



Figure 4.11 Editing Name Screening Alert Summary: the version banner, Description (136/500), Task and Role, with Cancel and Publish v3.

1. The version banner: "Editing from v2 · publishing creates v3".
2. **Description** with its character counter at the right (136/500).
3. **Task**.
4. **Role**.
5. **Cancel** and **Publish v3**.

Field	Helper text on screen	Required	Format
Description	what the purpose is for	Yes (*)	Text, with a counter out of 500 characters
Task	one instruction	Yes (*)	Text
Role	persona and rules	Yes (*)	Multi-line text; the rules are written as lines starting with "-"

Step 1 **Open the prompt for editing**

Open the prompt's card on **Prompt Config**, then click **Edit**.

Step 2 **Change the text**

Edit **Description**, **Task** and **Role**. Watch the Description counter, which shows the length against 500.

Step 3 **Publish or cancel**

Click **Publish v3** (the button names the version that will be created), or **Cancel** to leave the form without publishing.

Note

The edit form holds Description, Task and Role only. The Expected Response fields are not part of the form.

Agentic Workflows: Model Config

Fyscal ARCX → Case Manager → Config → Agentic Workflows → Model Config

Use Model Config to see which model configuration is active, to update it, or to restore an earlier one. The **Model Config** tab shows the active model configuration at the top and the earlier ones under **Previous configurations**.

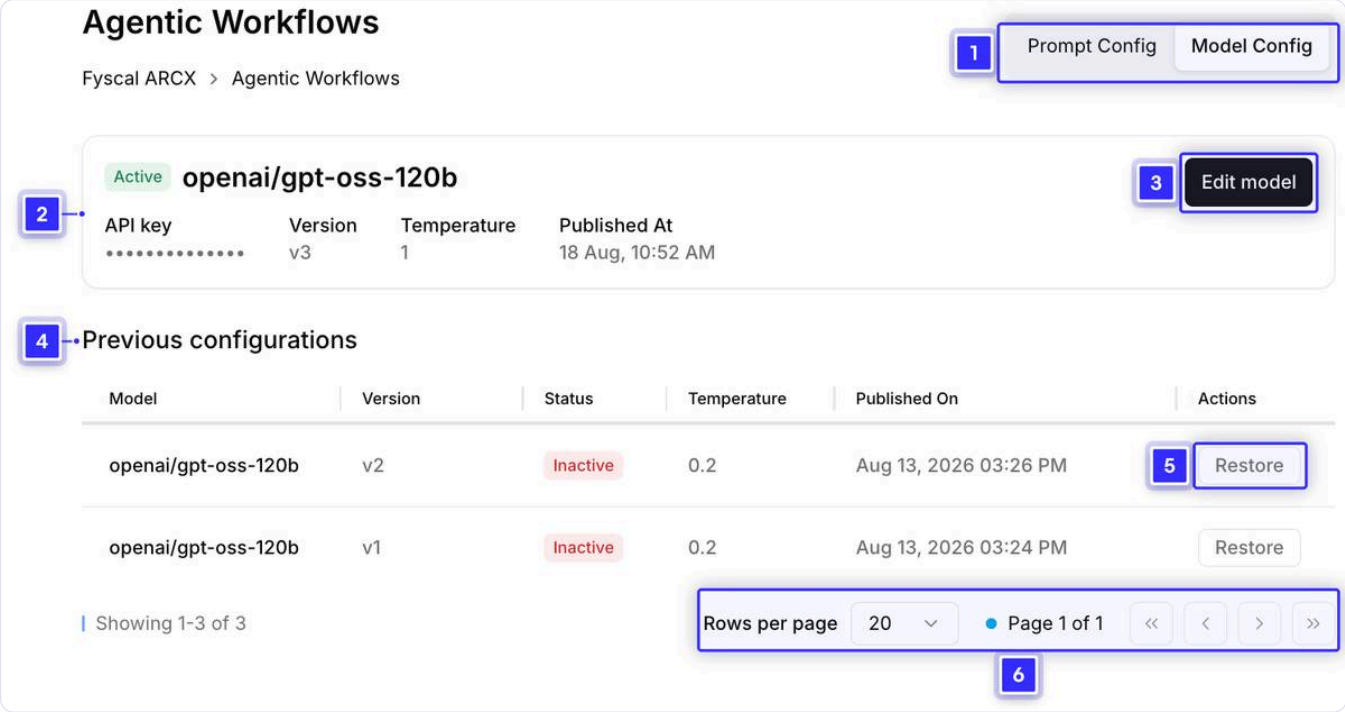


Figure 4.12 Model Config: the Active configuration openai/gpt-oss-120b v3, Edit model, and Previous configurations with Restore.

1. **Prompt Config** and **Model Config** tabs.
2. The active configuration: **Active**, the model name (**openai/gpt-oss-120b**), **API key** (masked on screen), **Version** (v3), **Temperature** (1) and **Published At** (18 Aug, 10:52 AM).
3. **Edit model** opens the **Update model** dialog.
4. **Previous configurations**: a table of earlier configurations.
5. **Restore**, one per row.
6. **Rows per page** (20), the page indicator and page buttons. The count reads **Showing 1-3 of 3**.

Column	What it shows	Example
Model	The model name	openai/gpt-oss-120b
Version	The configuration's version label	v2, v1
Status	The configuration's status	Inactive
Temperature	The temperature value	0.2
Published On	When the configuration was published	Aug 13, 2026 03:26 PM
Actions	Row action	Restore

Status	Where it appears
Active	The configuration at the top of the tab
Inactive	The rows under Previous configurations

Step 1 **Open Update model**

Click **Edit model**. The **Update model** dialog opens with the text "Saving publishes a new configuration and retires the current one. The API key cannot be read back, so enter it again." **Model**, **Version** and **Temperature** show the current values (openai/gpt-oss-120b, v3, 1 (Creative)). **Agent Key** is empty.

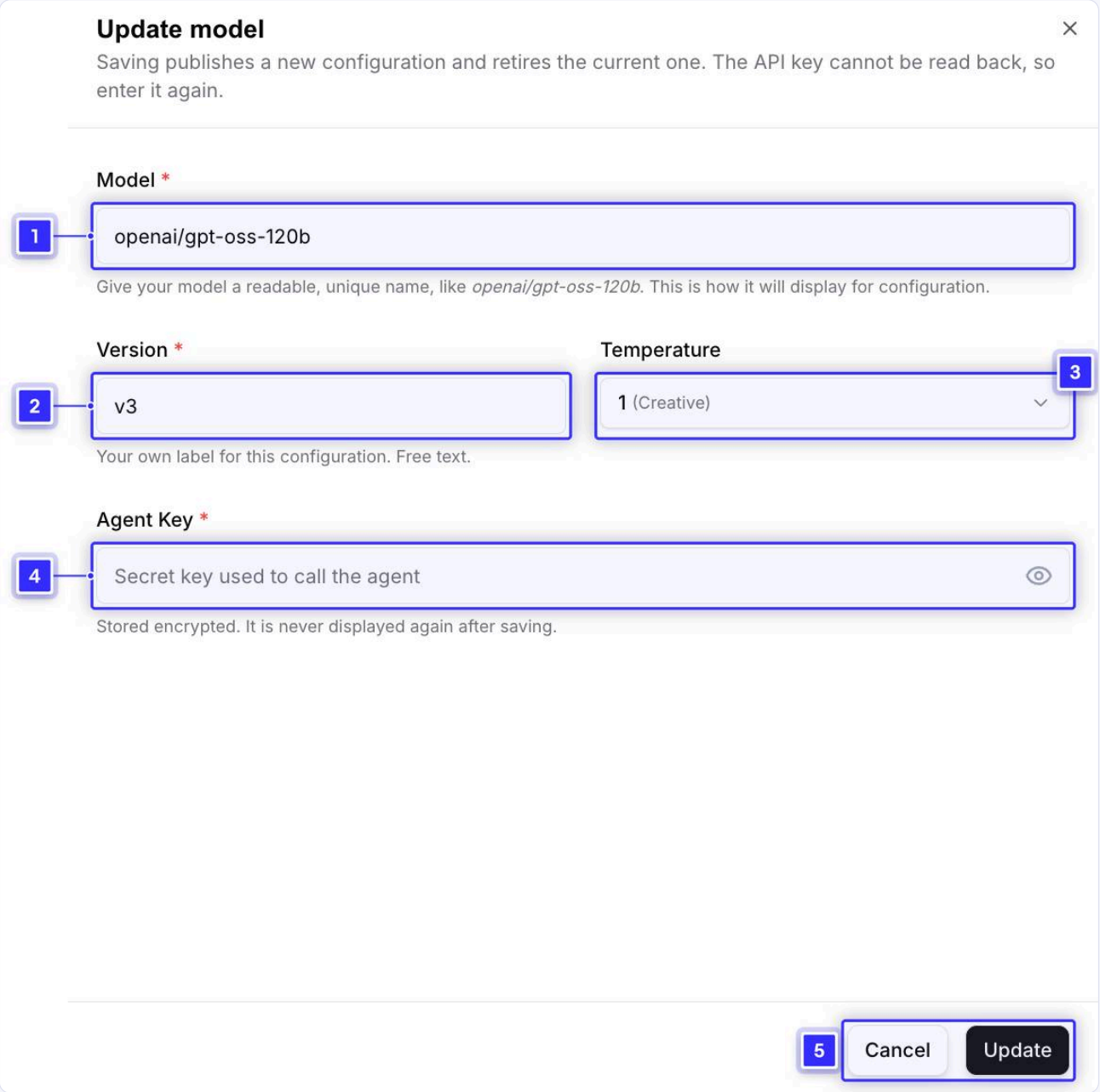


Figure 4.13 Update model: Model (1), Version (2), Temperature (3), Agent Key (4), and Cancel and Update (5)

Field	Helper text on screen	Required	Options or format
Model (1)	"Give your model a readable, unique name, like openai/gpt-oss-120b. This is how it will display for configuration."	Yes (*)	Text
Version (2)	"Your own label for this configuration. Free text."	Yes (*)	Text
Temperature (3)	(none)	No	0.2 (Server default), 0.5 (Slightly varied wording), 0.7 (Varied), 1 (Creative)
Agent Key (4)	"Stored encrypted. It is never displayed again after saving."	Yes (*)	Secret text; placeholder "Secret key used to call the agent"; an eye icon at the right of the field

Step 2 **Complete the fields**

Check or change **Model** and **Version**, choose a **Temperature**, and enter the **Agent Key**. The dialog states that the key cannot be read back, so it must be entered each time.

Step 3 **Update or cancel**

Click **Update** (5). As the dialog states, saving publishes a new configuration and retires the current one. Click **Cancel** or × to close the dialog without saving.

Note

The active configuration labels the secret **API key** and the Update model dialog labels it **Agent Key**.

The new configuration becomes the **Active** one at the top of the tab, and the one it replaces is listed under **Previous configurations** with the status **Inactive**.

Team Management: the hierarchy list

Fyscal ARCX → Case Manager → Config → Team Management

Team Management lists the hierarchy templates. From here you add a hierarchy, view its details, and open the builder where its roles and members are arranged. A warning sits at the top of the page: "Changing these values may impact system stability. Proceed only if you understand the configuration."

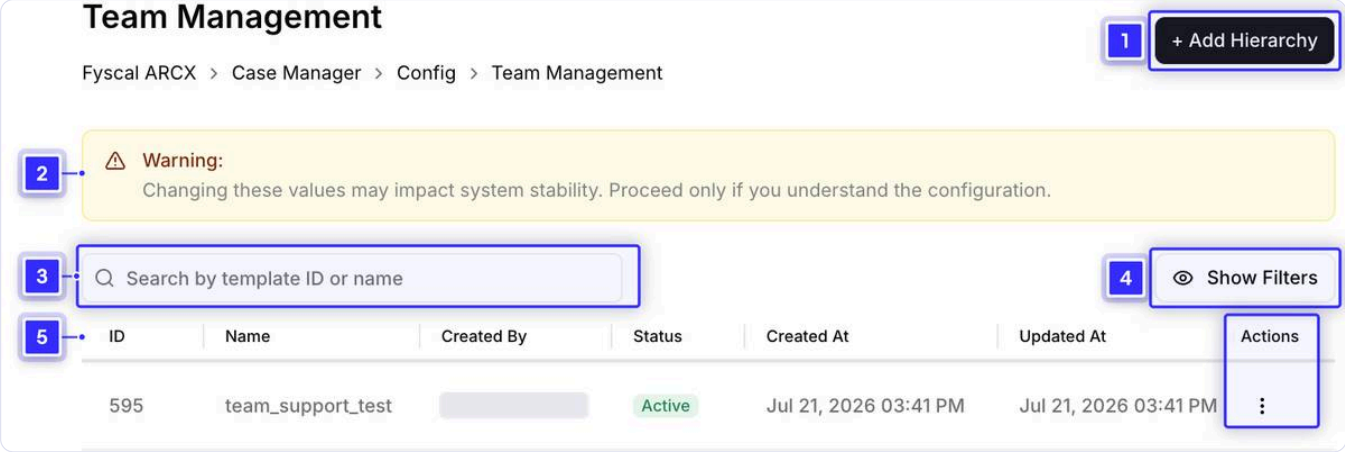


Figure 4.14 Team Management: + Add Hierarchy (1), the warning (2), the search box (3), Show Filters (4) and the list columns, ending with Actions (5)

1. **+ Add Hierarchy** opens the **Add New Hierarchy Template** dialog (see Add a hierarchy).
2. The **Warning** banner.
3. The search box: *Search by template ID or name*.
4. **Show Filters** shows the Status filter. The button then reads **Hide Filters**.
5. The columns, ending with **Actions**, where each row has a ⋮ menu.

Column	What it shows	Example
ID	The hierarchy's numeric ID	4
Name	The hierarchy's name	AML Hierarchy
Created By	The staff member who created it	A staff member's name
Status	The hierarchy's status	Active, Inactive or Removed
Created At	When it was created	Mar 31, 2026 01:59 PM
Updated At	When it was last updated	Mar 31, 2026 01:59 PM
Actions	A ⋮ menu	Edit, View, Hierarchy Builder

Below the list: the row count (for example **Showing 1-20 of 89**), **Rows per page** (20), the page indicator (**Page 1 of 5**) and first, previous, next and last page buttons. The list is ordered by ID, highest first, so the example **AML Hierarchy** (ID 4) is on the last page.

Status	Meaning as shown on screen
Active	Shown in green. Also the default Status for a new hierarchy.
Inactive	Shown in red. Can be chosen when adding a hierarchy.
Removed	Shown in blue. Available as a filter value.

Step 1 **Find a hierarchy**

Type a template ID or name into **Search by template ID or name**.

Step 2 **Filter by status**

Click **Show Filters**; the button now reads **Hide Filters** (1). A **Status** filter appears above the list. Open **Select Status** (2) and choose **Active**, **Inactive** or **Removed** (3). Click **Hide Filters** to hide the filter again.

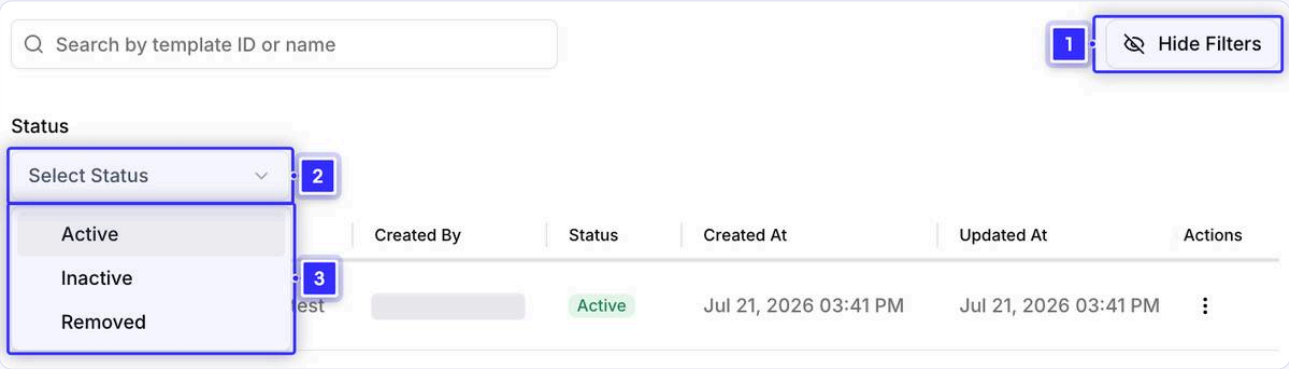


Figure 4.15 Filters shown: Hide Filters (1), the Status filter (2) and its list, Active, Inactive and Removed (3)

Step 3 **Open a row's actions**

Click ⋮ (1) in the **Actions** column. The **Actions** menu lists **Edit** (2), **View** (3) and **Hierarchy Builder** (4).

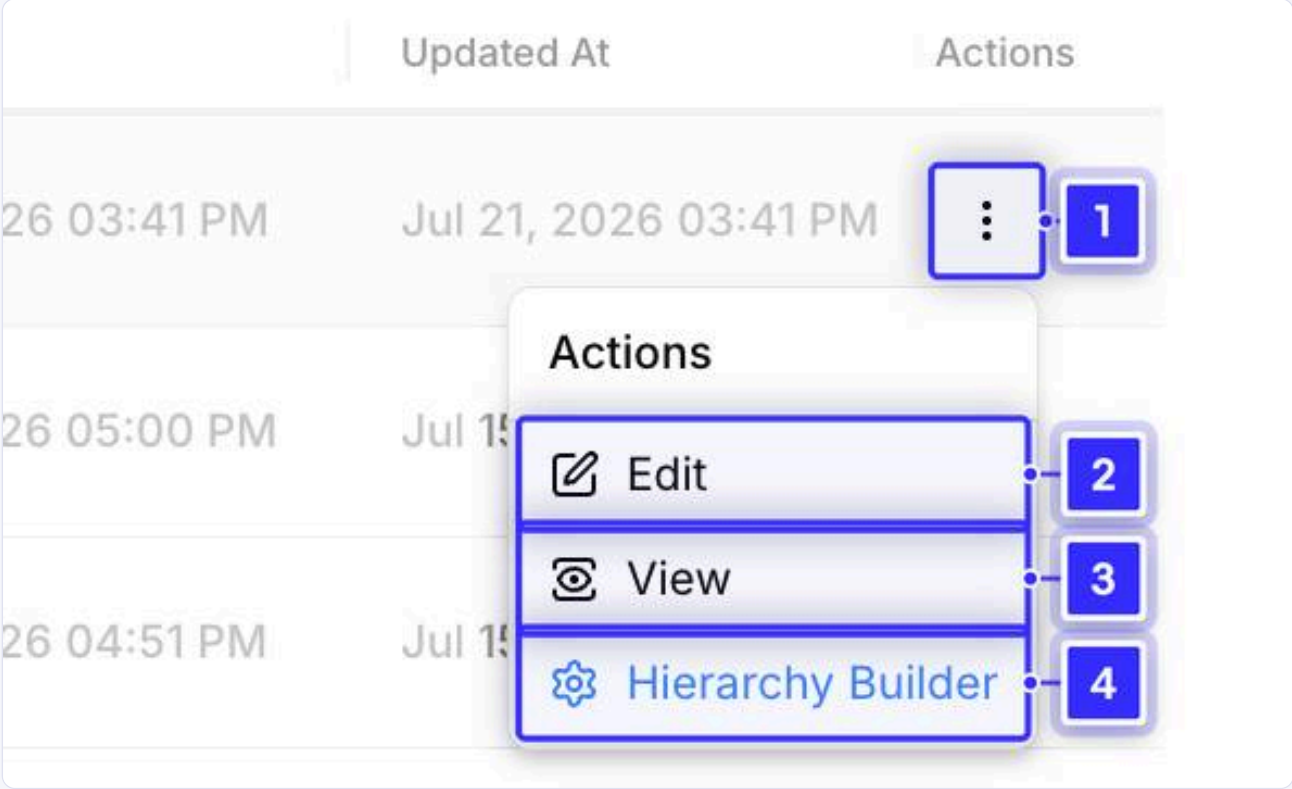


Figure 4.16 A row's ⋮ button (1) and its Actions menu: Edit (2), View (3) and Hierarchy Builder (4)

Add a hierarchy

Fyscal ARCX → Case Manager → Config → Team Management → + Add Hierarchy

Use this dialog when you need a new hierarchy template. **+ Add Hierarchy** opens the **Add New Hierarchy Template** dialog: "Create a new hierarchy template to define organizational structures."

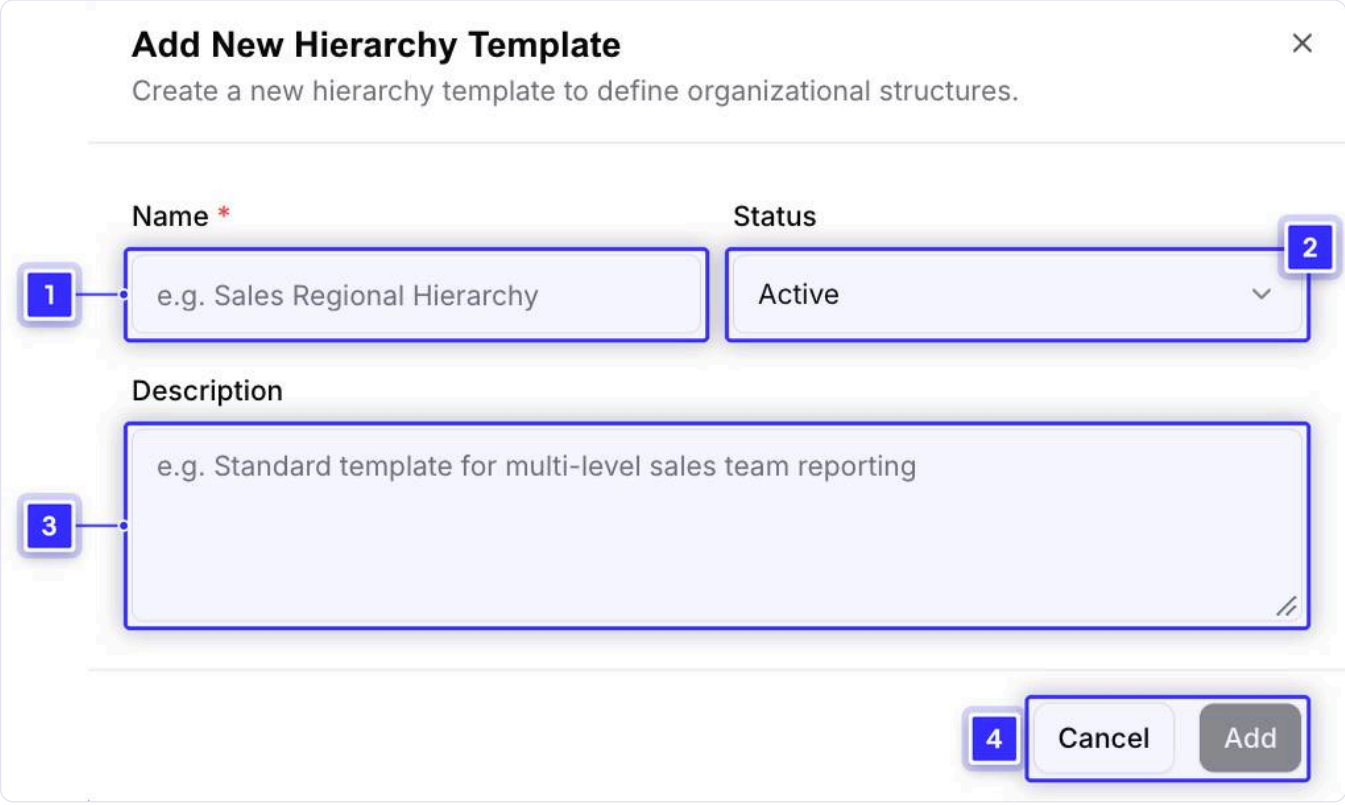


Figure 4.17 Add New Hierarchy Template: Name (1), Status (2), Description (3), and Cancel and Add (4)

#	Field	What it expects	Required	Options or format
1	Name	The hierarchy's name	Yes (*)	Text; placeholder "e.g. Sales Regional Hierarchy"
2	Status	The hierarchy's status	No	Active (default), Inactive
3	Description	A description of the hierarchy	No	Multi-line text; placeholder "e.g. Standard template for multi-level sales team reporting"
4	Cancel / Add	Close without saving, or add the hierarchy	–	**Add** is greyed out when the dialog opens empty

Step 1 **Open the dialog**

Click **+ Add Hierarchy** at the top right of Team Management.

Step 2 **Complete the form**

Enter a **Name**, leave **Status** at **Active** or choose **Inactive**, and add a **Description** if you need one.

Step 3 **Add or cancel**

Click **Add**, or **Cancel** or × to close the dialog without adding.

View a hierarchy's details

Fyscal ARCX → Case Manager → Config → Team Management → ⋮ → View

Open a hierarchy's details to check its IDs, description, status and dates without changing anything. Choose **View** from a row's Actions menu. A details dialog opens, titled **View API Key** (1), with a two-column table (**Name**, **Value**) and a **Close** button. Figure 4.18 shows the details of **AML Hierarchy**, ID 4.

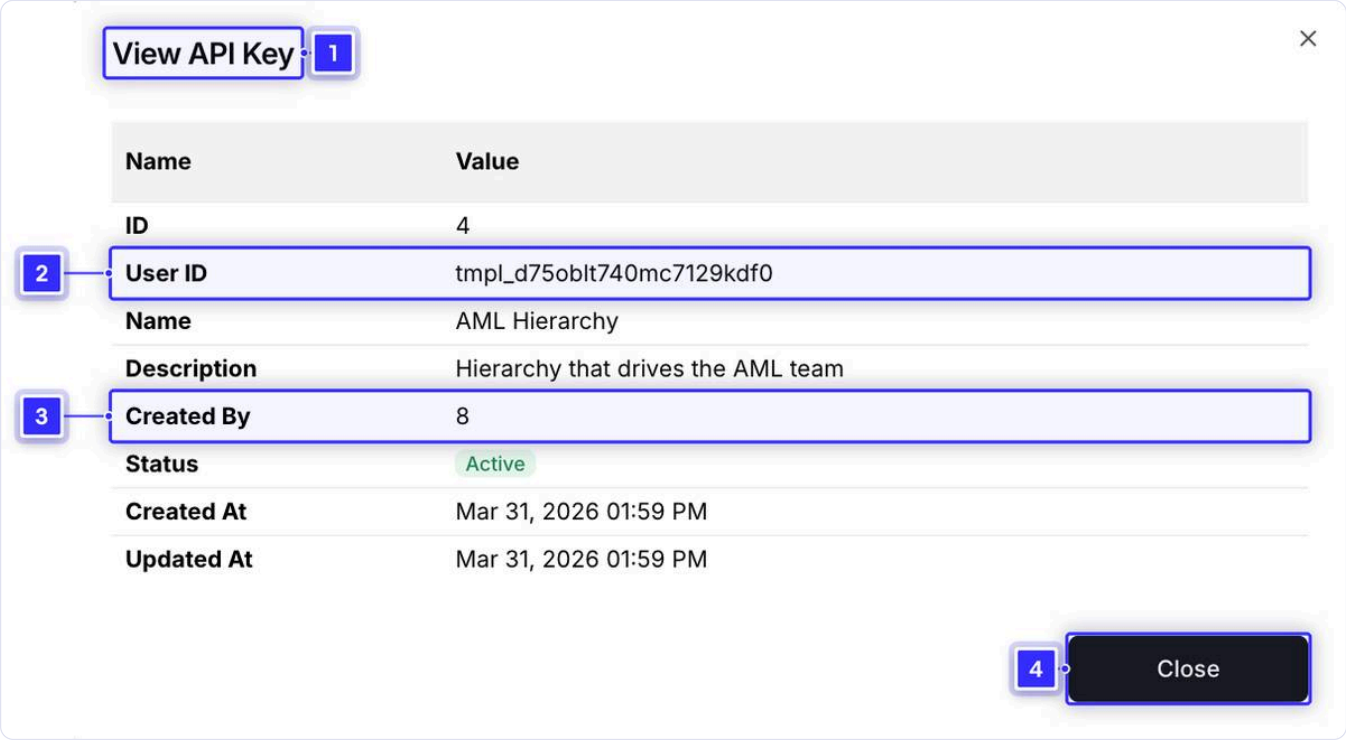


Figure 4.18 Details of AML Hierarchy (ID 4): the dialog title (1), the template ID in the row labelled User ID (2), Created By shown as a number (3) and Close (4)

Row label	What it shows	Example (AML Hierarchy)
ID	The numeric ID from the list	4
User ID (2)	The hierarchy's template ID	tmpl_d75oblt740mc7129kdf0
Name	The hierarchy's name	AML Hierarchy
Description	The description entered for it	Hierarchy that drives the AML team
Created By (3)	A number (the list shows a name in this column)	8
Status	The hierarchy's status	Active
Created At	When it was created	Mar 31, 2026 01:59 PM
Updated At	When it was last updated	Mar 31, 2026 01:59 PM

Click **Close** (4) or × to close the dialog.

The hierarchy builder: Template Builder tab

Fyscal ARCX → Case Manager → Config → Team Management → ⋮ → Hierarchy Builder → Template Builder

Use the Template Builder tab to see which roles a hierarchy has and the level each role sits at. Choosing **Hierarchy Builder** from a row's Actions menu opens the builder for that hierarchy. The builder has two tabs, **Template Builder** and **Hierarchy Builder**. The Template Builder tab is headed **Hierarchy Template Builder**: "Create a template, assign roles, and arrange their hierarchy levels."

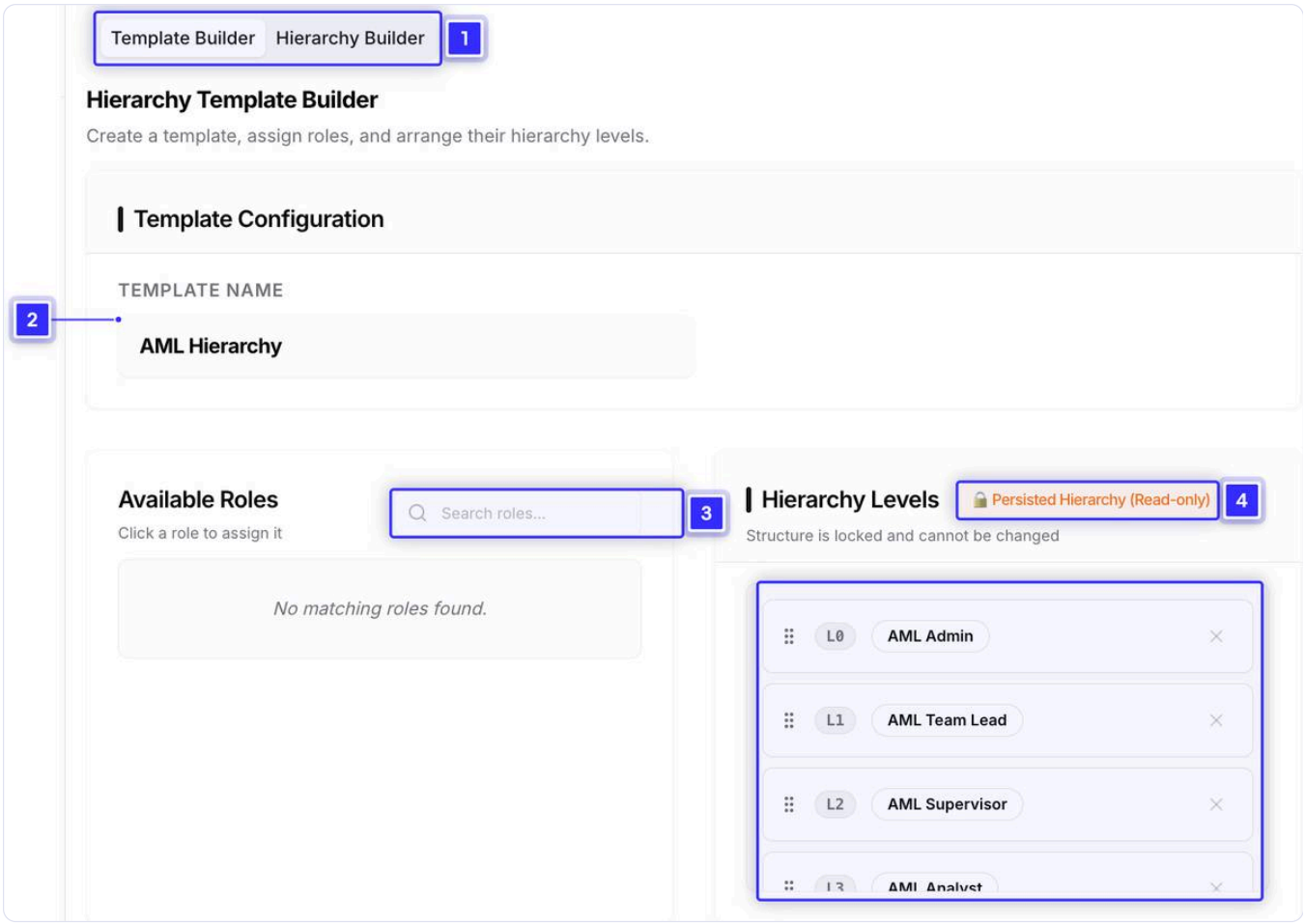


Figure 4.19 Template Builder for AML Hierarchy: the tabs (1), Template Configuration (2), Available Roles with its search (3), and Hierarchy Levels marked Persisted Hierarchy (Read-only) with L0 AML Admin to L3 AML Analyst (4); the level list scrolls, so L3 is partly hidden

1. The **Template Builder** and **Hierarchy Builder** tabs.
2. **Template Configuration**: **TEMPLATE NAME**, here **AML Hierarchy**.
3. **Available Roles** ("Click a role to assign it"): a *Search roles...* box and the role list. For AML Hierarchy the list shows *No matching roles found.*
4. **Hierarchy Levels**, tagged **Persisted Hierarchy (Read-only)** with the text "Structure is locked and cannot be changed". Each level is a row with a drag handle, the level (L0 to L3), the role, and a greyed-out × at the right.

Level	Role (Template Builder)	Depth card (Hierarchy Builder)
L0	AML Admin	Depth 0, AML ADMIN, 4 Members
L1	AML Team Lead	Depth 1, AML TEAM LEAD, 7 Members
L2	AML Supervisor	Depth 2, AML SUPERVISOR, 6 Members
L3	AML Analyst	Depth 3, AML ANALYST, 2 Members

The hierarchy builder: Hierarchy Builder tab

Fyscal ARCX → Case Manager → Config → Team Management → ⋮ → Hierarchy Builder → Hierarchy Builder

Use the Hierarchy Builder tab to see who belongs to each depth of the hierarchy and how the members are connected. The **Hierarchy Builder** tab shows the hierarchy as a chart on a canvas. Each person is a card labelled with their role (for example AML ADMIN, AML TEAM LEAD) and their name, and lines connect each card to the cards at the next depth below it. On this tab the sidebar is shown as a narrow icon rail.

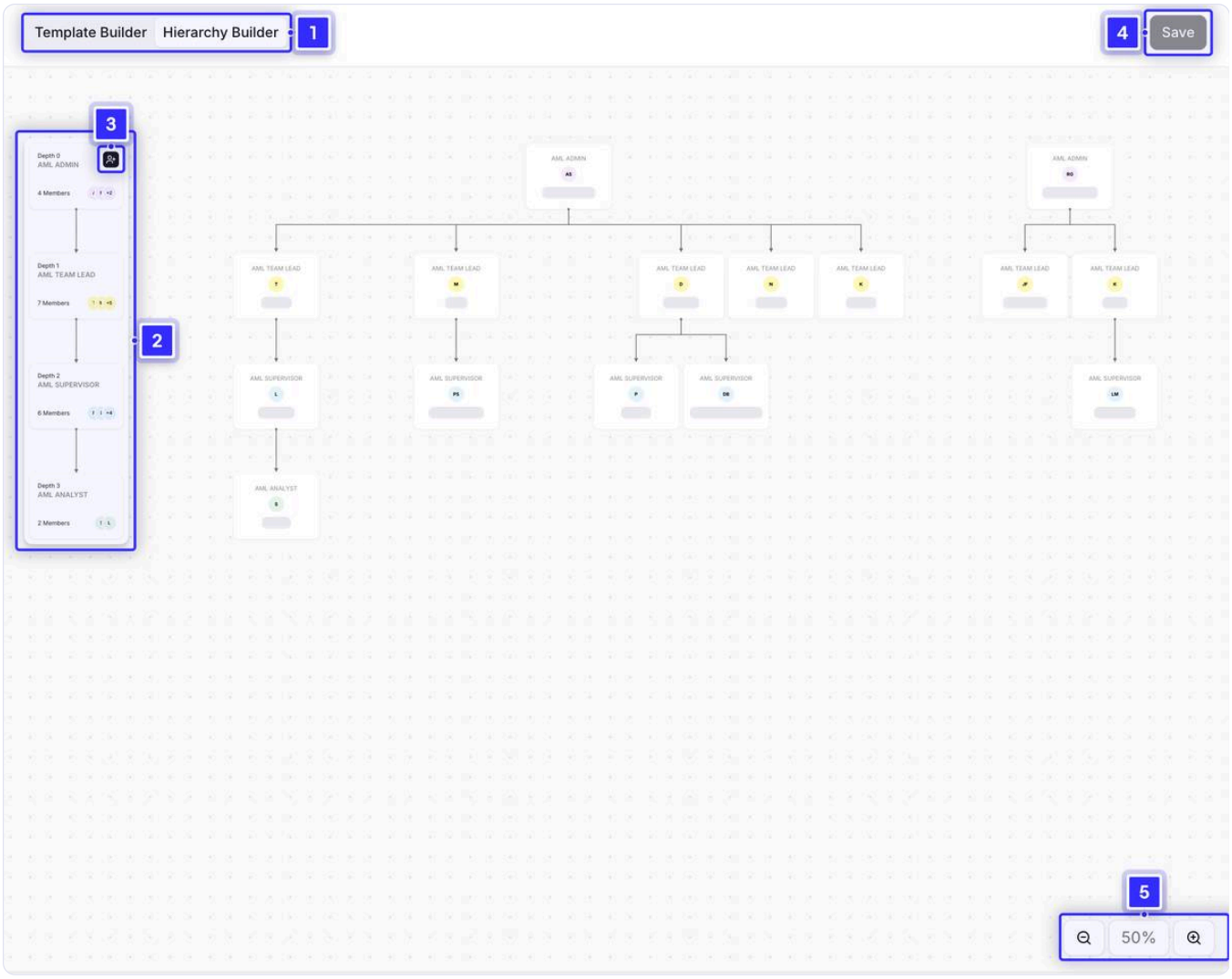


Figure 4.20 Hierarchy Builder for AML Hierarchy: the tabs (1), the depth panel (2), the person-and-plus button (3), Save (4) and the zoom controls at 50% (5); member names hidden

1. The **Template Builder** and **Hierarchy Builder** tabs.
2. The depth panel: one card per depth (**Depth 0** AML ADMIN, **Depth 1** AML TEAM LEAD, **Depth 2** AML SUPERVISOR, **Depth 3** AML ANALYST), each with its member count and member initials.
3. A button with a person-and-plus icon on the Depth 0 card.
4. **Save**, at the top right. It is shown greyed out in Figure 4.20.
5. Zoom out, the zoom level (**50%** when the tab opens) and zoom in.

RELATED IN CORE WORKFLOW

Case Manager | Customer 360 | Regulatory Reports

CORE WORKFLOW

5 Customer 360

Fyscal ARCX → Customers → Customer 360

Customer 360 is where you look a customer up. Analysts and reviewers use it during an investigation to find a customer in the list and open their Customer Profile, which brings together identity and KYC details, accounts, transaction analytics, transactions, prior cases and alerts, screening history and STR history. Administrators set up the customer risk profile (CRP) next to it, under **Customers**: which customer details are scored, how much each one weighs, and the score bands that turn a score into a risk level.

FOR
Analysts, supervisors and team leads; administrators for the CRP

IN THE MENU
Fyscal ARCX → Customers → Customer 360, Risk Score Configuration, Score Configuration

READING TIME
About 26 min

The customer list: read the customer table and move between pages.

Search and filter the list: find one customer, or narrow the list by KYC level, risk tier or country.

The Customer Profile: check a customer's profile tags, financial details and accounts.

Customer Risk Score tab: see the customer's risk score and how each attribute adds to it.

Analytics tab: see the customer's incoming and outgoing totals, top counterparties and transaction types.

Transactions tab: chart the customer's activity, filter their transactions and export them.

Other Cases / Alerts tab: see the cases and alerts already raised for the customer.

Screening History tab: see which name-screening runs included the customer and their result.

STR History tab: see the STRs linked to the customer.

Review a customer during an investigation: go through the profile tab by tab, with a worked example comparing the profile with the activity.

Customer risk profile (CRP): how a customer's risk score is worked out from scored attributes and weightages.

Set up the risk score attributes: add attributes, score their values from 0 to 100 and weight them up to 100% in total.

Set the score bands: set the score ranges for Low, Medium and High.

Configuration history: see which version is active and who changed it.

The customer list

Fyscal ARCX → Customers → Customer 360

Start from the customer list to find the customer you need. The **Customer 360** page shows one row per customer, with a search box, a **Refresh** button and a **Show Filters** button above the table.

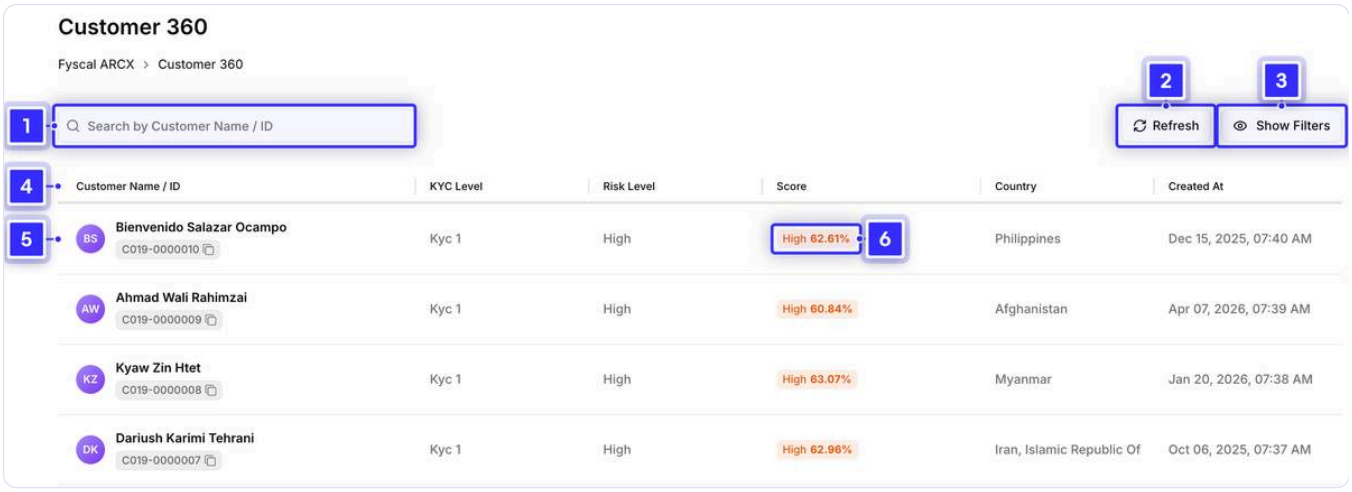


Figure 5.1 The Customer 360 list: search (1), Refresh (2), Show Filters (3), the column headings (4), a customer row (5) and the Score tag (6)

1. **Search by Customer Name / ID**: finds customers by name or Customer ID.
2. **Refresh**: reloads the list.
3. **Show Filters**: opens the filter bar (KYC Level, Risk Tier, Country). The button then reads **Hide Filters**.
4. Column headings: **Customer Name / ID**, **KYC Level**, **Risk Level**, **Score**, **Country**, **Created At**.
5. A customer row: initials avatar, customer name, and the Customer ID with a copy icon.
6. **Score**: the score band and percentage, as a coloured tag (here **High 62.61%**).

Column	What it shows	Format or values seen
Customer Name / ID	The customer's name (individual or business), with the Customer ID below it and a copy icon next to the ID. Long names are shortened with "...".	For example **Bienvenido Salazar Ocampo**, **C019-0000010**
KYC Level	The customer's KYC level as held in the customer data.	**Kyc 0**, **Kyc 1** (see the note under Search and filter the list)
Risk Level	The customer's risk level, as a coloured tag.	**Low**, **Medium**, **High**
Score	The customer's score band and percentage, as a coloured tag (see Customer risk profile (CRP)).	For example **High 62.61%**
Country	The customer's country.	For example **Philippines**
Created At	The date and time of the customer record.	For example **Dec 15, 2025, 07:40 AM**

Below the table, the count line and the page controls show where you are in the list. The list shows 20 customers per page.

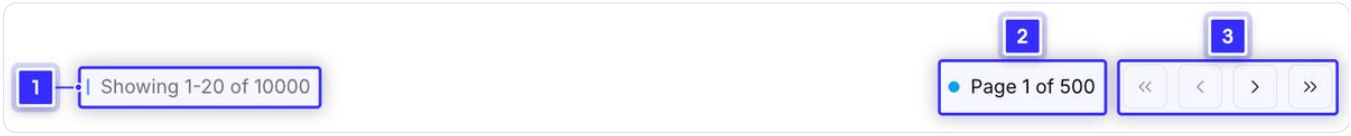


Figure 5.2 The count line, Showing 1-20 of 10000 (1), the page indicator, Page 1 of 500 (2), and the page buttons (3)

1. **Showing 1-20 of 10000**: the rows on this page and the total number of customers that match the current search and filters.
2. **Page 1 of 500**: the page you are on.
3. Four buttons: first page, previous page, next page and last page.

Search and filter the list

Fyscal ARCX → Customers → Customer 360 → Show Filters

Use the search box to find one customer, and the filters to narrow the list by KYC level, risk tier or country.

Filter	Default	Options shown
KYC Level	**All**	**All**, **Advanced**, **Basic**, **Complete**

Filter	Default	Options shown
Risk Tier	**All**	A list with a search box: **Low**, **Medium**, **High**
Country	**All**	A list of country names with a search box, in alphabetical order from **Afghanistan** (243 options, including **Unknown**).

Step 1 **Search for a customer**

Click the **Search by Customer Name / ID** box and type the customer's name or Customer ID, for example **CUST-FYSCAL-604554**.

Step 2 **Open the filters**

Click **Show Filters**. Three filters appear below the search box: **KYC Level** (1), **Risk Tier** (2) and **Country** (3), each set to **All**. The button now reads **Hide Filters** (4); click it to close the filter bar.



Figure 5.3 The filter bar: KYC Level (1), Risk Tier (2) and Country (3), with Hide Filters (4)

Step 3 **Filter by KYC Level**

Click the **KYC Level** box (1) and choose one option. A tick marks the current choice (**All** (2)). The other options are **Advanced**, **Basic** and **Complete**.

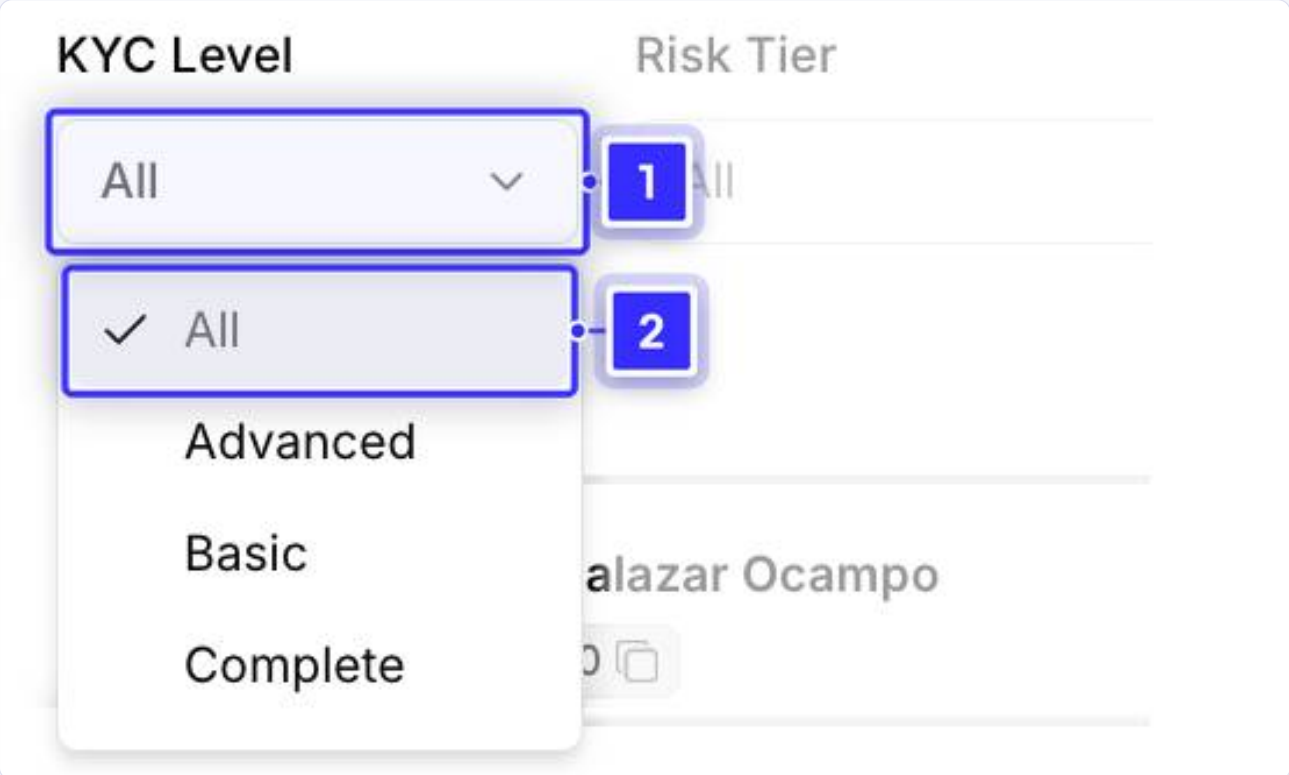


Figure 5.4 The KYC Level filter (1): All ticked (2), then Advanced, Basic and Complete

> **Note**
> The KYC Level filter options (Advanced, Basic and Complete) do not match the values shown in the customer data. The **KYC Level** column shows values such as **Kyc 0** and **Kyc 1**, and the Customer Profile shows values such as **KYC L2**. The screens do not show how the filter options relate to these values.

:::

Step 4 **Filter by Risk Tier**

Click the **Risk Tier** box. The list has a search box (1), followed by **Low**, **Medium** and **High**. Click the tier to show.

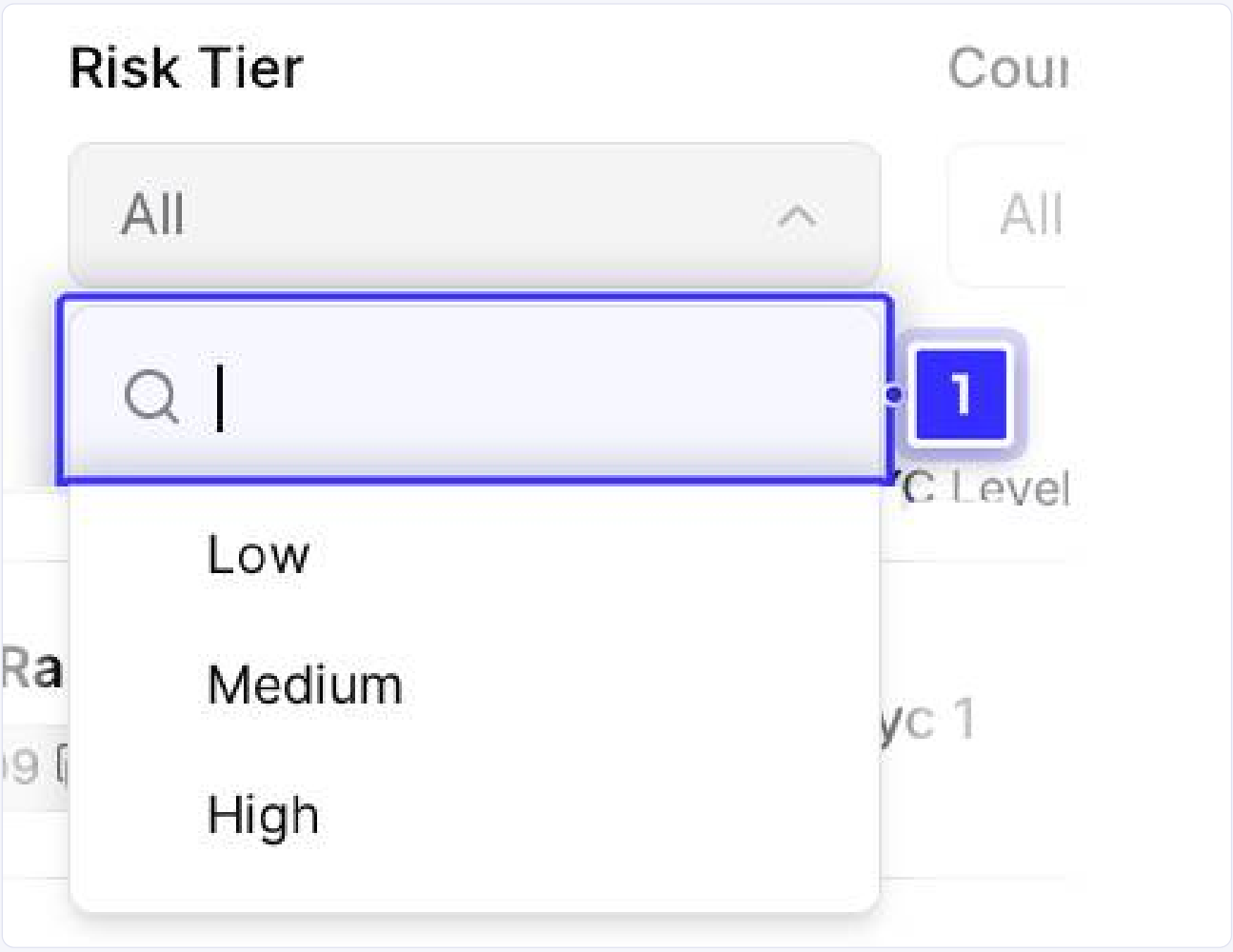


Figure 5.5 The Risk Tier filter: the search box (1), then Low, Medium and High

> **Note**
> The **Risk Level** values seen in the list are **Low**, **Medium** and **High**, but in testing a search of the Risk Tier list for High, Medium or Low returned no options.

:::

Step 5 **Filter by Country**

Click the **Country** box. Type part of a country name in the search box (1) at the top of the list, then click the country. The list (2) is alphabetical and long (243 options), so searching is quicker than scrolling.

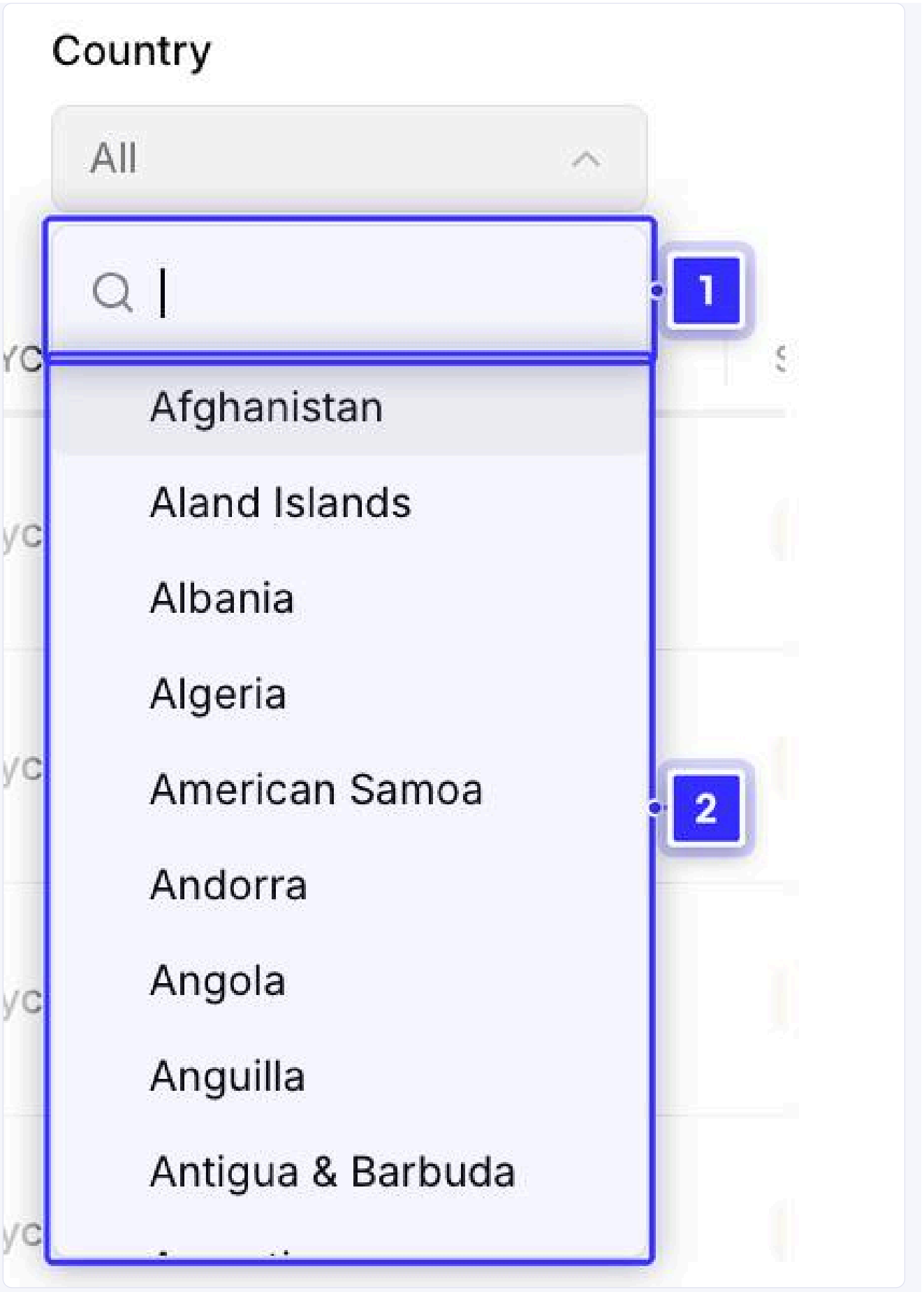


Figure 5.6 The Country filter: the search box (1) and the alphabetical list of countries (2)

Step 6 **Reload the list**

Click **Refresh** to reload the list.

The Customer Profile

Fyscal ARCX → Customers → Customer 360 → *customer name*

Open the Customer Profile to see everything held on one customer: profile tags, financial details, accounts and the tabs described below, starting with the Customer Risk Score. Click a customer in the list to open the **Customer Profile**. The breadcrumb reads **Fyscal ARCX › Customer 360 ›**customer name*; click **Customer 360** in it to return to the list. The examples in this chapter use the customer **Rafael Serrano Dimaculangan** (**CUST-FYSCAL-604554**).

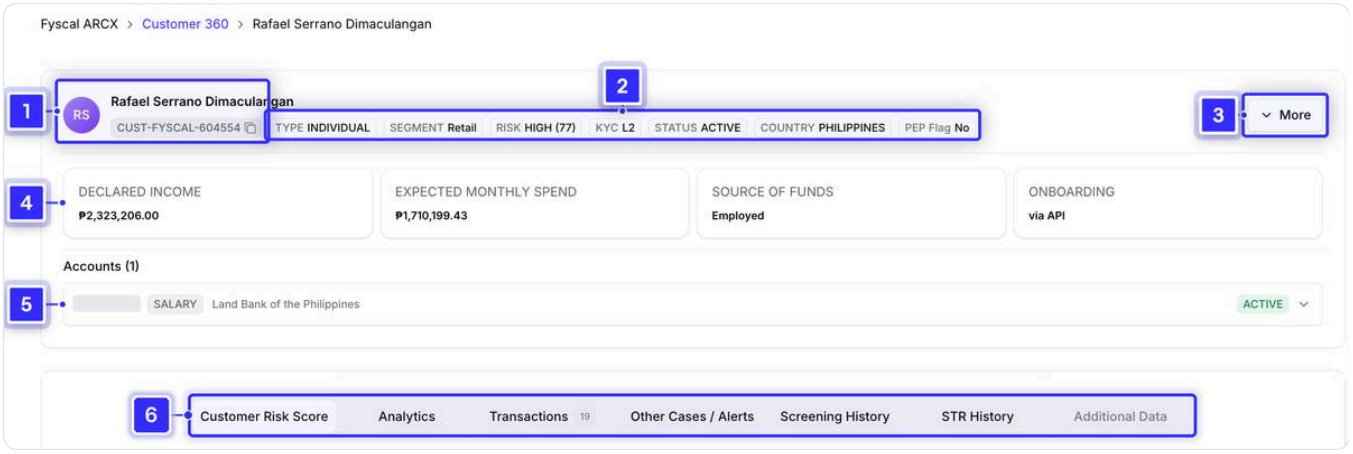


Figure 5.7 The Customer Profile for Rafael Serrano Dimaculangan: name and ID (1), profile tags (2), More (3), summary cards (4), Accounts (5) and the tabs, starting with Customer Risk Score (6)

1. The customer's name, initials avatar and Customer ID (with a copy icon).
2. Profile tags: **TYPE**, **SEGMENT**, **RISK**, **KYC**, **STATUS**, **COUNTRY** and **PEP Flag**.
3. **More**: expands the profile card with three detail panels (Figure 5.8). It then reads **Less**.
4. Summary cards: **DECLARED INCOME**, **EXPECTED MONTHLY SPEND**, **SOURCE OF FUNDS**, **ONBOARDING**.
5. **Accounts (1)**: the customer's accounts, with the number of accounts in brackets.
6. Tabs: **Customer Risk Score** (selected: the profile opens on it), **Analytics**, **Transactions** (with a count, here 19), **Other Cases / Alerts**, **Screening History**, **STR History** and **Additional Data** (greyed out, not described in this edition).

Note

The profile opens on the **Customer Risk Score** tab, which is explained first below, before **Analytics**. The customer's risk score also appears as a coloured tag next to their name (see Customer Risk Score tab).

Field	What it shows	Example
TYPE	Customer type.	**INDIVIDUAL**
SEGMENT	Customer segment.	**Retail**
RISK	Risk tier, with a number in brackets.	**HIGH (77)**
KYC	KYC level.	**L2**
STATUS	Customer status.	**ACTIVE**
COUNTRY	Customer country.	**PHILIPPINES**
PEP Flag	Whether the customer is flagged as a politically exposed person.	**No**
DECLARED INCOME	Income declared by the customer.	**₱2,323,206.00**
EXPECTED MONTHLY SPEND	Expected monthly spend.	**₱1,710,199.43**

Field	What it shows	Example
SOURCE OF FUNDS	Declared source of funds.	**Employed**
ONBOARDING	Onboarding channel.	**via API**
Accounts row	Account number, account type, institution and account status, with an expand arrow at the right.	account number (hidden in the figures), **SALARY**, **Land Bank of the Philippines**, **ACTIVE**

Step 1 **See the full customer details**

Click **More** at the top right of the profile card. Three panels open between the summary cards and **Accounts**. The button now reads **Less** (1); click it to close them.

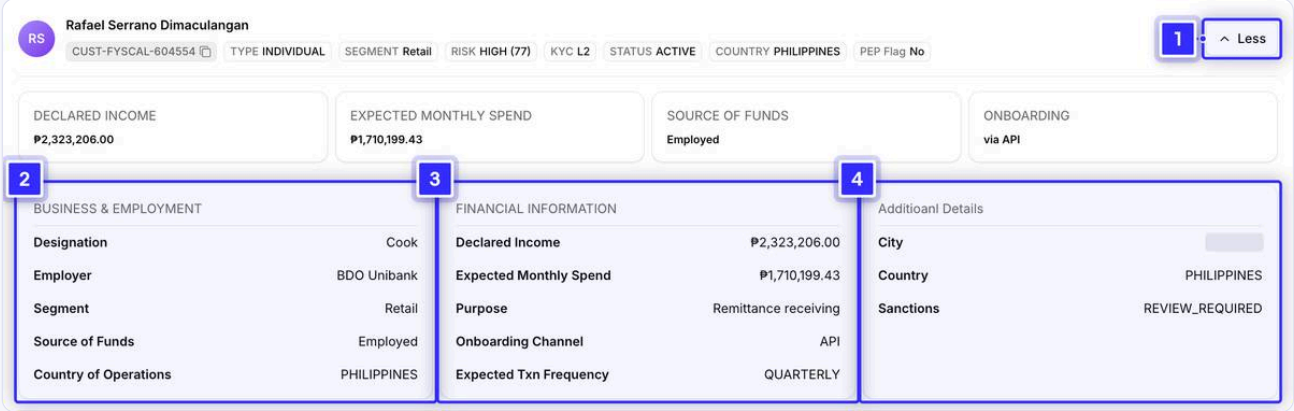


Figure 5.8 The profile card expanded: Less (1), BUSINESS & EMPLOYMENT (2), FINANCIAL INFORMATION (3) and Additioanl Details (4)

Panel	Fields	Example values
2 BUSINESS & EMPLOYMENT	**Designation**, **Employer**, **Segment**, **Source of Funds**, **Country of Operations**	Cook, BDO Unibank, Retail, Employed, PHILIPPINES
3 FINANCIAL INFORMATION	**Declared Income**, **Expected Monthly Spend**, **Purpose**, **Onboarding Channel**, **Expected Txn Frequency**	₱2,323,206.00, ₱1,710,199.43, Remittance receiving, API, QUARTERLY
4 Additioanl Details (spelled this way on screen)	**City**, **Country**, **Sanctions**	city (hidden in the figure), PHILIPPINES, REVIEW_REQUIRED

AML context

Customer due diligence records what the institution expects of a customer: who they are, their risk rating, whether they are a politically exposed person, their income and source of funds, and how much and how often they expect to transact. Monitoring and investigations compare actual activity with this expected behaviour.

Customer Risk Score tab

Fyscal ARCX → Customers → Customer 360 → *customer name* → Customer Risk Score

The **Customer Risk Score** tab shows the result of the customer risk profile (CRP) for one customer: their risk score, its band, and how each attribute adds to it. It is the first tab of the Customer Profile. The same score appears as a coloured tag next to the customer's name, so you see the risk level as soon as you open the profile.

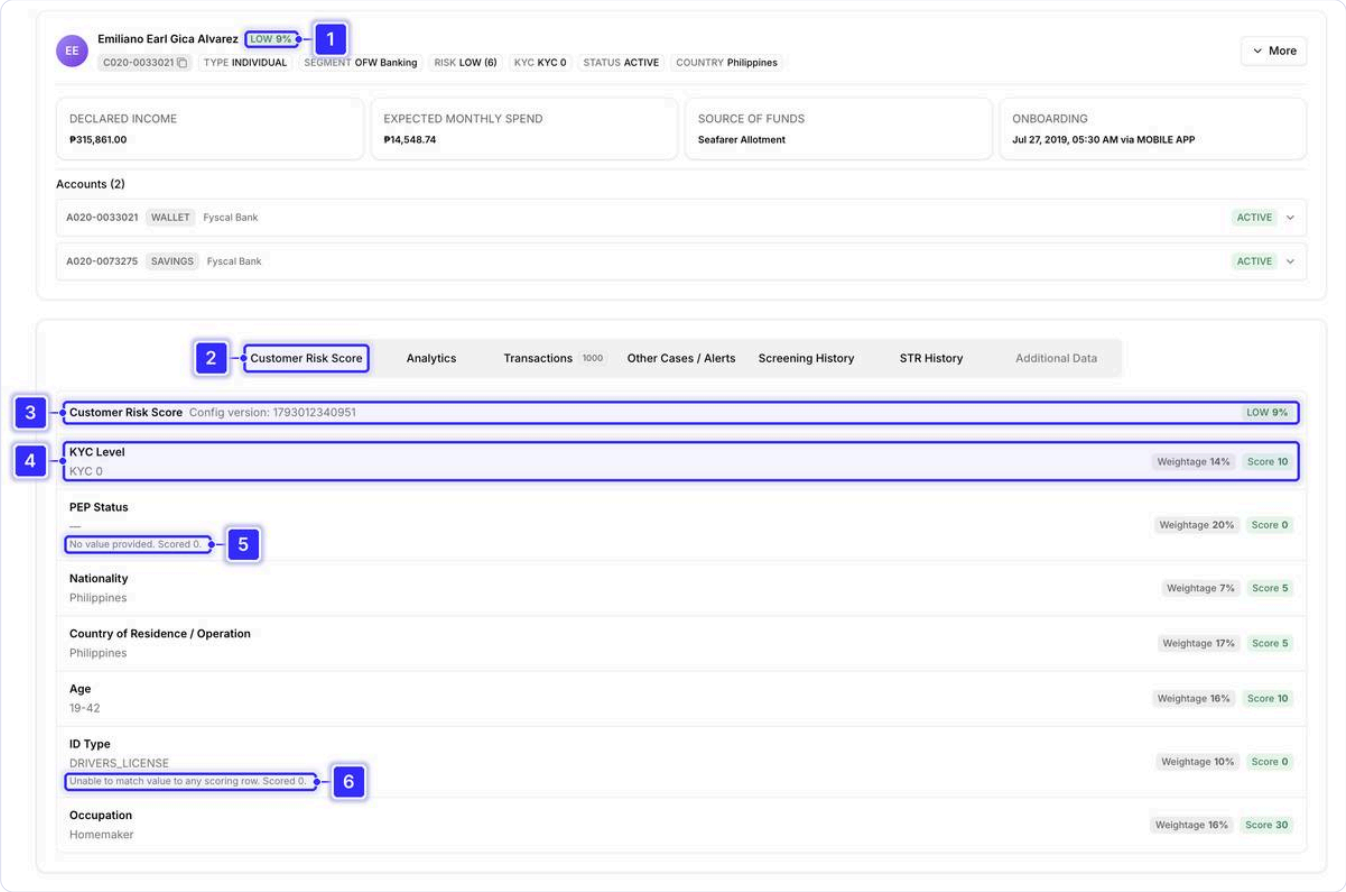


Figure 5.9 The Customer Risk Score tab for Emiliano Earl Gica Alvarez: the score tag next to the name (1), the Customer Risk Score tab (2), the total with the Config version (3), one attribute with its value, weightage and score (4), and the two reasons a value scores 0 (5, 6)

1. The risk score as a tag next to the customer's name, in the colour of its band: **LOW 9%**.
2. **Customer Risk Score**: the first tab of the profile.
3. **Customer Risk Score** with the **Config version** used to calculate it (**1793012340951**, the active version in Configuration history), and the total, **LOW 9%**.
4. An attribute: its name (**KYC Level**), the customer's value (**KYC 0**), the attribute's **Weightage** (**14%**) and the value's **Score** (**10**).
5. *No value provided. Scored 0.*: the customer data has no value for this attribute (**PEP Status** shows —), so it scores 0.
6. *Unable to match value to any scoring row. Scored 0.*: the message shown when the customer has a value (**DRIVERS_LICENSE**) that no row of the attribute matches. This screen shows the attribute with **Score 0**; how such a value is scored is not confirmed for this edition (see Customer risk profile (CRP)).

Each row shows the attribute's **Weightage** and the **Score** of the customer's value. The total at the top is the sum of score × weightage for all attributes, as described in How the risk score is worked out. For this customer:

Attribute	Customer's value	Weightage	Score	Score × weightage
KYC Level	**KYC 0**	14%	10	1.4
PEP Status	— (no value)	20%	0	0
Nationality	**Philippines**	7%	5	0.35
Country of Residence / Operation	**Philippines**	17%	5	0.85
Age	**19-42**	16%	10	1.6
ID Type	**DRIVERS_LICENSE** (no matching row)	10%	0	0
Occupation	**Homemaker**	16%	30	4.8
Total		**100%**		**9**, shown as **LOW 9%**

> **Tip**
> A score of 0 from *No value provided* or *Unable to match value to any scoring row* can make a customer look lower-risk than they are. If you see either message, check the customer's data, and ask the administrator of the risk score configuration whether a scoring row is missing for that value (here, **DRIVERS_LICENSE** under **ID Type**).

> **Note**
> The **RISK** tag in the profile header (here **RISK LOW (6)**) is a separate value held in the customer data; it is not the CRP score. Use the **Customer Risk Score** tab, or the score tag next to the name, for the CRP result.

Analytics tab

Customer Profile → Analytics

Use Analytics for a summary of how money moves in and out of the customer's accounts. **Analytics** is the tab that is open when the profile loads. It summarises the customer's incoming and outgoing transactions, the top counterparties and the transaction types. The panel header shows the customer's name.

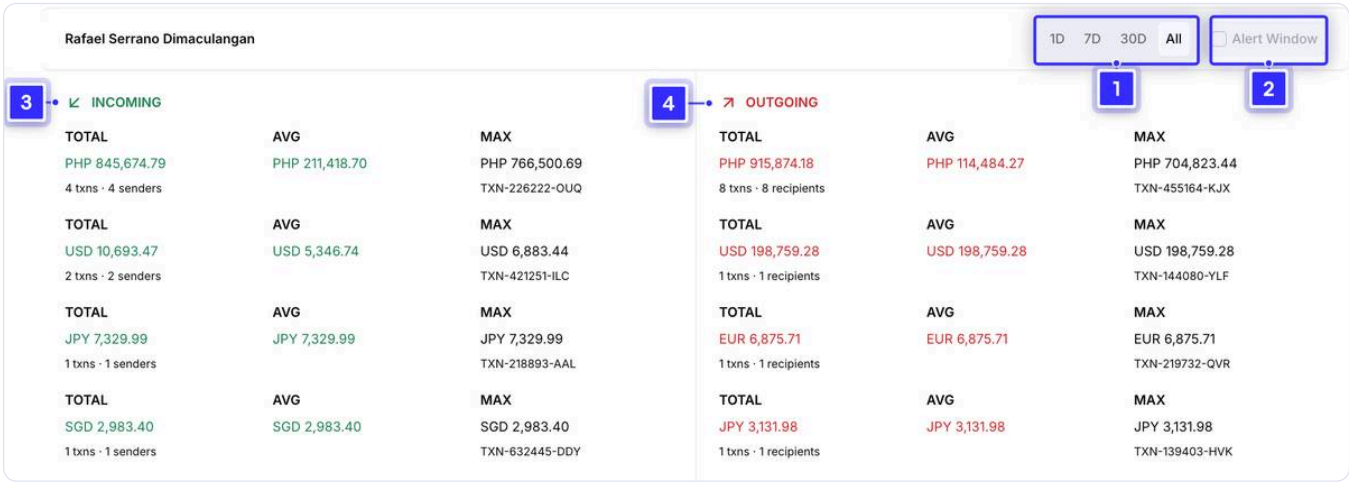


Figure 5.10 Analytics: the period buttons (1), Alert Window (2), and the INCOMING (3) and OUTGOING (4) totals per currency

1. Period buttons: **1D**, **7D**, **30D**, **All**. In the figure, **All** is selected.
2. **Alert Window**: a check box, shown unticked and greyed in the figure.
3. **INCOMING**: one row per currency, each with **TOTAL** (amount, and the number of transactions and senders, for example "4 txns · 4 senders"), **AVG** and **MAX** (amount and the transaction ID of the largest transaction).
4. **OUTGOING**: the same layout for money sent, counting recipients instead of senders.

In the example, incoming money is shown in PHP, USD, JPY and SGD, and outgoing money in PHP, USD, EUR and JPY. Totals are not converted to a single currency.

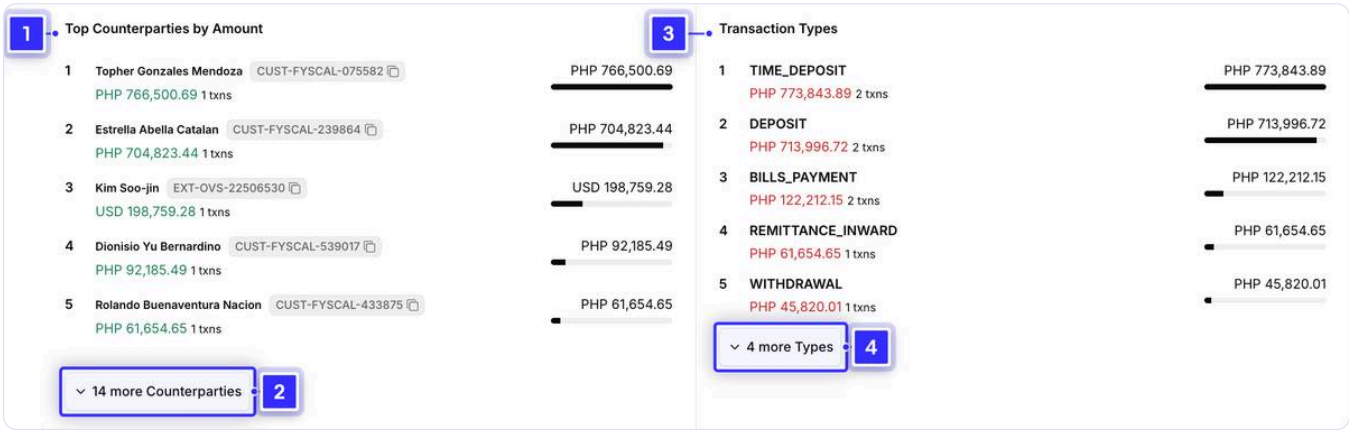


Figure 5.11 Analytics: Top Counterparties by Amount (1) with 14 more Counterparties (2), and Transaction Types (3) with 4 more Types (4)

1. **Top Counterparties by Amount**: the five largest counterparties, ranked, each with name, ID (with a copy icon), amount, number of transactions and a bar at the right.
2. **14 more Counterparties** (in the example): lists the rest of the counterparties.
3. **Transaction Types**: the five largest transaction types (for example **TIME_DEPOSIT**, **DEPOSIT**, **BILLS_PAYMENT**), each with amount, number of transactions and a bar.
4. **4 more Types** (in the example): lists the rest of the transaction types.

Transactions tab

Customer Profile → Transactions

Use the Transactions tab when you need the individual transactions behind the analytics, or a CSV export of them. The **Transactions** tab shows charts of the customer's transaction activity and a table of the transactions. The count on the tab (19 in the example) is the number of transactions.

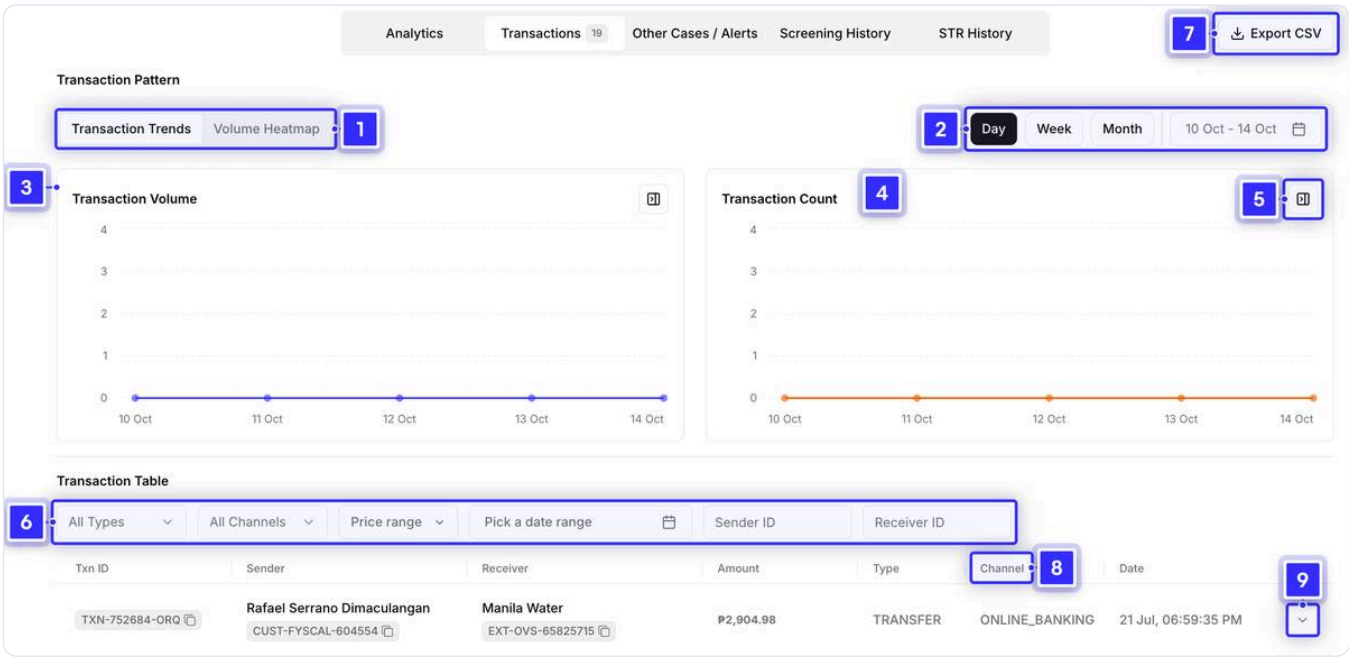


Figure 5.12 The Transactions tab: the Transaction Trends / Volume Heatmap switch (1), grouping and date range (2), the Transaction Volume (3) and Transaction Count (4) charts, Expand (5), the table filters (6), Export CSV (7), the Channel column (8) and a row's expand arrow (9)

1. **Transaction Trends** / **Volume Heatmap**: switches the **Transaction Pattern** view. **Transaction Trends** is selected in the figure.
2. The grouping buttons **Day**, **Week**, **Month** (**Day** selected) and the date range (here **10 Oct - 14 Oct**, with a calendar icon).
3. **Transaction Volume** chart for the selected date range.
4. **Transaction Count** chart for the selected date range.
5. Each chart has an expand button at its top right (*Expand Transaction Volume*, *Expand Transaction Count*).
6. **Transaction Table** filters: **All Types**, **All Channels**, **Price range**, **Pick a date range**, **Sender ID**, **Receiver ID**.
7. **Export CSV**, at the right of the tab bar.
8. **Channel**: the channel of each transaction, for example **ONLINE_BANKING**, **OTC**, **POS**.
9. The arrow at the end of each row.

In the example, the charts cover 10 Oct to 14 Oct and show no activity, while the table lists 19 transactions dated 21 Jul. Change the date range above the charts to chart a different period.

Column	What it shows	Example
Txn ID	Transaction ID, with a copy icon.	**TXN-752684-ORQ**
Sender	Sender name and ID.	Rafael Serrano Dimaculangan, CUST-FYSCAL-604554
Receiver	Receiver name and ID.	Manila Water, EXT-OVS-65825715
Amount	Amount in the transaction currency.	₱2,904.98; SGD 2,983.40; $3,810.03; €6,875.71
Type	Transaction type. Long types are shortened with "...".	TRANSFER, LOAN_PAYMENT, WITHDRAWAL, TIME_DEPOSIT
Channel	Transaction channel.	ONLINE_BANKING, OTC, POS, MOBILE_BANKING
Date	Date and time.	21 Jul, 06:59:35 PM

Other Cases / Alerts tab

Customer Profile → Other Cases / Alerts

Check this tab to see whether the customer has been investigated before. The **Other Cases / Alerts** tab lists the cases and alerts raised for this customer. Cases are managed in Case Manager.

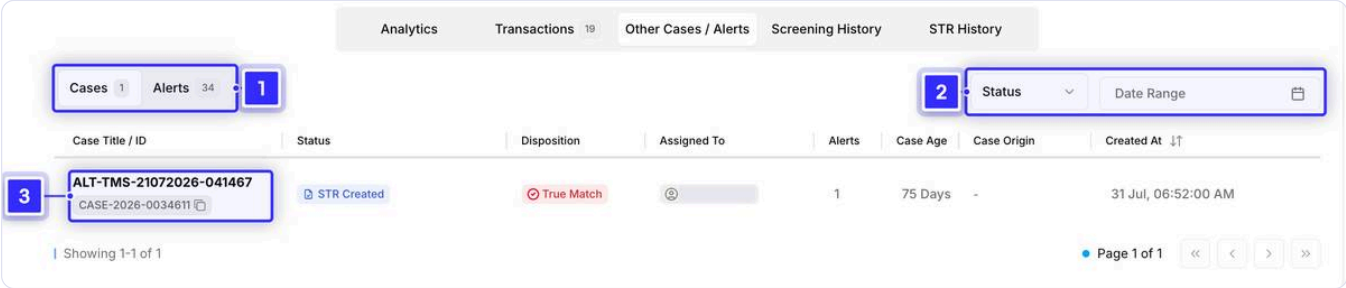


Figure 5.13 Other Cases / Alerts: the Cases and Alerts sub-tabs (1), the Status and Date Range filters (2), and one case, CASE-2026-0034611, in status STR Created (3)

1. Sub-tabs **Cases** and **Alerts**, each with a count (1 case and 34 alerts in the example).
2. Filters: **Status** and **Date Range**.
3. A case row: the case title with the case ID below it; the columns are described in the table below.

Column (Cases)	What it shows	Example
Case Title / ID	Case title, with the case ID and a copy icon below it.	ALT-TMS-21072026-041467, CASE-2026-0034611
Status	Case status.	**STR Created**
Disposition	Case disposition.	**True Match**
Assigned To	The user the case is assigned to.	(hidden in the figure)
Alerts	Number of alerts in the case.	1
Case Age	Age of the case.	75 Days
Case Origin	How the case was created.	-
Created At	Date and time the case was created. The heading has a sort icon.	31 Jul, 06:52:00 AM

Screening History tab

Customer Profile → Screening History

Use this tab to see when the customer was screened against the watchlists and with what result. The **Screening History** tab lists the name-screening runs that included this customer, newest first.

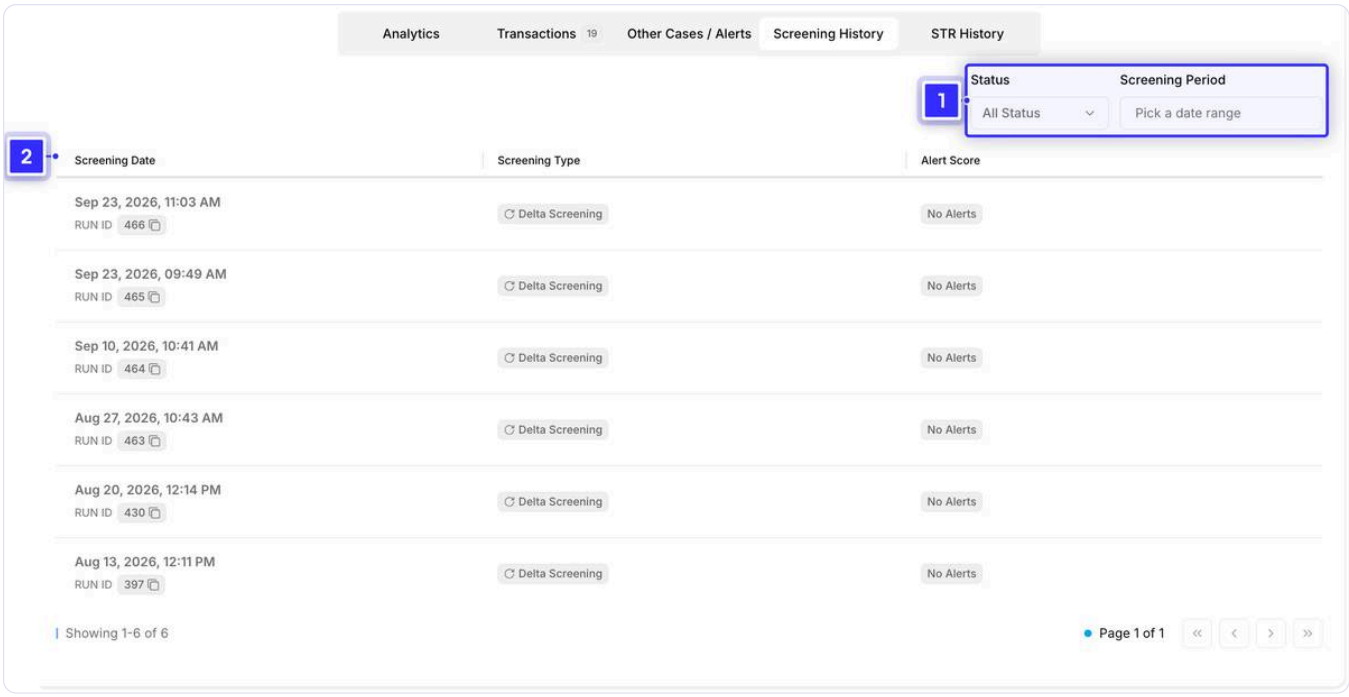


Figure 5.14 Screening History: the Status and Screening Period filters (1) and the columns (2), with six Delta Screening runs, each with No Alerts

1. Filters: **Status** (default **All Status**) and **Screening Period** (**Pick a date range**).
2. Columns: **Screening Date**, **Screening Type**, **Alert Score**.

Column	What it shows	Example
Screening Date	Date and time of the run, with the **RUN ID** (and a copy icon) below it.	Sep 23, 2026, 11:03 AM; RUN ID 466
Screening Type	The kind of screening run.	**Delta Screening**
Alert Score	The result of the run for this customer.	**No Alerts**

The example shows six runs (RUN IDs 466, 465, 464, 463, 430 and 397), all **Delta Screening** with **No Alerts**. Screening runs are described in Name Screening.

STR History tab

Customer Profile → STR History

Use this tab to check whether STRs have already been filed that involve the customer. The **STR History** tab lists Suspicious Transaction Reports (STRs) linked to this customer, in the same columns as the Regulatory Reports register.

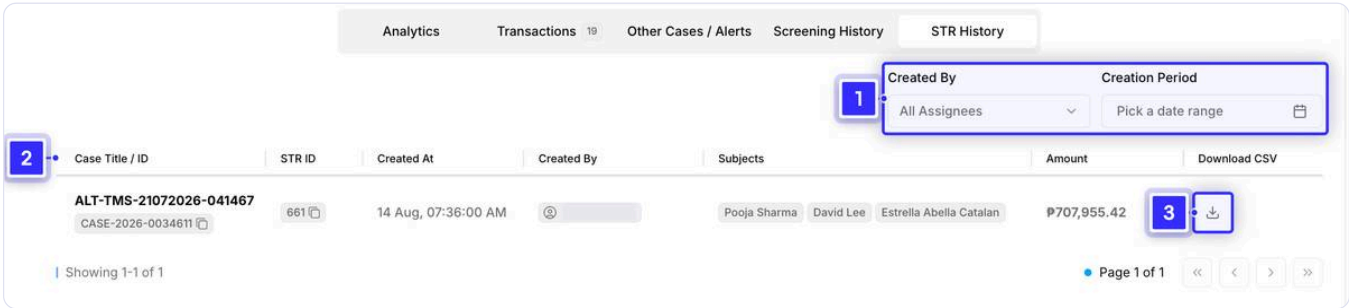


Figure 5.15 STR History: the Created By and Creation Period filters (1), the columns (2) and the Download CSV icon (3), with STR 661 for case CASE-2026-0034611, amount ₱707,955.42

1. Filters: **Created By** (default **All Assignees**) and **Creation Period** (**Pick a date range**).
2. The columns, described in the table below.
3. **Download CSV**: a download icon in each row.

Column	Example
Case Title / ID	ALT-TMS-21072026-041467, CASE-2026-0034611
STR ID	661
Created At	14 Aug, 07:36:00 AM
Created By	(hidden in the figure)
Subjects	Pooja Sharma, David Lee, Estrella Abella Catalan
Amount	₱707,955.42
Download CSV	A download icon (3 in the figure)

The case in this row, CASE-2026-0034611, is the case listed under Other Cases / Alerts. For what each column means and how to open a filed STR, see Regulatory Reports.

> **Note**
> The **Subjects** of STR 661 shown here are Pooja Sharma, David Lee and Estrella Abella Catalan; they do not include Rafael Serrano Dimaculangan. David Lee and Estrella Abella Catalan appear as his counterparties on the Transactions tab.

Review a customer during an investigation

Fyscal ARCX → Customers → Customer 360 → *customer name*

WHEN	WHERE	EDITS	OUTPUT
While you work an alert or case for the customer	Customer 360 → the Customer Profile	None: the profile shows no edit controls	Notes for the case timeline and the rationale

Use the Customer Profile to compare what the customer said they would do with what they actually did, and to check their history. Work through it in the order below and note what you find in the case's Timeline and notes.

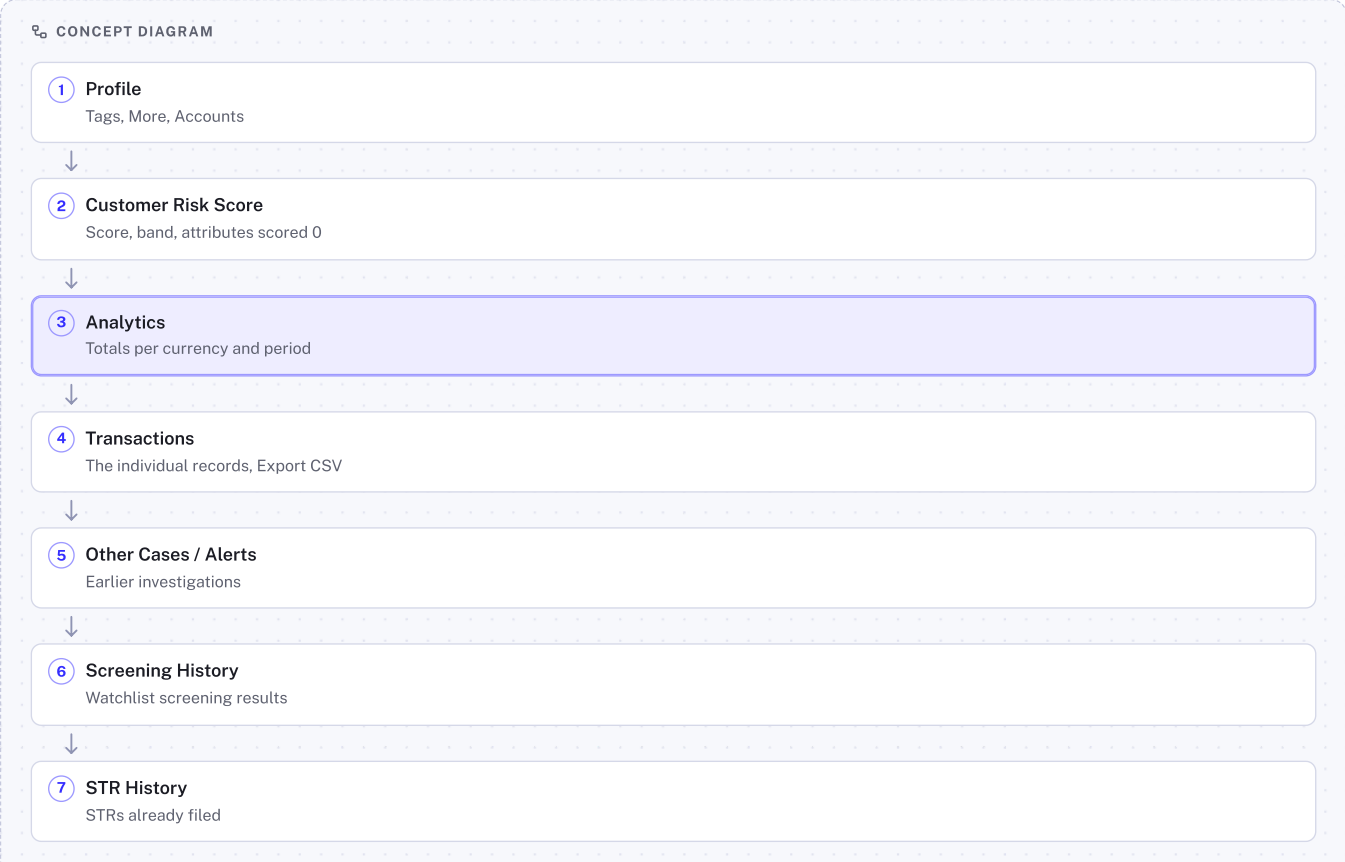


Diagram 5.1 — Reviewing a customer, tab by tab

The order goes from what the customer declared, to what they did, to what the institution already knows about them. Each step below matches one box of the diagram.

Step 1 Read the profile

Open the customer (see The Customer Profile). Note **RISK**, **KYC**, **STATUS** and **PEP Flag**, then click **More** and note **Expected Monthly Spend**, **Purpose**, **Expected Txn Frequency** and **Sanctions**. Check the account status under **Accounts**.

Step 2 Check the risk score

On Customer Risk Score, note the score and its band, which attributes add the most to it, and any attribute scored 0 because of *No value provided* or *Unable to match value to any scoring row*.

Step 3 Compare with the Analytics totals

On Analytics, choose the period (**1D**, **7D**, **30D** or **All**) that you want to compare with the profile. Read **INCOMING** and **OUTGOING** one currency at a time: totals are not converted to a single currency. Note the largest transaction (**MAX**) and the top counterparties.

Step 4 Check the individual transactions

On Transactions, find the transactions behind the totals: their dates, types and counterparties. Set the date range above the charts to the period of the transactions, and use **Export CSV** if you need the list outside the platform.

Step 5 Look for earlier cases and alerts

On Other Cases / Alerts, check the **Cases** and **Alerts** counts and the status and disposition of earlier cases.

Step 6 Check the screening results

On Screening History, check when the customer was last screened and the **Alert Score** of each run.

Step 7 Check for earlier STRs

On STR History, check whether STRs have already been filed and open them in Regulatory Reports if you need the detail.

Worked example: profile against activity

The values below are all on screen for Rafael Serrano Dimaculangan (CUST-FYSCAL-604554), with **All** selected on Analytics (Figure 5.10) and the profile expanded with More (Figure 5.8). The Transactions tab lists 19 transactions, all dated 21 Jul.

Profile says	Activity shows	Point to note in the case
Expected Monthly Spend ₱1,710,199.43	**OUTGOING** PHP 915,874.18 (8 txns · 8 recipients), plus USD 198,759.28, EUR 6,875.71 and JPY 3,131.98 in one transaction each	Compare spend currency by currency; the foreign-currency amounts are not included in the PHP total.
Expected Txn Frequency QUARTERLY	19 transactions, all on 21 Jul	Many transactions on one day against a quarterly expectation.
Purpose Remittance receiving	**INCOMING** PHP 845,674.79 (4 txns · 4 senders); **OUTGOING** PHP 915,874.18	More PHP sent out than received, against a stated purpose of receiving remittances.
Designation Cook; **Declared Income** ₱2,323,206.00	Largest outgoing transaction PHP 704,823.44 (TXN-455164-KJX) to Estrella Abella Catalan	The size of single transactions against the stated occupation and income.
Sanctions REVIEW_REQUIRED	Screening History: six Delta Screening runs, each **No Alerts**	What the REVIEW_REQUIRED value refers to, and whether it has been resolved.

None of these points decides the case on its own. Record them, with the values, in your notes and in the rationale when you dispose the alerts (see Dispose alerts and close a case).

Customer risk profile (CRP)

Fyscal ARCX → Customers → Risk Score Configuration

The customer risk profile (CRP) gives every customer a risk score from 0 to 100, worked out from their customer data. Administrators decide which customer details count towards the score and how much each one counts; the platform applies the same settings to every customer. The CRP is set up on two pages under **Customers**, next to **Customer 360**:

- **Risk Score Configuration**: the attributes that are scored, the score of each attribute value, and the weightage of each attribute.
- **Score Configuration**: the score bands, such as **Low**, **Medium** and **High**, that turn a score into a risk level.

Each customer's score, and how each attribute adds to it, is shown on the Customer Risk Score tab of their Customer Profile.

WHO	WHERE	CHANGES	LIMITS
Administrators and compliance heads who own the risk methodology	Fyscal ARCX → Customers → Risk Score Configuration and Score Configuration	Made in a draft, then activated; every version is kept in the history	Each value score 0 to 100; weightages 100% in total at most

AML context

A risk-based approach means knowing which customers carry more money-laundering risk and giving them more attention: closer monitoring, more frequent reviews and enhanced due diligence. The CRP records that assessment in one place and applies it the same way to every customer, so the risk rating can be explained to supervisors and auditors.

How the risk score is worked out

The configuration has three parts. Each **attribute** is a customer detail, such as **KYC Level**, **PEP Status** or **Nationality**. Each attribute has rows that give a **Score** from 0 to 100 to one or more of its values, for example **KYC 1** scores 20 and **KYC 0** scores 10. Each attribute also has a **Weightage**, the share of the total risk score it carries, in per cent.



Diagram 5.2 — From customer data to a risk level

For each attribute, the platform takes the score of the customer's value and multiplies it by the attribute's weightage. The risk score is the sum of these weighted scores:

Risk score = (score × weightage) for each attribute, added together

The score used for each attribute is the score of the row that matches the customer's value. There is no normalisation, and the scores of the rows within one attribute do not have to add up to 100: each row's score stands on its own.

Because every value score is between 0 and 100 and the weightages add up to 100% at most, the risk score is always between 0 and 100. The score bands in Score Configuration then give the risk level: with the bands of the draft shown in Set the score bands, a score below 71 is **Low**, 71 to below 80 is **Medium**, and 80 to 100 is **High**.

Worked example

These values are from the Customer Risk Score tab of the customer Emiliano Earl Gica Alvarez (Figure 5.9), scored with the active configuration in Figure 5.17.

Attribute	Weightage	Customer's value	Value score	Weighted score
KYC Level	14%	**KYC 0**	10	10 × 14% = 1.4
PEP Status	20%	none	0	0 × 20% = 0
Nationality	7%	**Philippines**	5	5 × 7% = 0.35
Country of Residence / Operation	17%	**Philippines**	5	5 × 17% = 0.85
Age	16%	**19-42**	10	10 × 16% = 1.6
ID Type	10%	**DRIVERS_LICENSE**	0 (no matching row)	0 × 10% = 0
Occupation	16%	**Homemaker**	30	30 × 16% = 4.8
Total	**100%**			**9**, band **Low**

Occupation adds the most here: 4.8 of the 9 points. If the same customer were a PEP, **PEP Status** would add 80 × 20% = 16 points and the score would be 25. Raising an attribute's weightage makes its values move the risk score more; lowering it makes them count less.

When the customer data has no value for an attribute, the Customer Risk Score tab shows *No value provided. Scored 0.* for it.

> **Not covered in this edition**
> This edition does not confirm how a customer is scored when their value matches no row of an attribute (the screen above shows *Unable to match value to any scoring row. Scored 0.*), or when a newly activated configuration is applied to existing customers' scores.

Set up the risk score attributes

Fyscal ARCX → Customers → Risk Score Configuration

Open **Risk Score Configuration** to see the attributes, scores and weightages in use. The page has two tabs: **Active Configuration**, the configuration in force, and **Configuration History**, every version saved (see Configuration history).

> **Step 1** **Start when no attributes are configured**
> Before any attribute is added, the page shows **0 Attributes** and the message *No attributes configured yet*, and **Total Weightage** is **0%**. Click **Add Attributes**, tick the attributes to score, and click **Add**. **Edit** and **Activate** stay unavailable until there is something to activate.

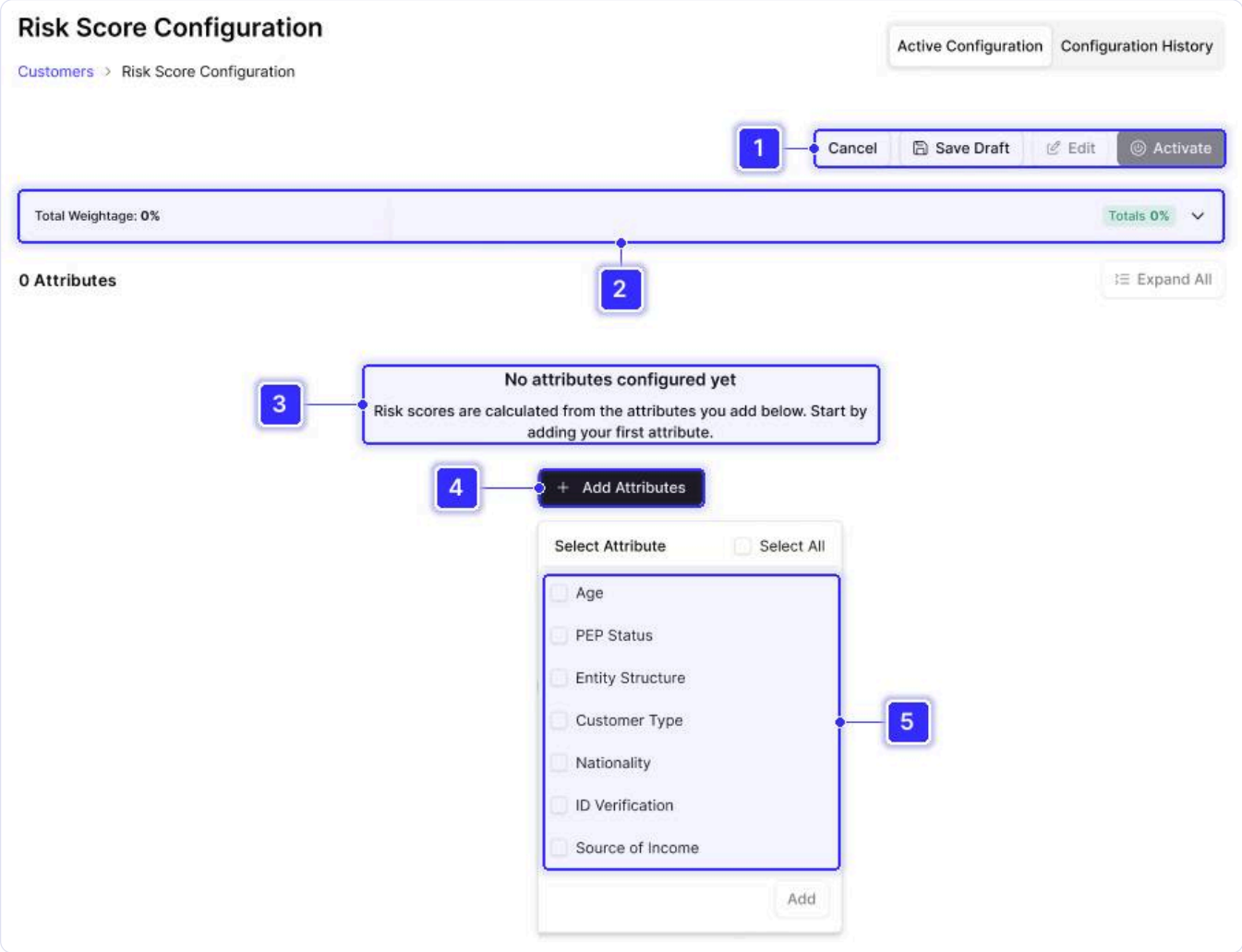


Figure 5.16 A configuration with no attributes: Cancel, Save Draft, Edit and Activate (1), Total Weightage 0% (2), the empty-state message (3), Add Attributes (4) and the list of attributes to choose from (5)

1. **Cancel**, **Save Draft**, **Edit** and **Activate**. **Edit** and **Activate** are greyed out while there is nothing to edit or activate.
2. **Total Weightage: 0%** with the **Totals 0%** tag: no weightage has been given yet.
3. *No attributes configured yet*: risk scores are calculated from the attributes you add.
4. **Add Attributes**: opens the list of customer attributes.
5. The attributes to choose from, each with a checkbox; **Select All** ticks them all.

> **Note**
> Figure 5.16 is from the product design. In the product, **Add Attribute** opens as a dialog with more attributes (see the step *Add attributes* below).

Step 2 **Read the active configuration**

When a configuration is active, the page shows who created it and when, its **Config version** and the status **ACTIVE**. The **Total Weightage** panel shows each attribute's weightage as a bar, and each attribute below lists its values and their scores.

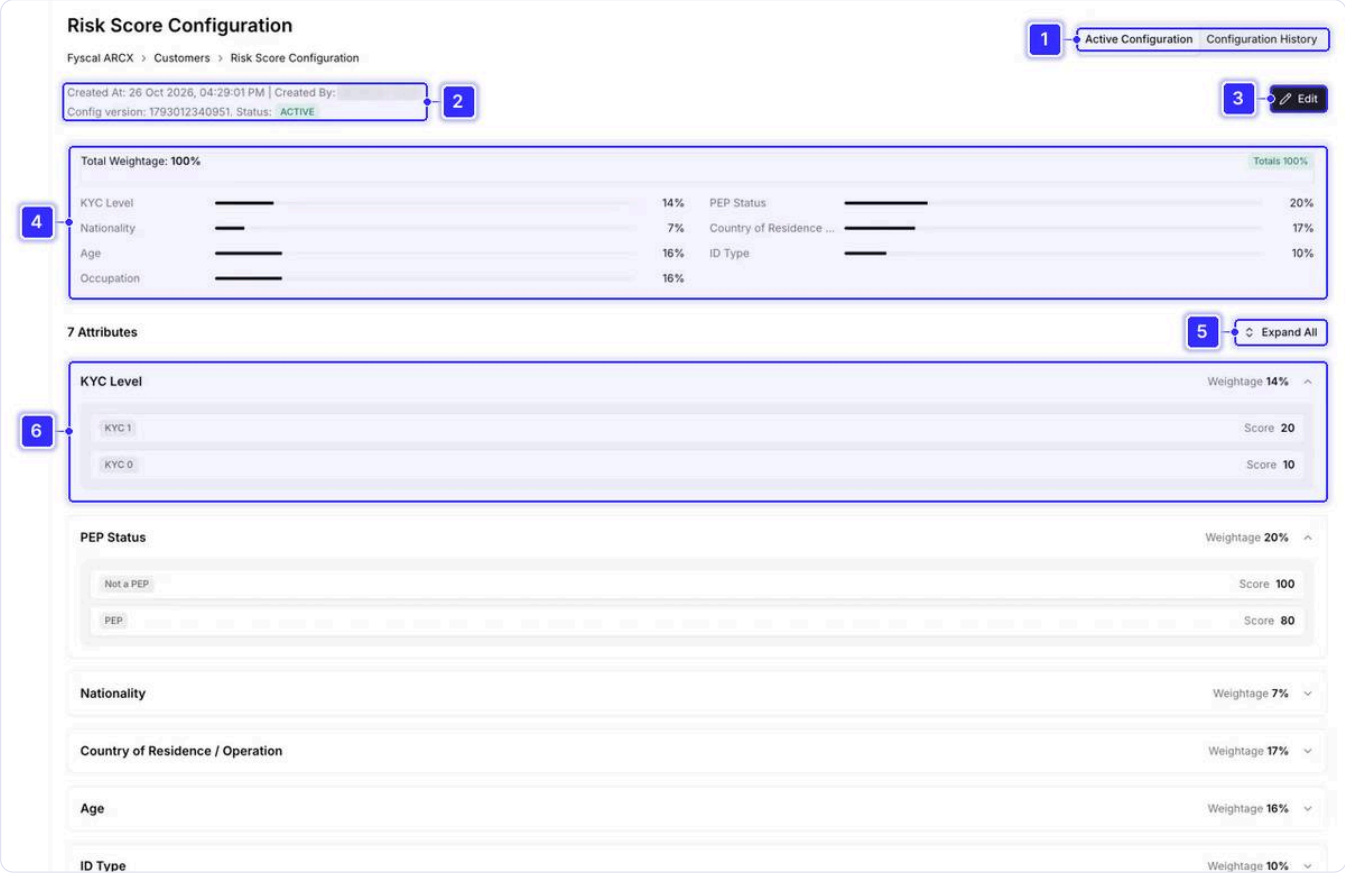


Figure 5.17 The active configuration: the tabs (1), the version details (2), Edit (3), the Total Weightage panel (4), Expand All (5) and the KYC Level attribute with its values and scores (6)

1. **Active Configuration** and **Configuration History** tabs.
2. **Created At**, **Created By**, **Config version** and **Status** (**ACTIVE**).
3. **Edit**: starts a draft of a new version.
4. **Total Weightage: 100%** with **Totals 100%**, and a bar for each attribute's weightage (here **KYC Level** 14%, **PEP Status** 20%, **Nationality** 7%, **Country of Residence / Operation** 17%, **Age** 16%, **ID Type** 10%, **Occupation** 16%).
5. **Expand All**: opens every attribute to show its values.
6. An attribute, **KYC Level**, with **Weightage 14%**: the value **KYC 1** has **Score 20** and **KYC 0** has **Score 10**.

Step 3 **Edit: work in a draft**

Click **Edit**. The page opens a draft with the status **DRAFT** and its own **Config version**; the active configuration stays in force until you activate the draft. Each attribute now has a **Weightage** box, a delete icon and an arrow that opens its values.

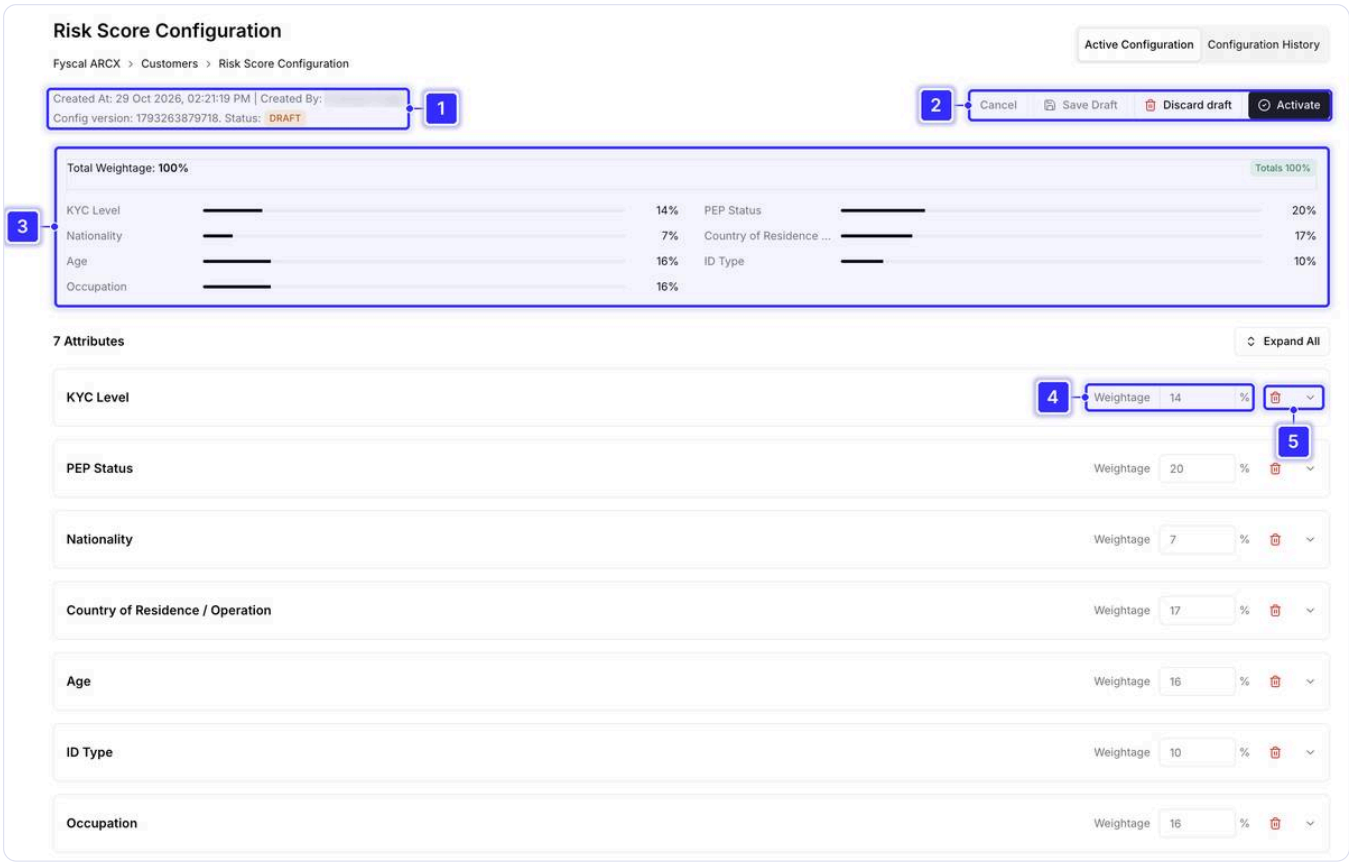


Figure 5.18 A draft: the version details with DRAFT (1), Cancel, Save Draft, Discard draft and Activate (2), the Total Weightage panel (3), the Weightage box (4), and the delete icon and arrow (5)

1. **Created At**, **Created By**, **Config version** and **Status: DRAFT**.
2. **Cancel** leaves editing; **Save Draft** saves it without activating; **Discard draft** deletes the draft; **Activate** makes the draft the active configuration.
3. **Total Weightage** and the **Totals** tag, updated as you type.
4. **Weightage** of the attribute, in per cent.
5. The delete icon removes the attribute from the draft; the arrow opens its values.

Step 4 **Add attributes**

Click **Add Attribute** below the last attribute. In the dialog, tick each customer attribute to score, or **Select All**, and click **Add**. The attributes are added to the draft, each with a weightage to fill in.

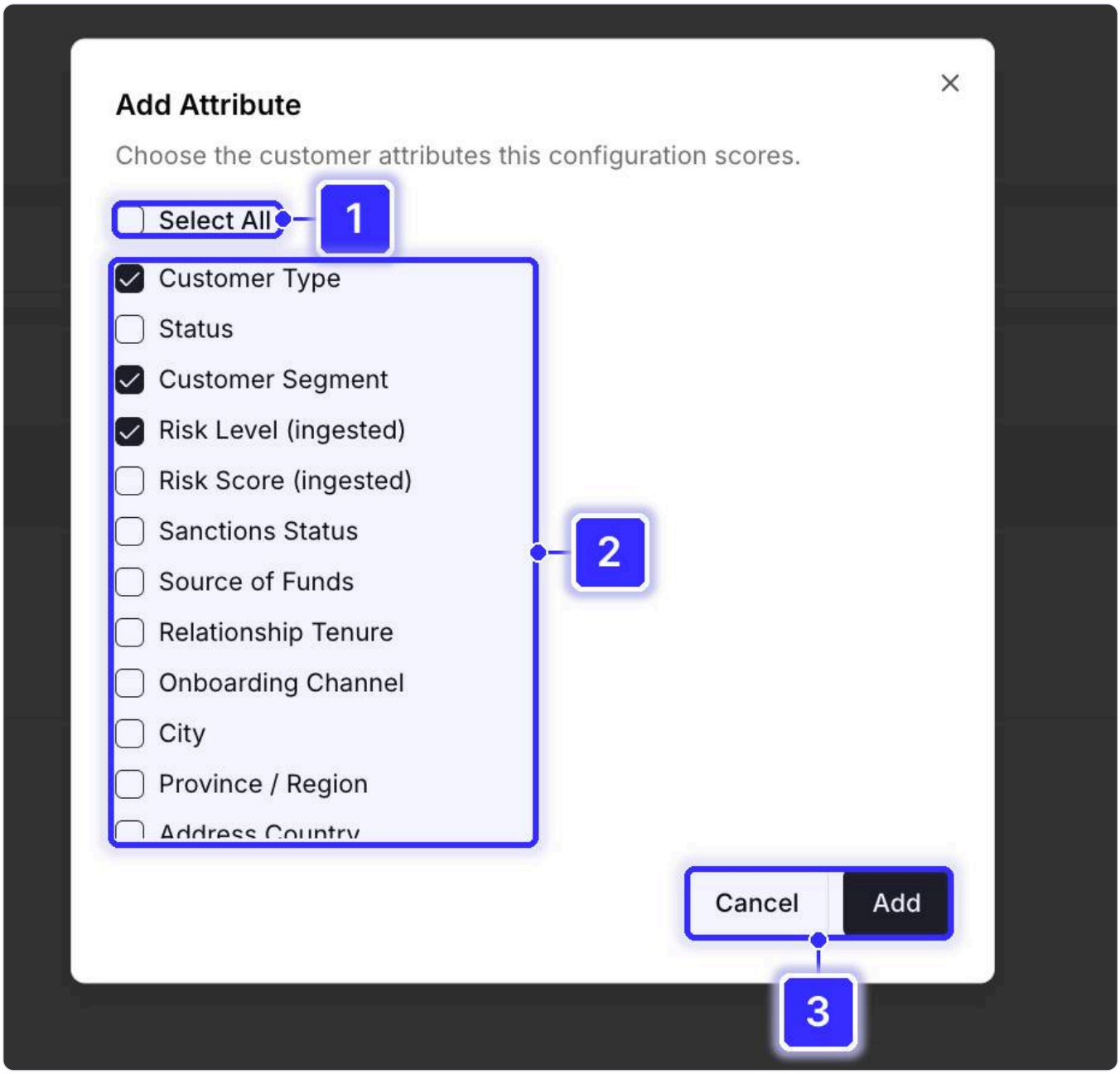


Figure 5.19 The Add Attribute dialog: Select All (1), the customer attributes with three ticked (2), and Cancel and Add (3)

1. **Select All**: ticks every attribute in the list.
2. The customer attributes, for example **Customer Type**, **Status**, **Customer Segment**, **Risk Level (ingested)**, **Risk Score (ingested)**, **Sanctions Status**, **Source of Funds**, **Relationship Tenure**, **Onboarding Channel**, **City**, **Province / Region** and **Address Country**; scroll for more.
3. **Cancel** closes the dialog; **Add** adds the ticked attributes.

Step 5 **Give each value a score**

Open an attribute with its arrow. Each row links one or more values of the attribute to a score: choose the values in the row's list (they appear as tags, such as **KYC 1**), then type the **Score**, from 0 to 100. Click **Add Row** for another value, and the delete icon at the end of a row to remove it.

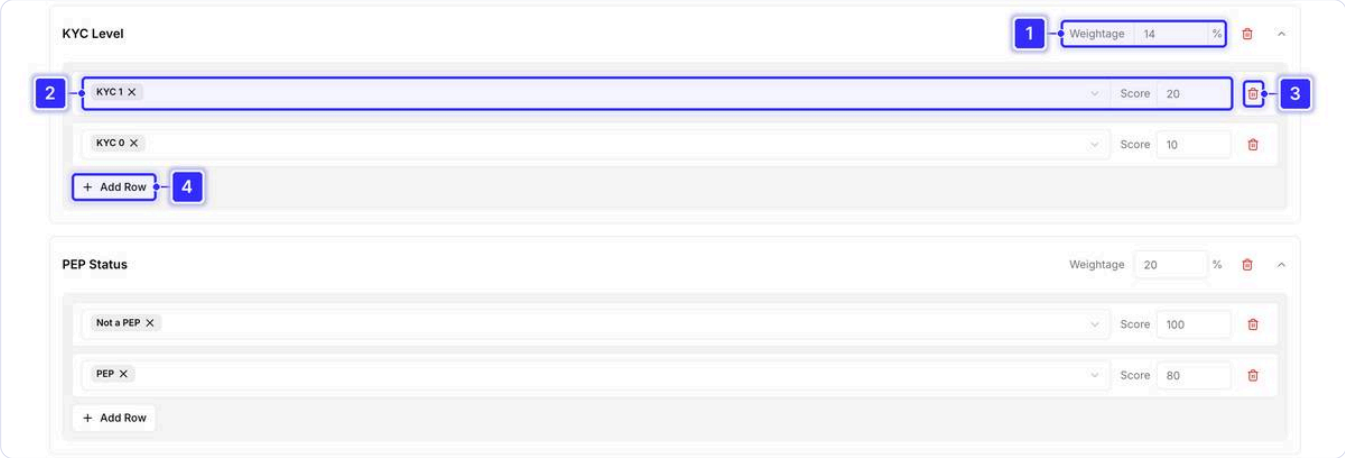


Figure 5.20 Scoring the values of KYC Level: Weightage (1), a row with its value KYC 1 and Score 20 (2), the delete icon of the row (3) and Add Row (4)

1. **Weightage** of the attribute (here 14%).
2. A row: the value or values it applies to (**KYC 1**), and its **Score** (20).
3. Deletes the row.
4. **Add Row**: adds a row for another value.

Step 6 **Set the weightages**

Type a **Weightage** for each attribute. Watch **Total Weightage** at the top: the weightages of all attributes together must not exceed 100%. When they add up to exactly 100%, the tag reads **Totals 100%** and the risk score can use the full range from 0 to 100.

Step 7 **Save or activate**

Click **Save Draft** to keep the draft and come back to it later, or **Activate** to put it in force. The activated version becomes **ACTIVE** in Configuration history, and the version that was active before becomes **INACTIVE**. To drop the draft, click **Discard draft**.

Rules the configuration follows

What	Allowed	Example
Score of a value row	A number from 0 to 100. Higher means more risk.	**PEP** → 80
Weightage of an attribute	A percentage from 0 to 100.	**PEP Status** → 20%
Total Weightage	The weightages of all attributes together: 100% at most.	14 + 20 + 7 + 17 + 16 + 10 + 16 = 100%
Risk score of a customer	Always between 0 and 100, because of the two rules above.	9 in the worked example

Important

Keep **Total Weightage** at 100%. If the weightages add up to less, no customer can reach the top of the score range; for example, with a total of 70% the highest possible risk score is 70, which is below the **High** band of the draft in Set the score bands.

Note

The scores in these screenshots are from a test configuration. For example, **Not a PEP** scores 100 and **PEP** scores 80; in a live configuration, the value with more risk normally has the higher score.

Set the score bands

Fyscal ARCX → Customers → Score Configuration

Score Configuration sets the bands that turn a risk score into a risk level. Each band has a name, a colour and a score range; together the bands cover the whole range from 0 to 100. Like the risk score configuration, the bands are changed in a draft and then activated, and every version is kept under **Score Configuration History**.



Figure 5.21 A draft of the score bands: the tabs (1), the draft details (2), Cancel, Save Draft, Discard draft and Activate (3), the name and colour of the Low band (4), its Min score and Max score (5), the delete icon (6) and Add band (7)

1. **Active Score Configuration** and **Score Configuration History** tabs.
2. **Draft Score Configuration**: **Created At**, **Created By**, **Config version** and **Status: DRAFT**.
3. **Cancel**, **Save Draft**, **Discard draft** and **Activate**, as for the risk score configuration.
4. **Name** (**Low**) and **Color** (**#15803D**, green) of the band.
5. **Min score** and **Max score**. The band includes its minimum and goes up to, but not including, its maximum (**< 71**). **Min score** cannot be edited: it follows the previous band's **Max score**.
6. Deletes the band.
7. **Add band**: adds a band.

The bands of the draft in Figure 5.21, which is not the active configuration:

Band	Color	Scores
Low	**#15803D** (green)	0 to below 71
Medium	**#d9c708** (yellow)	71 to below 80
High	**#e90c0c** (red)	80 to 100

Step 1 **Change the bands**

Open the draft and edit a band's **Name**, **Color** or **Max score**. You only type the maximum. **Min score** cannot be edited: each band's **Min score** follows the previous band's **Max score** automatically (here **Medium** starts at 71 because **Low** ends below 71). The first band starts at 0 and the last band ends at **≤ 100**.

Step 2 **Add or remove a band**

Click **Add band** to add a band, or the delete icon to remove one. Check that the bands still run from 0 to 100 without a gap.

Step 3 **Activate**

Click **Activate** to put the bands in force, or **Save Draft** to finish later.

Note

The **Risk Level** and **Score** columns of the customer list, and the **Risk Tier** filter, show risk levels such as **Low**, **Medium** and **High**. Figure 5.21 shows a draft, with bands at 71 and 80, not the active score configuration. That is why its bands do not match the scores in the customer list, for example **High 62.61%**.

Configuration history

Fyscal ARCX → Customers → Risk Score Configuration → Configuration History

Every version of the risk score configuration is kept. Open the **Configuration History** tab to see which version is in force, who created each version and when. Score Configuration has the same list under **Score Configuration History**.

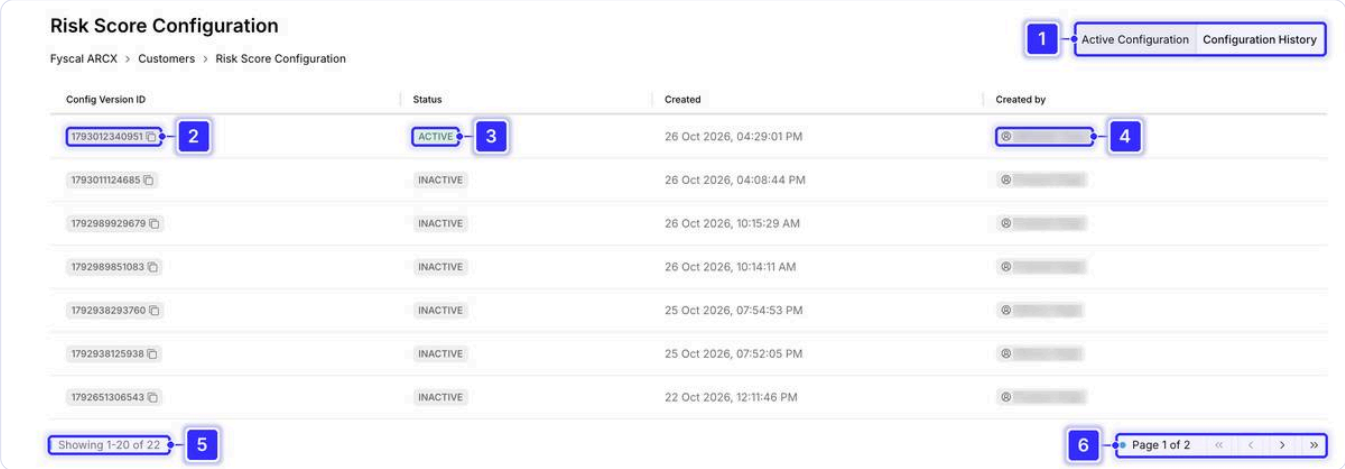


Figure 5.22 Configuration History: the tabs (1), a Config Version ID with its copy icon (2), the status ACTIVE (3), Created by (4), the count line (5) and the page controls (6)

1. **Active Configuration** and **Configuration History** tabs.
2. **Config Version ID**, with a copy icon.
3. **Status**: **ACTIVE** for the version in force, **INACTIVE** for earlier versions, and **DRAFT** for a draft not yet activated.
4. **Created by**: the user who created the version.
5. **Showing 1-20 of 22**: 20 versions per page.
6. **Page 1 of 2** and the first, previous, next and last page buttons.

Status	Meaning
ACTIVE	The version in force. Only one version is active at a time.
DRAFT	Saved with **Save Draft** and not yet activated.
INACTIVE	An earlier version, replaced when a newer one was activated.

Use the history to answer an auditor's question about which risk methodology applied on a given date: find the version that was **ACTIVE** at that time, by its **Created** date and the date of the next activation.

RELATED IN CORE WORKFLOW

Case Manager | Case Manager Configuration | Regulatory Reports

CORE WORKFLOW

6 Regulatory Reports

Fyscal ARCX → Regulatory Reports

Regulatory Reports holds the reports the institution files with the AMLC. It has two tabs, switched at the top right of the page. **STR** is the register of Suspicious Transaction Reports (STRs) filed on the platform, one row per STR: find a filed STR, download its CSV, and open it to read what was reported in each of its six steps. STRs are filed from a case in Case Manager, not from this page. **CTR** lists the Covered Transaction Reports (CTRs) that the platform creates by itself once a day from ingested transactions, each with a CSV file in the GoTRACS format (see The CTR register).

FOR	IN THE MENU	READING TIME
Analysts, supervisors and team leads	Fyscal ARCX → Regulatory Reports	About 19 min

The STR register: read the list of filed STRs and its columns.

Search and filter the register: find an STR by case or STR ID, filter by date or creator, and download its CSV.

Open a filed STR: open an STR read-only and move between its steps.

Step 1: Select Alerts: see which of the case's alerts the STR covers.

Step 2: Report Type: check the STR type, filing details and filing deadline.

Step 3: Reason for suspicion: see the reason codes the STR cites.

Step 4: Transaction: see the transactions included and their total amount.

Step 5: Subject parties: check the parties named in the STR and their details.

Step 6: Narratives: read the STR narrative and the alerts it covers.

Where STRs come from: find out where STRs are filed and where else they appear.

The CTR register: read the list of CTRs and its columns.

How CTRs are generated: see when CTRs are created, the ₱500,000 threshold and the filing deadline.

Find and download a CTR: find a CTR, download its CSV and file it with the AMLC.

CONCEPT DIAGRAM

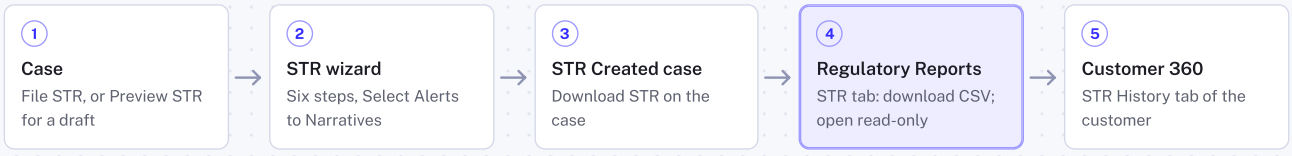


Diagram 6.1 — Where an STR is filed and where it appears afterwards

An STR is prepared from a case in Case Manager with the six-step STR wizard. A filed STR appears as a row on the **STR** tab. In the examples, the case then shows the status **STR Created** with **Download STR**, and STRs are also listed on the STR History tab of a customer in Customer 360. The field-by-field reference for the six steps is in Case Manager (Step 1 to Step 6); this chapter shows what a filed STR looks like, using STR 694.

AML context

Institutions keep a record of every STR they file, with the evidence behind it, so that they can answer follow-up requests from the financial intelligence unit and show supervisors and auditors what was reported and when. The register is that record on the platform.

The STR register

Fyscal ARCX → Regulatory Reports → STR

Use the register to see the filed STRs and pick the one you need. **Regulatory Reports** opens on the **STR** tab, which shows the filed STRs, newest first, with a search box, a **Refresh** button and a **Show Filters** button above the table. Use the **STR** / **CTR** switch at the top right to change tab.

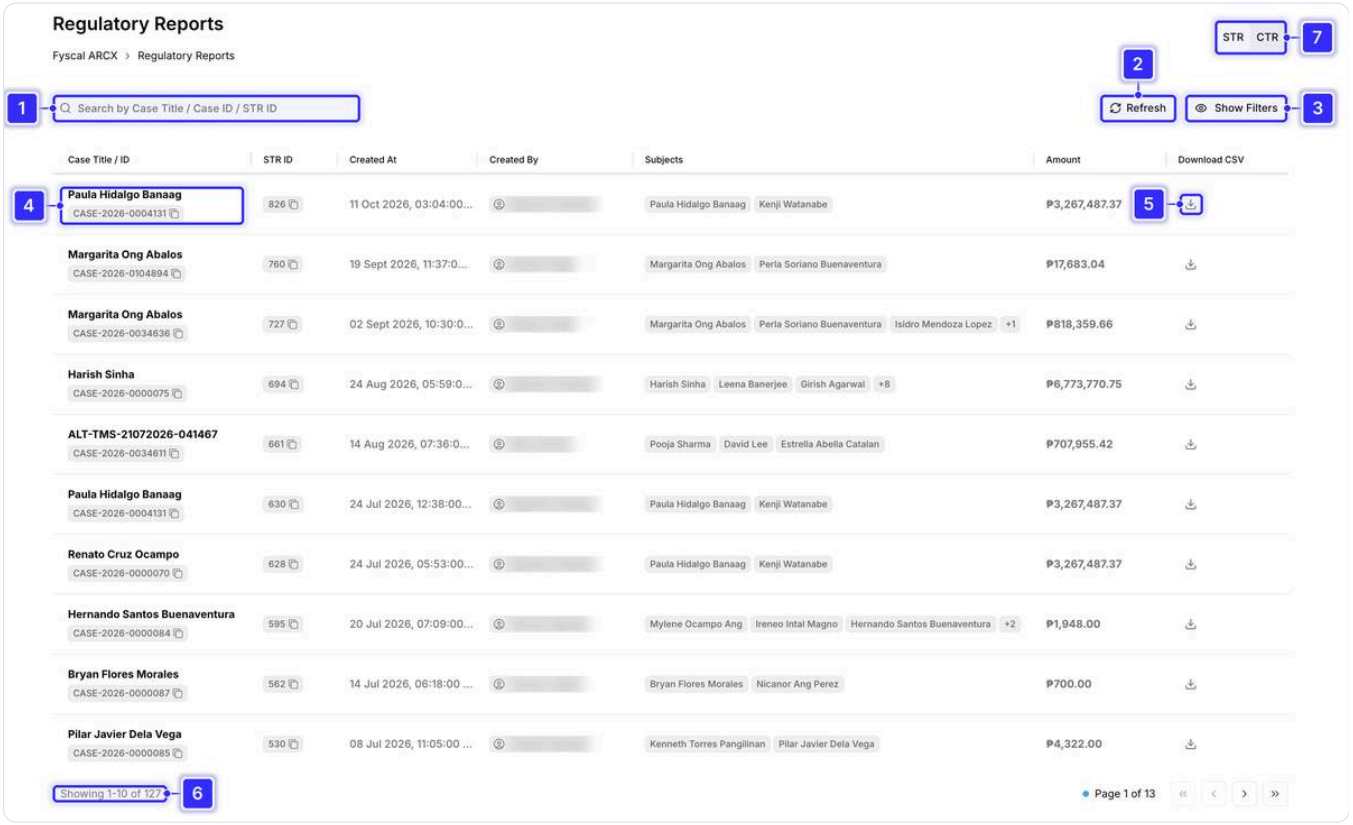


Figure 6.1 The STR tab of Regulatory Reports: search (1), Refresh (2), Show Filters (3), an STR row (4), Download CSV (5), the count line (6) and the STR / CTR switch (7); user names are blurred

1. **Search by Case Title / Case ID / STR ID**: finds STRs by the case title, the case ID or the STR ID.
2. **Refresh**: reloads the register.
3. **Show Filters**: opens the filters **Creation Period** and **Created By**. The button then reads **Hide Filters**.
4. An STR row. Click a row to open that STR (see Open a filed STR).
5. **Download CSV**: the download icon on each row downloads a CSV file for that STR.
6. The count line (**Showing 1-10 of 127**) and, at the right, **Page 1 of 13** with first, previous, next and last page buttons. The register shows 10 STRs per page.
7. **STR** / **CTR**: switches between the STR register and the CTR register. The selected tab is highlighted.

Column	What it shows	Example
Case Title / ID	The title of the case the STR was filed from, with the case ID and a copy icon below it. The case title is often the customer's name; it can also be an alert ID.	Harish Sinha, CASE-2026-0000075; ALT-TMS-21072026-041467, CASE-2026-0034611
STR ID	The STR's ID number, with a copy icon.	694
Created At	Date and time the STR was created.	24 Aug 2026, 05:59:00 PM
Created By	The user who created the STR.	(hidden in the figures)
Subjects	The parties named in the STR, as name tags. When there are more than fit, a ***+n*** tag shows how many more.	Harish Sinha, Leena Banerjee, Girish Agarwal, +8
Amount	The amount shown for the STR, in Philippine pesos.	₱6,773,770.75
Download CSV	A download icon for the STR's CSV file.	download icon

Search and filter the register

Fyscal ARCX → Regulatory Reports → STR → Show Filters

Use the search box when you know the case title, case ID or STR ID, and the filters to narrow the register by creation date or by the user who created the STR.

Filter	Default	Options or format
Creation Period	**Pick a date range**	A two-month calendar (for example October 2026 and November 2026) with arrows to move between months. Today's date is highlighted.
Created By	**All Assignees**	A list of users. Your own entry is marked **(You)**; in testing it was the only entry.

Step 1 **Search for an STR**

Click the **Search by Case Title / Case ID / STR ID** box and type a case title (for example **Harish Sinha**), a case ID (for example **CASE-2026-0000075**) or an STR ID (for example **694**).

Step 2 **Open the filters**

Click **Show Filters**. The **Creation Period** (1) and **Created By** (2) filters appear below the search box, and the button reads **Hide Filters** (3). Click **Hide Filters** to close them.



Figure 6.2 The STR tab filters: Creation Period (1) and Created By (2), with Hide Filters (3)

Step 3 **Filter by the user who created the STR**

Click the **Created By** box (1) (it shows **All Assignees**) and click a user in the list (2). In testing, the list showed one entry, the signed-in user, marked **(You)**.

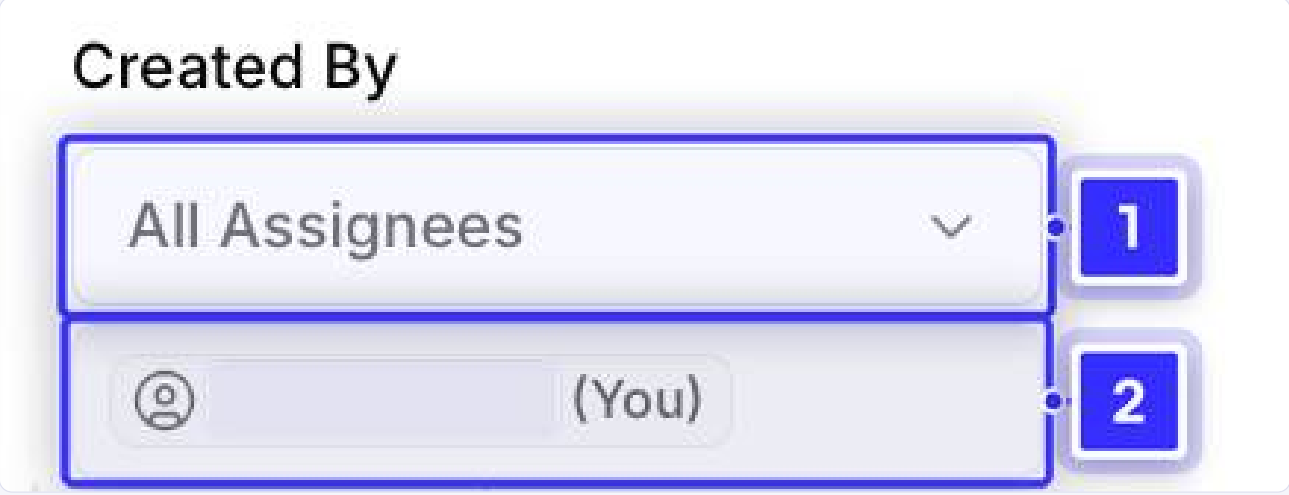


Figure 6.3 The Created By filter (1) open, with one entry marked (You) (2); the user name is hidden

Step 4 **Filter by creation date**

Click the **Creation Period** box (it shows **Pick a date range**). A two-month calendar opens. Pick the start and end dates of the range. Use the arrows (1, 2) beside the month names to change month. Today's date is highlighted (3).

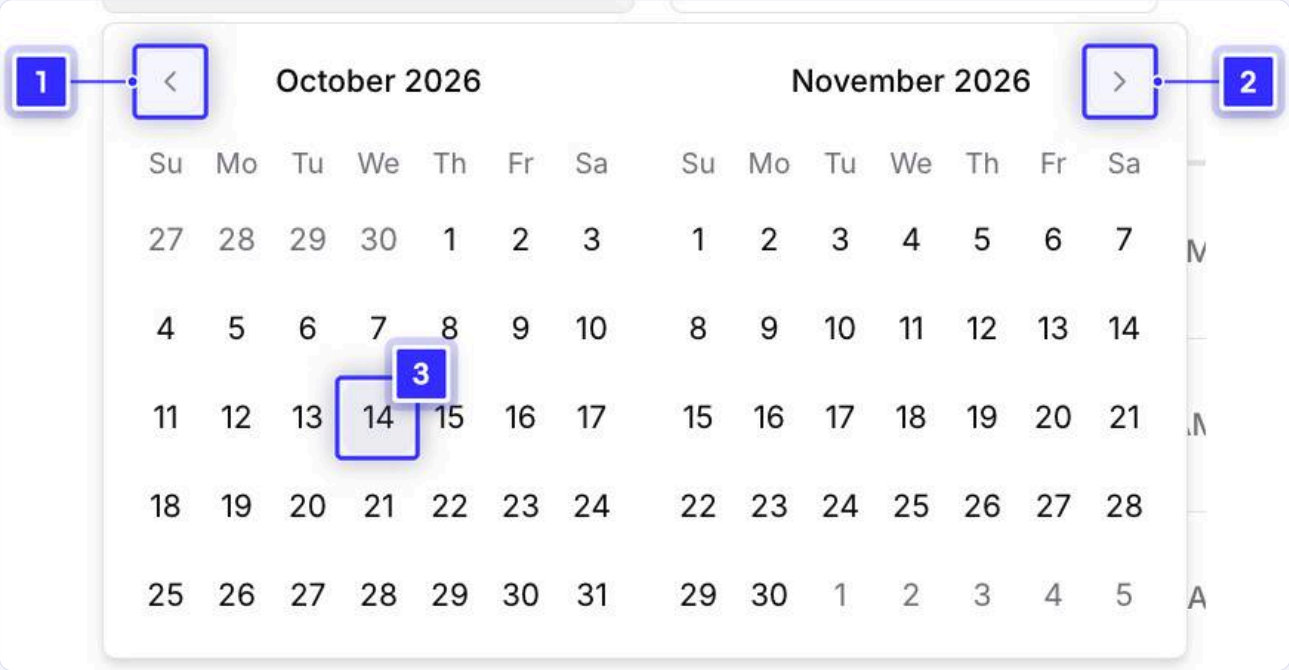


Figure 6.4 The Creation Period calendar, October and November 2026: previous month (1), next month (2) and today's date highlighted (3)

Step 5 **Download an STR's CSV**

In the row of the STR, click the download icon in the **Download CSV** column (5 in Figure 6.1).

Open a filed STR

Fyscal ARCX → Regulatory Reports → STR → *STR row*

WHERE	MODE	STEPS	FIELD REFERENCE
Regulatory Reports → STR → click a row	Read-only: no save or submit button	The same six steps as the STR wizard	File an STR in Case Manager

Open a filed STR to read exactly what was reported, step by step. Click an STR row to open it. The STR opens in a dialog over the page, titled **Suspicious Transaction Report (STR)**, with the subtitle **GoTRACS-compliant STR filing for AMLC** and the case ID. The dialog has six steps, the same steps used to file an STR from a case: **Select Alerts**, **Report Type**, **Reason for suspicion**, **Transaction**, **Subject parties** and **Narratives**. A filed STR opens read-only: its values are shown in greyed fields and ticked or unticked boxes, and there is no save or submit button. Behind the dialog, the sidebar is shown collapsed to a narrow strip of icons.

The figures below show STR **694**, filed from case **CASE-2026-0000075** (Harish Sinha).

Control	What it does
Step bar	Shows the six steps. The current step has a blue number; steps already passed show a green tick.
Next Step	Moves to the next step. Not shown on step 6.
Previous Step	Moves back one step. Not shown on step 1.
× (top right)	Closes the dialog.

Step 1: Select Alerts

This step shows which of the case's alerts the STR covers. It lists the case's alerts under the heading **Alerts to include in STR**, with the instruction **Transactions and parties from selected alerts appear in subsequent steps.** A ticked box marks each alert included in the STR.

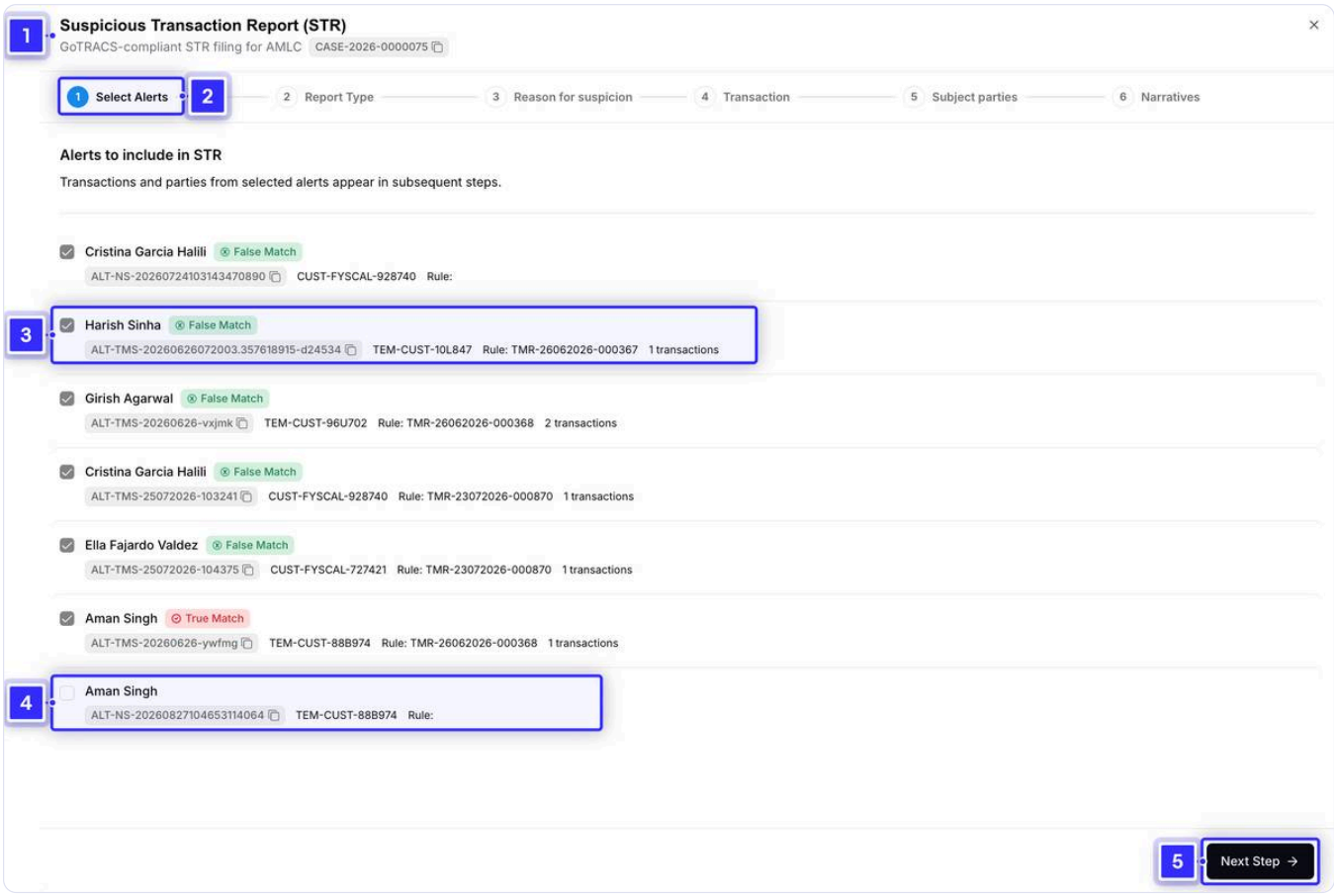


Figure 6.5 Step 1, Select Alerts, for STR 694: the title and case ID (1), the current step (2), an included alert (3), the one alert not included (4) and Next Step (5)

1. Dialog title, subtitle and case ID (**CASE-2026-0000075**).
2. Step bar, with **Select Alerts** as the current step.
3. An included alert: a ticked box, the customer name and the alert's disposition (here **Harish Sinha**, **False Match**), then the alert ID, the customer ID, the rule and, for transaction-monitoring alerts, the number of transactions.
4. The alert that is not included: its box is unticked (**ALT-NS-20260827104653114064**, Aman Singh, in the example).
5. **Next Step**.

Each alert shows the customer name, the alert's disposition (for example **False Match** or **True Match**; none when the alert has no disposition), its alert ID (for example **ALT-TMS-20260626072003.357618915-d24534**), the customer ID (for example **TEM-CUST-10L847**), the rule (for example **Rule: TMR-26062026-000367**) and, for transaction-monitoring alerts, the number of transactions (for example **1 transactions**). Name-screening alerts (IDs starting ALT-NS) show **Rule:** with no value.

Step 2: Report Type

This step shows the type of report and its filing details, including the date of determination from which the filing deadline is worked out.

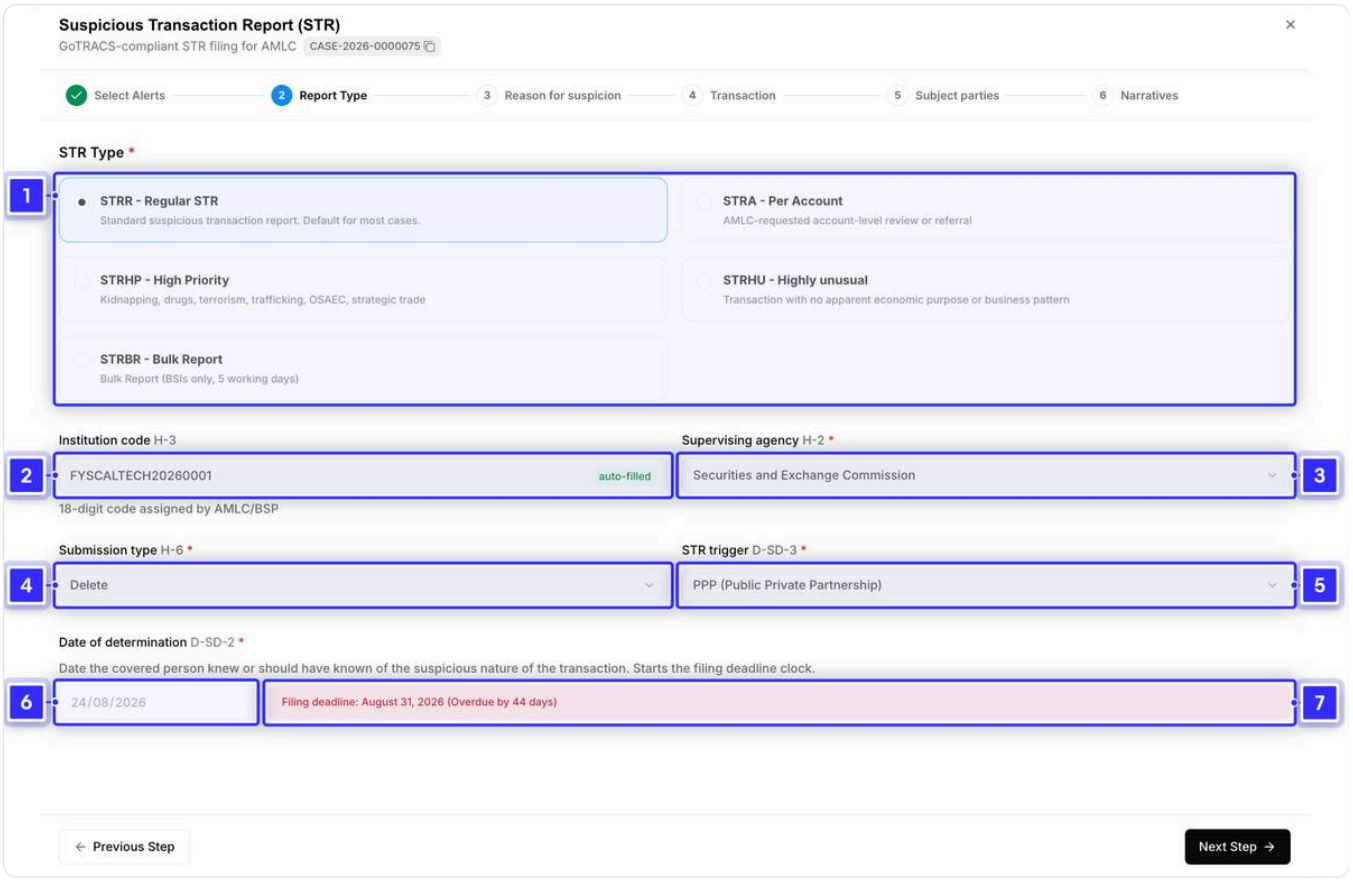


Figure 6.6 Step 2, Report Type: STR Type (1), Institution code (2), Supervising agency (3), Submission type (4), STR trigger (5), Date of determination (6) and the Filing deadline message (7)

#	Field	Value in STR 694
1	**STR Type**	STRR - Regular STR
2	**Institution code** H-3	FYSCALTECH20260001 (marked **auto-filled**)
3	**Supervising agency** H-2	Securities and Exchange Commission
4	**Submission type** H-6	Delete
5	**STR trigger** D-SD-3	PPP (Public Private Partnership)
6	**Date of determination** D-SD-2	24/08/2026
7	Filing deadline message	Filing deadline: August 31, 2026 (Overdue by 44 days)

For each field's options, required marker and help text, see Step 2: Report Type in Case Manager. The five STR types are compared in STR types compared.

Next to the date, a message shows the filing deadline worked out from it: in the example, **Filing deadline: August 31, 2026 (Overdue by 44 days)** on 14 October 2026, in red (7 in the figure). The number of days overdue grows each day. The codes after each label (H-3, D-SD-2 and so on) are the field codes shown on screen for the AMLC GoTRACS report.

Step 3: Reason for suspicion

This step shows the reason codes the STR cites, as primary codes and as additional codes.

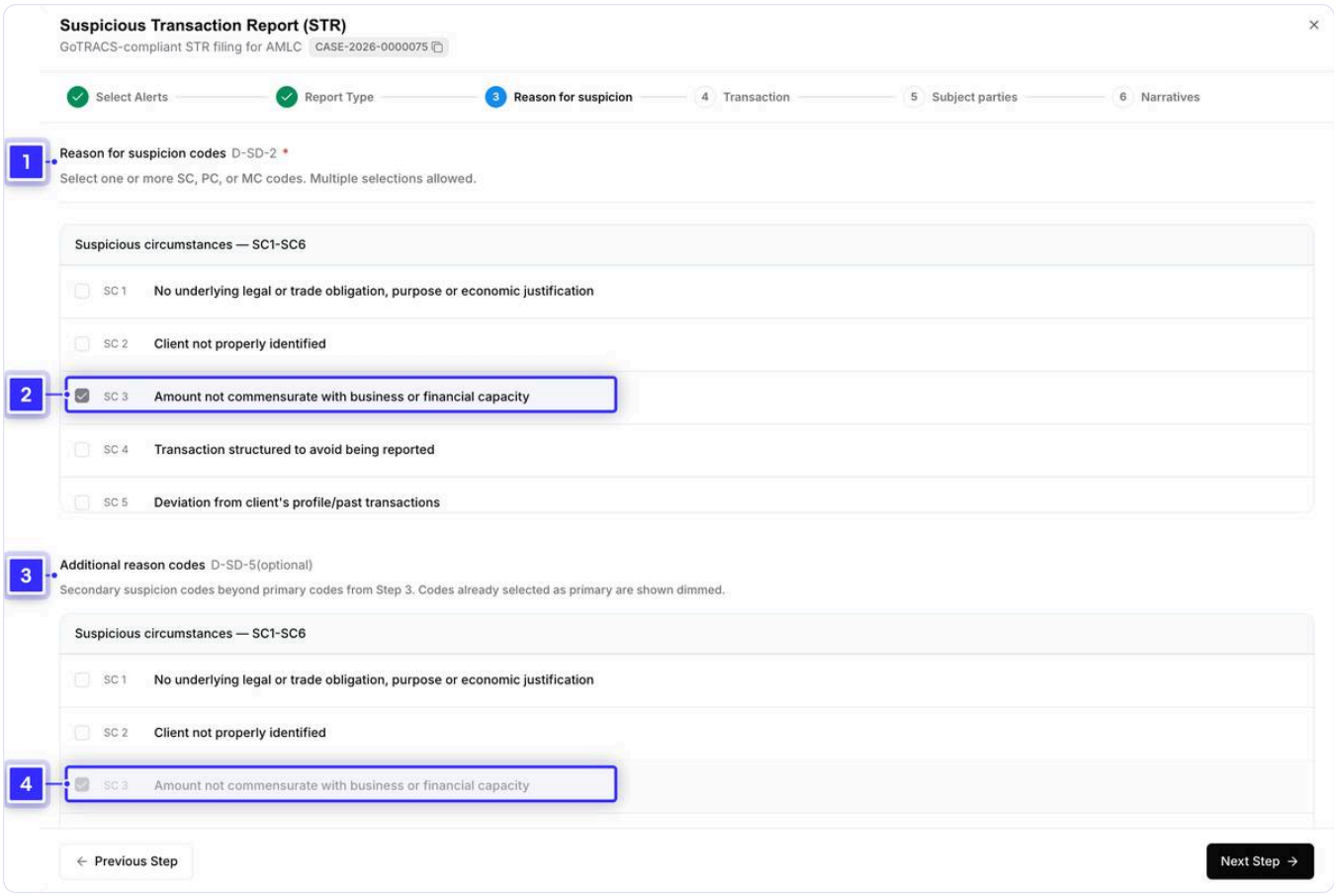


Figure 6.7 Step 3, Reason for suspicion: the reason codes (1) with SC 3 ticked (2), and Additional reason codes (3) with SC 3 shown dimmed (4)

1. **Reason for suspicion codes** D-SD-2 (required, *): "Select one or more SC, PC, or MC codes. Multiple selections allowed."
2. In STR 694, **SC 3** is ticked.
3. **Additional reason codes** D-SD-5 (optional): "Secondary suspicion codes beyond primary codes from Step 3. Codes already selected as primary are shown dimmed." The same code lists repeat here.
4. SC 3 is shown dimmed in the additional list.

A filed STR shows no selection counter on this step.

Each section has three groups, which scroll inside the dialog: **Suspicious circumstances — SC1-SC6**, **Predicate crimes — PC1-PC36** and **Transnational organized crime — MC1**.

The description of every code, and which predicate-crime codes carry a **KYC REQ** tag, is listed once in Step 3: Reason for suspicion in Case Manager.

Step 4: Transaction

This step shows which of the case's transactions are included in the STR, their total amount, and the role of each party in them.

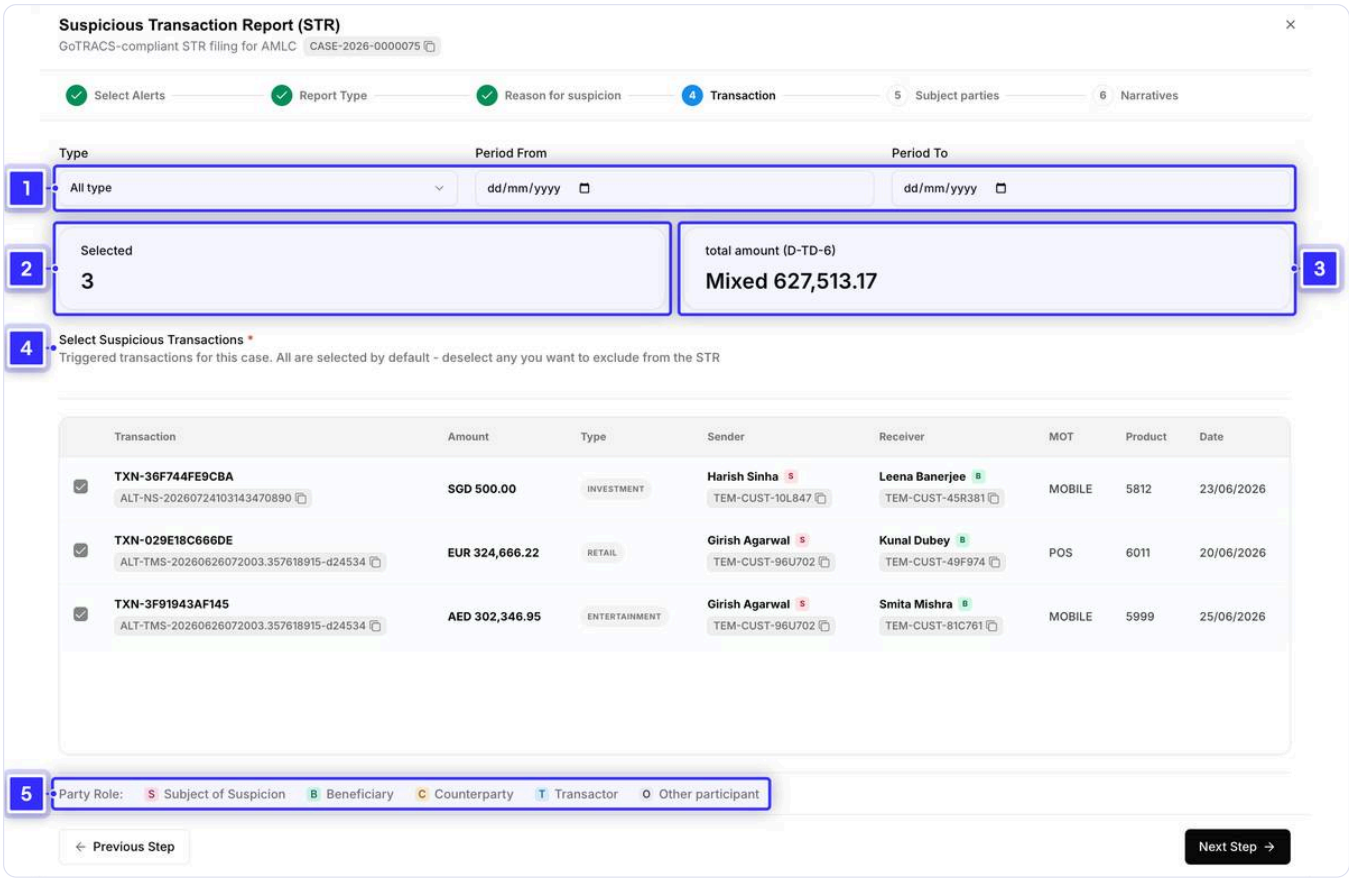


Figure 6.8 Step 4, Transaction: filters (1), Selected 3 (2), total amount Mixed 627,513.17 (3), Select Suspicious Transactions (4) and the Party Role legend (5)

1. Filters: **Type** (**All type**), **Period From** and **Period To** (dd/mm/yyyy).
2. **Selected**: the number of transactions included (3).
3. **total amount (D-TD-6)**: the total of the included transactions. When they are in different currencies it is labelled **Mixed** (here **Mixed 627,513.17**).
4. **Select Suspicious Transactions** (required, *): "Triggered transactions for this case. All are selected by default - deselect any you want to exclude from the STR".
5. **Party Role** legend.

Column	What it shows	Example
(check box)	Ticked when the transaction is included.	ticked
Transaction	Transaction ID, with the alert ID below it.	TXN-029E18C666DE, ALT-TMS-20260626072003.357618915-d24534
Amount	Amount and currency.	SGD 500.00; EUR 324,666.22; AED 302,346.95
Type	Transaction type.	INVESTMENT, RETAIL, ENTERTAINMENT
Sender	Sender name, party-role letter and customer ID.	Girish Agarwal, S, TEM-CUST-96U702
Receiver	Receiver name, party-role letter and customer ID.	Kunal Dubey, B, TEM-CUST-49F974
MOT	Mode of transaction.	MOBILE, POS
Product	Product code, or - when none.	5812, 6011, 5999
Date	Transaction date (dd/mm/yyyy).	20/06/2026

The party-role letters next to each sender and receiver (**S**, **B**, **C**, **T**, **O**) are explained in the **Party Role** table in Step 4: Transaction.

The note below the legend reads: "MOT, Product Type, Purpose of Remittance, and Transaction Code are sourced from ingested data and included automatically in the Format X CSV per selected transaction. Total amount can be manually overridden below."

Step 5: Subject parties

This step shows the parties named in the STR and their identity details. It lists the parties under the heading **Subject parties**: "Auto-derived from selected transactions. Click a row to expand and edit." Each party row shows a tag (**AH**), the name in the form *Last, First* (or *Last, First, Middle*) and the customer ID. Click a row to expand it.

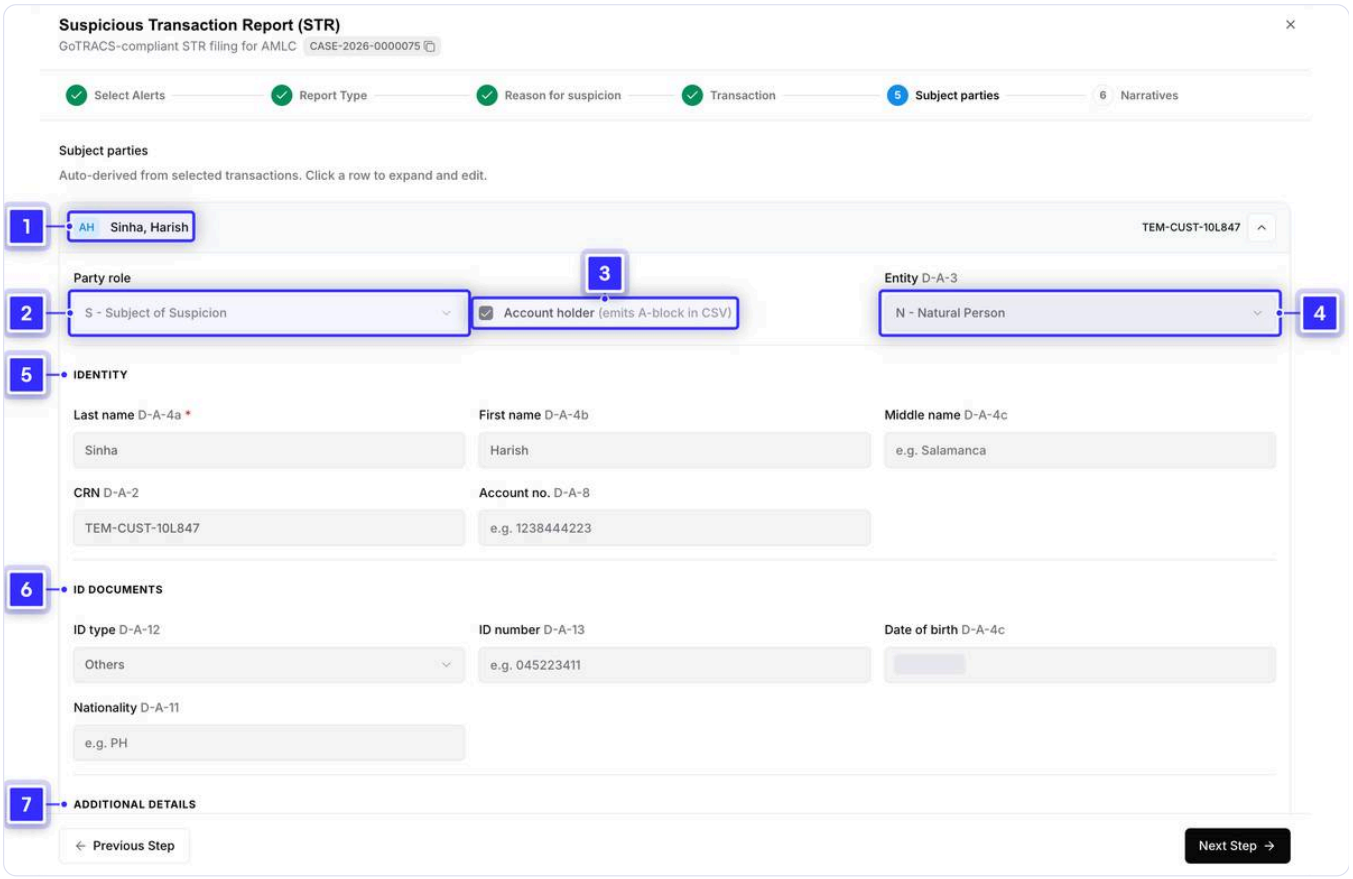


Figure 6.9 Step 5, Subject parties: Sinha, Harish expanded (1), Party role (2), Account holder (3), Entity (4), IDENTITY (5), ID DOCUMENTS (6) and ADDITIONAL DETAILS (7)

1. The party row: **Sinha, Harish**. The arrow at the right collapses the row.
2. **Party role**: **S - Subject of Suspicion**.
3. **Account holder** check box, labelled "(emits A-block in CSV)": ticked.
4. **Entity** D-A-3: **N - Natural Person**.
5. **IDENTITY** fields.
6. **ID DOCUMENTS** fields.
7. **ADDITIONAL DETAILS** fields, below the visible area (scroll the dialog).

Group	Field (code)	Value or placeholder in STR 694
IDENTITY	**Last name** D-A-4a	Sinha
IDENTITY	**First name** D-A-4b	Harish
IDENTITY	**Middle name** D-A-4c	empty (placeholder "e.g. Salamanca")
IDENTITY	**CRN** D-A-2	TEM-CUST-10L847
IDENTITY	**Account no.** D-A-8	empty (placeholder "e.g. 1238444223")
ID DOCUMENTS	**ID type** D-A-12	Others (drop-down)
ID DOCUMENTS	**ID number** D-A-13	empty (placeholder "e.g. 045223411")
ID DOCUMENTS	**Date of birth** D-A-4c	a date (hidden in the figure)
ID DOCUMENTS	**Nationality** D-A-11	empty (placeholder "e.g. PH")

Group	Field (code)	Value or placeholder in STR 694
ADDITIONAL DETAILS	**Complete address** D-A-5	not visible in the capture
ADDITIONAL DETAILS	**Country code** D-A-6	PH - Philippines
ADDITIONAL DETAILS	**ID City code — PSGC** D-A-7	not visible in the capture
ADDITIONAL DETAILS	**Place of birth** D-A-10	not visible in the capture
ADDITIONAL DETAILS	**Source of fund** D-A-6	Employed
ADDITIONAL DETAILS	**Contact no.** D-A-15	not visible in the capture
ADDITIONAL DETAILS	**Old account no.** D-A-16	not visible in the capture

For each field's required marker and placeholder, see Step 5: Subject parties in Case Manager.

STR 694 lists 11 parties: Sinha, Harish; Banerjee, Leena; Agarwal, Girish; Dubey, Kunal; Mishra, Smita; Villacorta, Rodolfo, Aguilar; Halili, Cristina, Garcia; Domingo, Benedict, Abella; Valdez, Ella, Fajardo; Singh, Aman; Joshi, Neha. These are the parties behind the **+8** tag in the register's **Subjects** column (three names shown plus eight more).

Step 6: Narratives

This last step shows the written narrative of the STR and the alerts it covers.

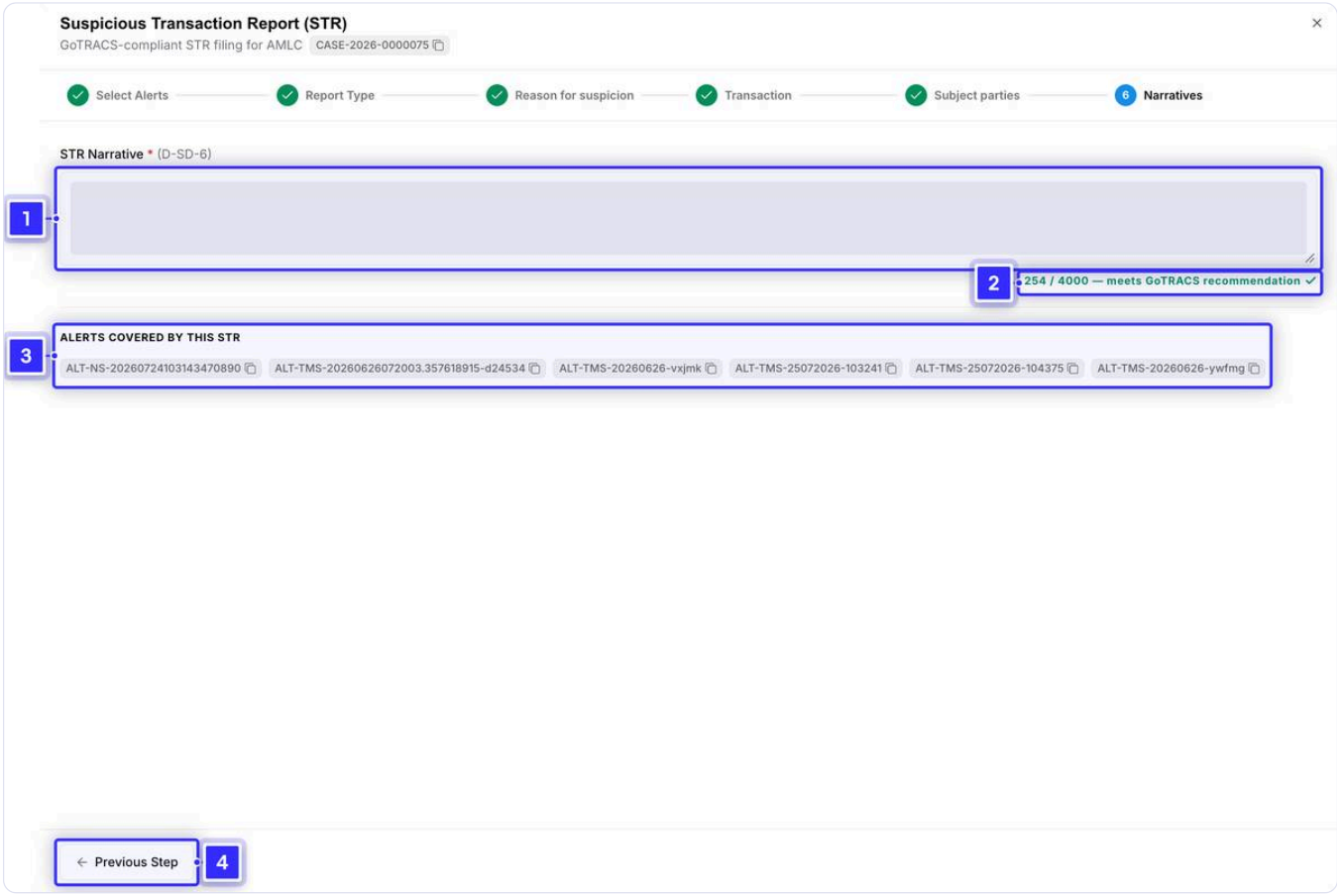


Figure 6.10 Step 6, Narratives: the STR Narrative, text hidden (1), its character counter (2), the alerts covered by the STR (3) and Previous Step (4)

1. **STR Narrative** (D-SD-6, required, *): the written narrative of the STR, in a text box.
2. Character counter: in the example **254 / 4000 — meets GoTRACS recommendation**, in green with a tick. The maximum shown is 4000 characters.
3. **ALERTS COVERED BY THIS STR**: the IDs of the alerts included in step 1, each with a copy icon. STR 694 covers six alerts.
4. **Previous Step**. This is the last step, so there is no **Next Step** button.

Close the dialog with the × at its top right to return to the register.

Where STRs come from

Read this if you want to file a new STR. The **STR** tab has no button to create an STR. An STR is filed from a case in Case Manager, using the same six steps shown above; see that chapter for how to file one, and Diagram 6.1 at the top of this chapter for the path an STR takes. A case whose STR has been filed shows the status **STR Created**, as in Figure 5.12. To see the STRs linked to one customer, open the customer's STR History tab in Customer 360.

The CTR register

Fyscal ARCX → Regulatory Reports → CTR

A Covered Transaction Report (CTR) tells the AMLC about a covered transaction. In general, that is a transaction of more than ₱500,000 (see How CTRs are generated). Fyscal ARCX creates CTRs by itself from the transactions it ingests; nobody types in filing data. Use the **CTR** tab to find a CTR, check its filing deadline and download its CSV for filing.

Click **CTR** in the switch at the top right of **Regulatory Reports**. The tab shows the CTRs, newest first.

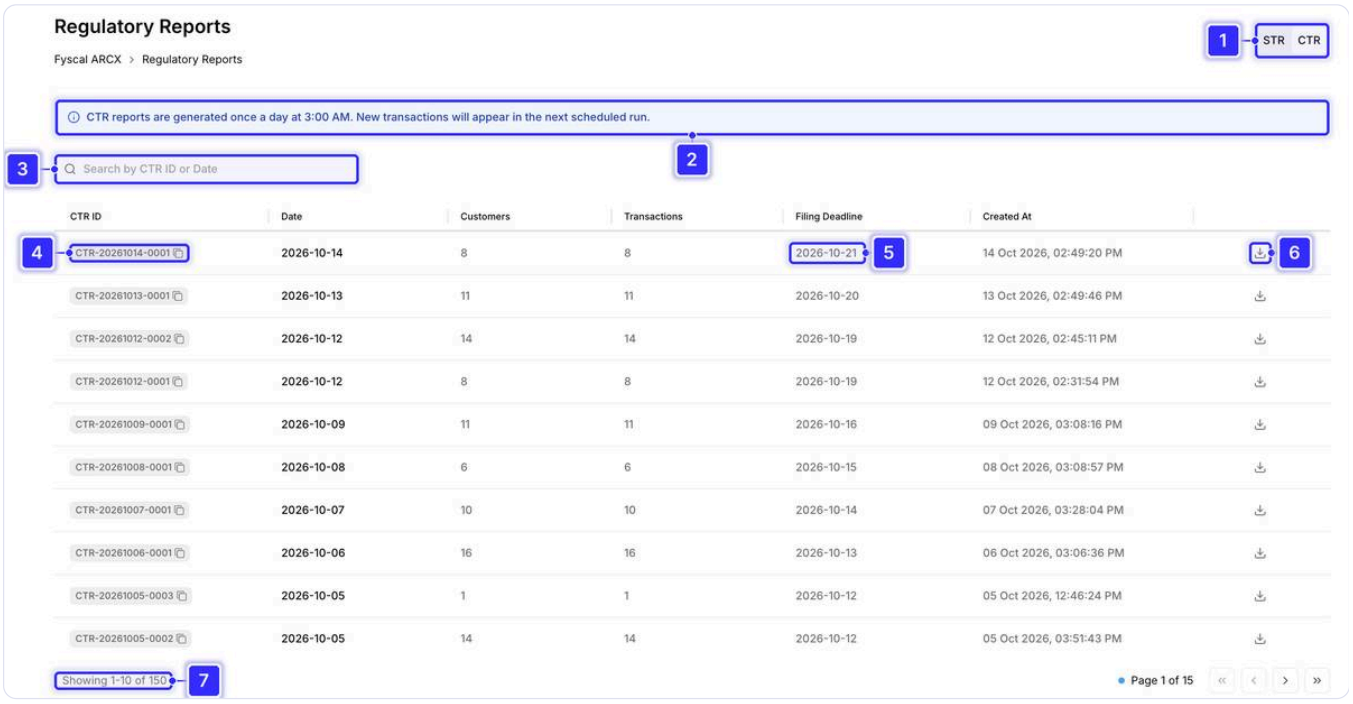


Figure 6.11 The CTR tab of Regulatory Reports: the STR / CTR switch (1), the schedule message (2), search (3), a CTR ID (4), its filing deadline (5), the download icon (6) and the count line (7)

1. **STR** / **CTR**: switches between the STR register and the CTR register. The selected tab is highlighted.
2. The message *CTR reports are generated once a day at 3:00 AM. New transactions will appear in the next scheduled run.* CTRs are created by a daily run, not as soon as a transaction arrives.
3. **Search by CTR ID or Date**: finds CTRs by their ID or date.
4. The CTR ID, with a copy icon.
5. **Filing Deadline**: the last day to file the CTR with the AMLC.
6. The download icon: downloads the CTR's CSV file. The column has no heading.
7. The count line (**Showing 1-10 of 150**) and, at the right, **Page 1 of 15** with first, previous, next and last page buttons. The register shows 10 CTRs per page.

Column	What it shows	Example
CTR ID	The CTR's ID: *CTR-*, the date as YYYYMMDD and a number for each CTR of that date, with a copy icon.	CTR-20261014-0001; CTR-20261012-0002
Date	The date of the transactions the CTR reports. One date can have more than one CTR.	2026-10-14
Customers	The number of customers in the CTR.	8
Transactions	The number of transactions in the CTR. In the examples it equals **Customers**.	8
Filing Deadline	The last day to file the CTR. In the examples it is five working days after **Date**.	2026-10-21
Created At	Date and time the platform created the CTR.	14 Oct 2026, 02:49:20 PM

Column	What it shows	Example
(download icon)	Downloads the CTR's CSV file in the GoTRACS format.	download icon

Not covered in this edition

This edition does not cover what happens when you click a CTR row, or how the register shows a CTR that could not be completed, for example because customer data is missing. The product requirements describe the statuses **PROCESSING**, **BLOCKED**, **READY** and **FAILED** for this, but they were not shown in the register when it was documented.

How CTRs are generated

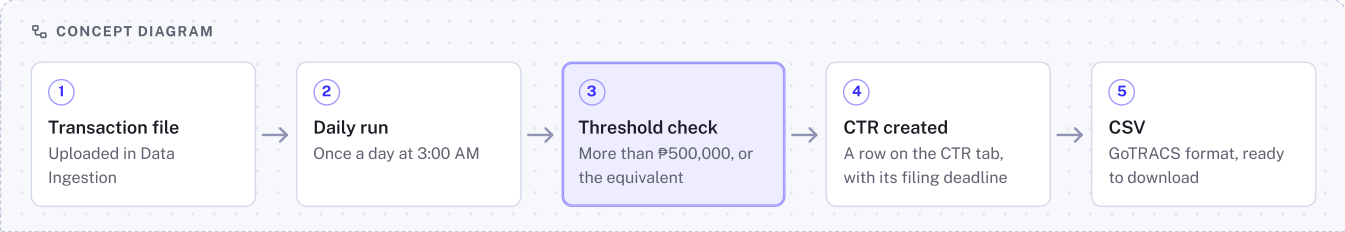


Diagram 6.2 — How a transaction becomes a CTR

You don't create CTRs by hand. When a transaction file is uploaded in Data Ingestion, its transactions are stored on the platform. Once a day, at 3:00 AM, the CTR run checks the stored transactions against the institution's approved CTR rules. Each covered transaction it finds goes into a CTR, and the platform creates the CTR's CSV file in the AMLC GoTRACS format. Transactions uploaded after a run, including late transactions for earlier dates, are picked up by the next run.

The threshold. The general rule is an amount of **more than ₱500,000**. An amount of exactly ₱500,000 is not over it. Amounts in other currencies are converted to pesos before they are compared.

Amount in PHP	Over the general threshold?
400,000	No
500,000	No. The amount must be more than ₱500,000.
500,001	Yes
750,000	Yes

Important

Not every transaction above ₱500,000 is reported, and the threshold is not the same for every institution. Which transactions are covered depends on the institution's sector, the AMLC transaction code and the mode of transaction (MOT), and some sectors, such as jewellery dealers, real estate developers and brokers, and casinos, have their own thresholds. These rules are approved by compliance and set up on the platform; they are not set on this page.

The filing deadline. A CTR must be filed by the fifth working day after the transaction. Weekends and Philippine non-working days are not counted. For example, transactions dated Wednesday 2026-10-14 have the deadline Wednesday 2026-10-21. The deadline is counted from the transaction date, so a late upload or a later run does not move it.

Missing data. A CTR is built only from transaction, customer and account data; there is no screen for typing in missing details. If a transaction or customer record is missing required data, correct it in the source data and upload it again so that the next run can use it.

AML context

Covered persons, such as banks, must report covered transactions to the AMLC within five working days. The CTR is filed through the AMLC's GoTRACS portal as a CSV file in the prescribed layout (Annex A of the GoTRACS guidelines). Fyscal ARCX prepares the file; filing it is still done in GoTRACS.

Find and download a CTR

Fyscal ARCX → Regulatory Reports → CTR

Use these steps to get a CTR's file ready for the AMLC before its filing deadline.

Step 1 **Open the CTR tab**

Open **Regulatory Reports** and click **CTR** at the top right (1 in Figure 6.11).

Step 2 **Find the CTR**

Click the **Search by CTR ID or Date** box and type a CTR ID (for example **CTR-20261014-0001**) or a date as shown in the **Date** column (for example **2026-10-14**). To work through the CTRs that are due soonest, check the **Filing Deadline** column.

Step 3 **Download the CSV**

In the row of the CTR, click the download icon (6 in Figure 6.11). The CSV file downloads.

Step 4 **File it with the AMLC**

Upload the CSV in the AMLC's GoTRACS portal before the filing deadline. Downloading the file does not file the CTR: Fyscal ARCX does not send CTRs to the AMLC, and the register does not record whether a CTR has been filed.

The CSV follows the GoTRACS CTR layout. It has no heading row; each line is a record that starts with a letter.

Record	What it contains
`H` (header)	The first line: the supervising agency code, the institution's 18-digit code, `CTR`, `X` and `A`. `A` means a new submission.
`D` (detail)	The transaction: date, AMLC transaction code, transaction reference, mode of transaction (MOT), amount in pesos and, for foreign currency, the amount and currency code. It is followed by the parties, such as the account holder, with their name, address, account, date of birth or registration, ID and source of funds.
`T` (trailer)	The last line: `T` and the number of detail records.

Amounts have no currency sign and no thousands separators, for example `650000.00`. The platform creates new submissions only: correcting or deleting a CTR that has already been filed is not done from this page.

RELATED IN CORE WORKFLOW

Case Manager | Case Manager Configuration | Customer 360

DETECTION & MONITORING

7 Name Screening

Fyscal ARCX → Name Screening

Name Screening checks names against the watchlist. Analysts use it to look up watchlist records and to screen a single name by hand. Compliance administrators use it to follow the batch and delta screening runs and to set the alert bands and field weightages that screening uses.

FOR	IN THE MENU	READING TIME
Analysts and administrators	Fyscal ARCX → Name Screening	About 24 min

Watchlist Search: look up watchlist records by name and narrow them with filters.

Watchlist Entity Details: read a watchlist record's identity, risk, network and source details.

Manual Screening: enter one person's or company's details and screen them on demand.

Batch Screening: check the batch screening runs, their status and the alerts they created.

Delta Screening: follow the delta screening runs and change their schedule.

Alert Configuration (**Configuration** → **Alerts**): review or change the alert bands.

Screening Configuration (**Configuration** → **Screening**): review or change the field weightages.

Review a name-screening match: what True Match, False Match and Potential Match mean for an analyst, and how to decide between them.

AML context

Name screening compares customers with lists of people and organisations that carry risk, such as sanctioned parties and politically exposed persons (PEPs). A possible match is not a finding. It prompts an analyst to check the record, decide whether it is the same person or organisation, and record why.

CONCEPT DIAGRAM

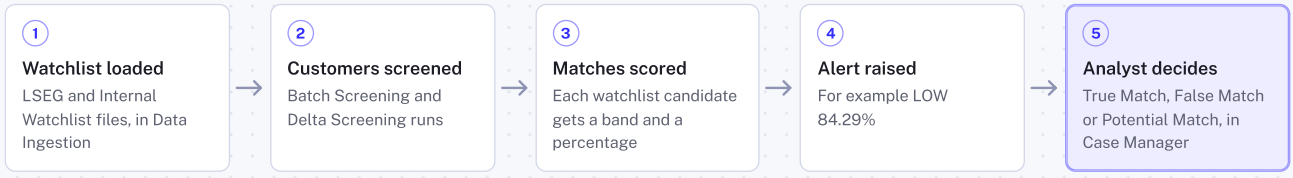


Diagram 7.1 — From watchlist to a decided name-screening alert

Diagram 7.1 shows where each part of this chapter fits. Watchlist files are loaded in Watchlist Ingestion and can be looked up in Watchlist Search. Batch Screening and Delta Screening list the runs and the alerts each one created. Each alert shows its band and percentage, and the bands are set in Alert Configuration. The analyst reviews the matches and records a disposition in Case Manager; Review a name-screening match explains how to decide.

Watchlist Search

Fyscal ARCX → Name Screening → Watchlist Search

Use Watchlist Search to look up records on the watchlist by name, narrow them with filters and open any record's details. The table stays empty until you search.

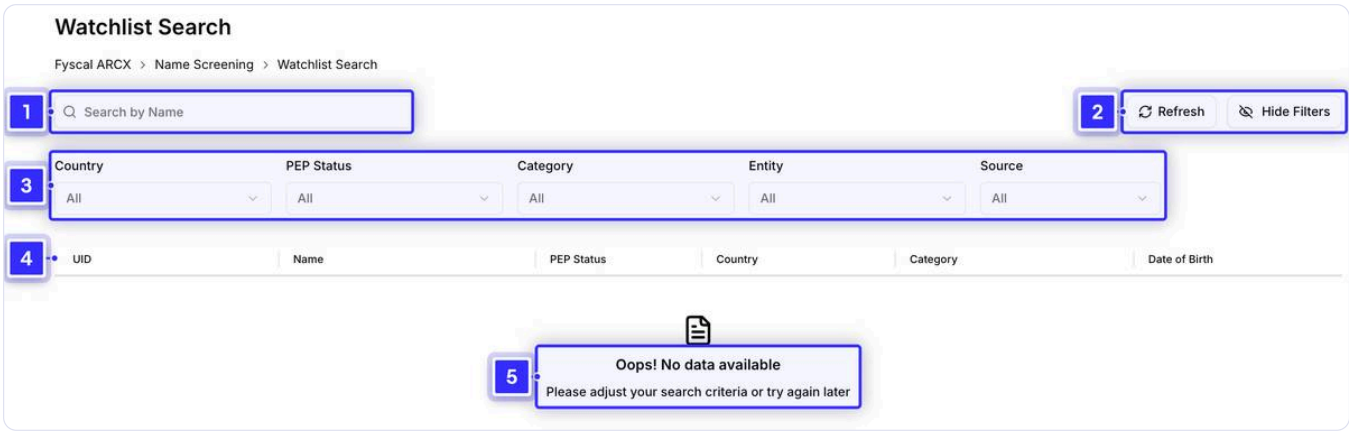


Figure 7.1 Watchlist Search before a search: Search by Name (1), Refresh and Hide Filters (2), the five filters (3), the results columns (4) and the empty state (5)

1. **Search by Name**: type the name of the person or entity to look up.
2. **Refresh** reloads the results. **Hide Filters** hides the filter row, which is shown when the page opens.
3. The filters: **Country**, **PEP Status**, **Category**, **Entity** and **Source**. Each one is set to **All** by default.
4. The results table, with the columns **UID**, **Name**, **PEP Status**, **Country**, **Category** and **Date of Birth**.
5. The empty state, **Oops! No data available** with the line "Please adjust your search criteria or try again later", which shows until a search returns records.

Filters

Each filter opens a list with a search box at the top, so you can type to find an option.

Filter	Options
Country	Default **All**. Choose a country.
PEP Status	**Active**, **NON-PEP**, **Unknown**
Category	**WEBSITE**, **MILITARY**, **AIRCRAFT**, **VESSEL**, **BANK**, **POLITICAL INDIVIDUAL**, **SHELL BANK OR COMPANY**, **RELIGION**, **CRIME - ORGANIZED**, **CRIME - TERROR**, **EMBARGO**, **POLITICAL PARTY**, **EMBARGO VESSEL**, **TRADE UNION**, **PORT**, **CRIME - FINANCIAL**, **ORGANISATION**, **CORPORATE**, **EMBARGO AIRCRAFT**, **INDIVIDUAL**, **COUNTRY**, **DIPLOMAT**, **CRIME - WAR**, **CRIME - OTHER**, **ADDRESS**, **CRIME - NARCOTICS**, **SPECIAL JURISDICTION**, **LEGAL**
Entity	**Male**, **Female**, **Entity**, **Unknown**
Source	**All**, **Internal Watchlist**, **LSEG**

Results columns

Column	What it shows
UID	The record's identifier on the watchlist, for example **3601955**. A record marked deleted shows a red **Deleted** label and a date (for example **15/04/2026**) under its UID.
Name	The name as held on the watchlist, for example **John SMITH**.
PEP Status	A green **PEP** chip, a red **NON-PEP** chip, or **-** when the record has no PEP status.
Country	The record's country, for example **UNITED KINGDOM**.
Category	The record's category, for example **INDIVIDUAL**, **LEGAL** or **CRIME - NARCOTICS**.
Date of Birth	The date of birth in YYYY/MM/DD format, or **-** when the record has none.
Source	The list the record comes from, for example **LSEG**. This column appears once results are shown.

Step 1 **Search by name**

Type the name in **Search by Name**, for example *John Smith*. The table fills with matching records and a **Name: John Smith** tag appears under the filters. A common name returns many records: this search returns 20, and the footer reads **Showing 20 results**.

Step 2 **Narrow the results with a filter**

Click a filter, for example **PEP Status** (1), and choose an option from the list (3). You can type in the list's search box (2) to find an option.

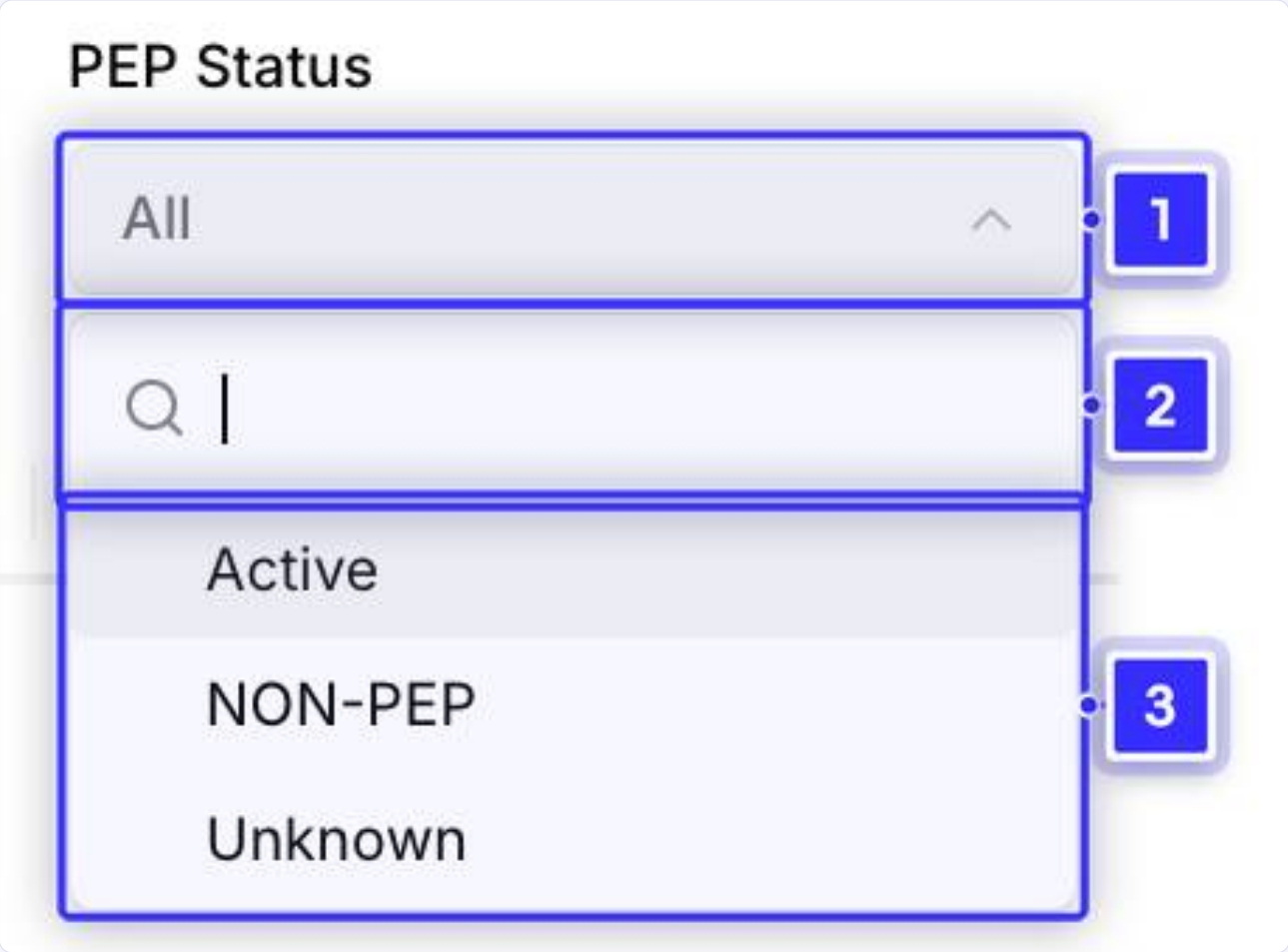


Figure 7.2 The PEP Status filter (1) open: the search box (2) and the options Active, NON-PEP and Unknown (3)

Step 3 **Read the results**

Compare UID, PEP Status, Country, Category and Date of Birth to tell records with the same name apart (dates of birth are hidden in the figure). Use the arrows at the bottom right to move between pages.

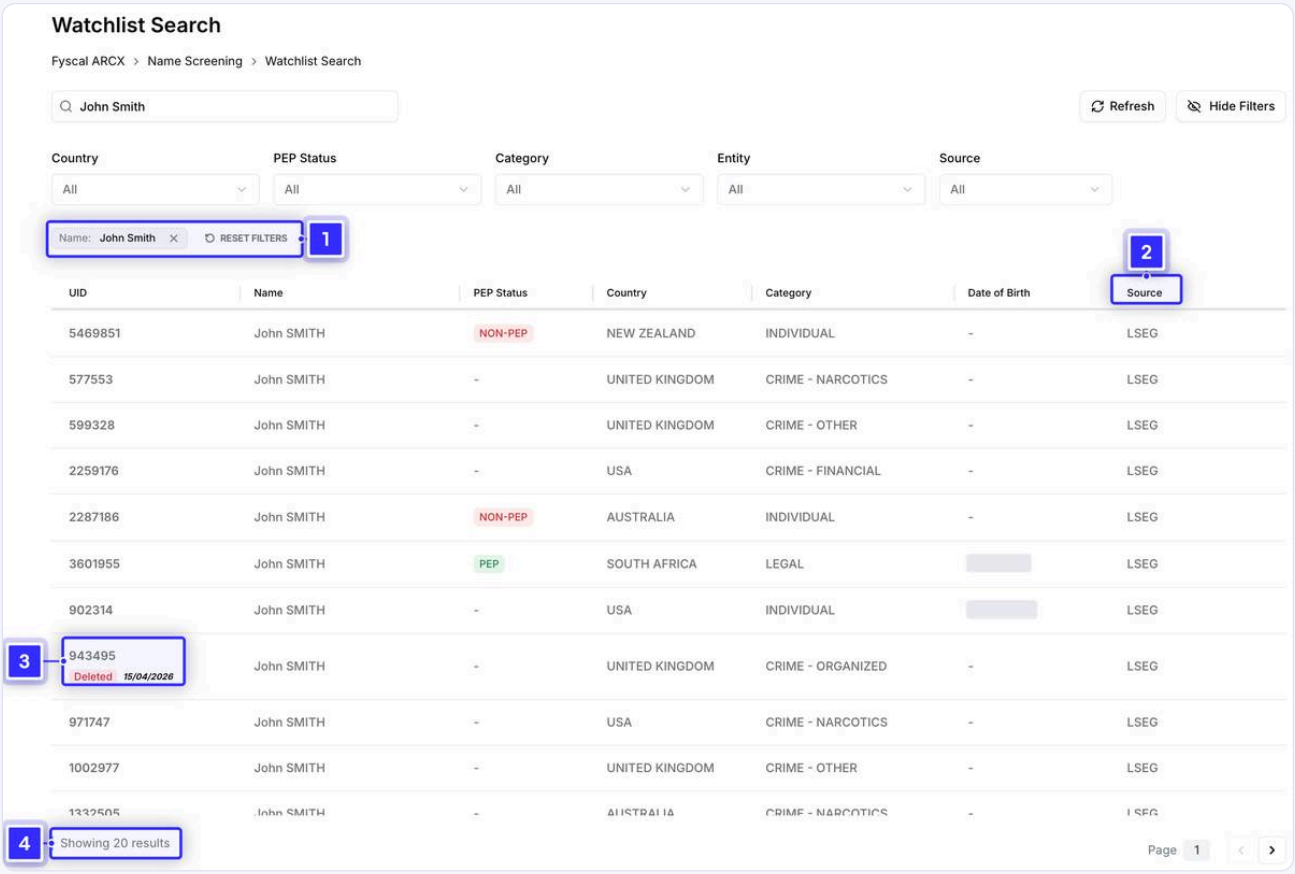


Figure 7.3 Results for John Smith: the Name tag and RESET FILTERS (1), the Source column (2), a record marked Deleted with its date (3) and the result count (4); dates of birth hidden

Step 4 **Clear the search**

Click the **×** on the **Name** tag to remove that one filter, or click **RESET FILTERS** to clear them all.

Watchlist Entity Details

Fyscal ARCX → Name Screening → Watchlist Search → a result row

Open a record's details when you need more than the results table shows: its identity, risk background, network and sources. Click a row in the results to open the **Watchlist Entity Details** dialog for that record. The dialog's heading is the entity name. Below it, two summary cards show **Entity Name**, **UID**, **PEP Status** and **Category**. These cards stay in place while you move between the four tabs: **Profile & Identity**, **Risk & Background**, **Network & Locations** and **Source**. A field shows **--** when the record has no value for it. Click **×** at the top right to close the dialog.

The figures below show record **3601955**, JOHN SMITH, with PEP Status **PEP** and Category **LEGAL**. Third-party details from the watchlist (date and place of birth, address, associates, biography, identification, reports and source links) are hidden in the figures.

Tab	Fields
Profile & Identity	**Gender/Type**, **Date of Birth**, **Place of Birth**, **Citizenship**, **Alternative Spelling**, **Age**, **Identification Number**, **Aliases**, **IDs / Passports**, **Deceased Date**
Risk & Background	**Position**, **PEP History**, **Title**, **Category**, **Sub-Category**, **Special Interests**, **PEP Status**, and a **Further Information/Biography** panel. In this record the panel is split into **BIOGRAPHY**, **IDENTIFICATION** and **REPORTS**.
Network & Locations	**Addresses**, **Associates** (shown as UIDs in blue), **Companies**
Source	**Links**: the source websites for the record, each shown as a link chip.

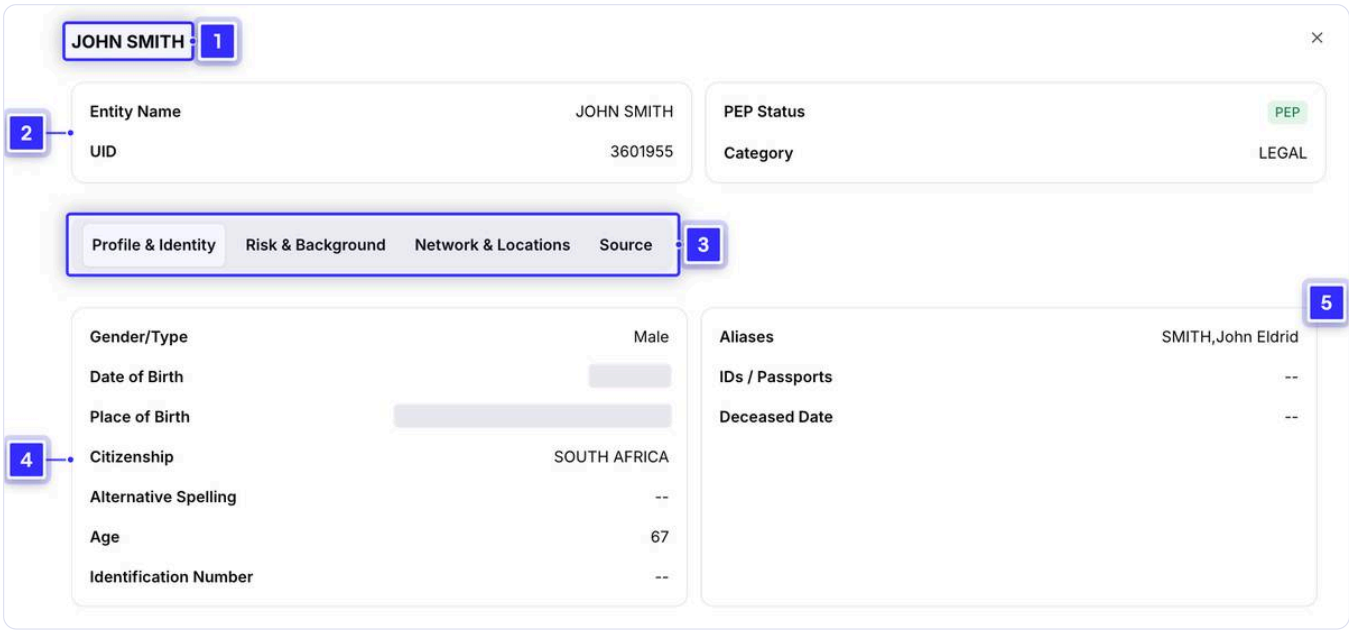


Figure 7.4 Profile & Identity tab: the entity name (1), the summary cards (2), the four tabs (3), the left column of identity fields (4) and the right column (5)

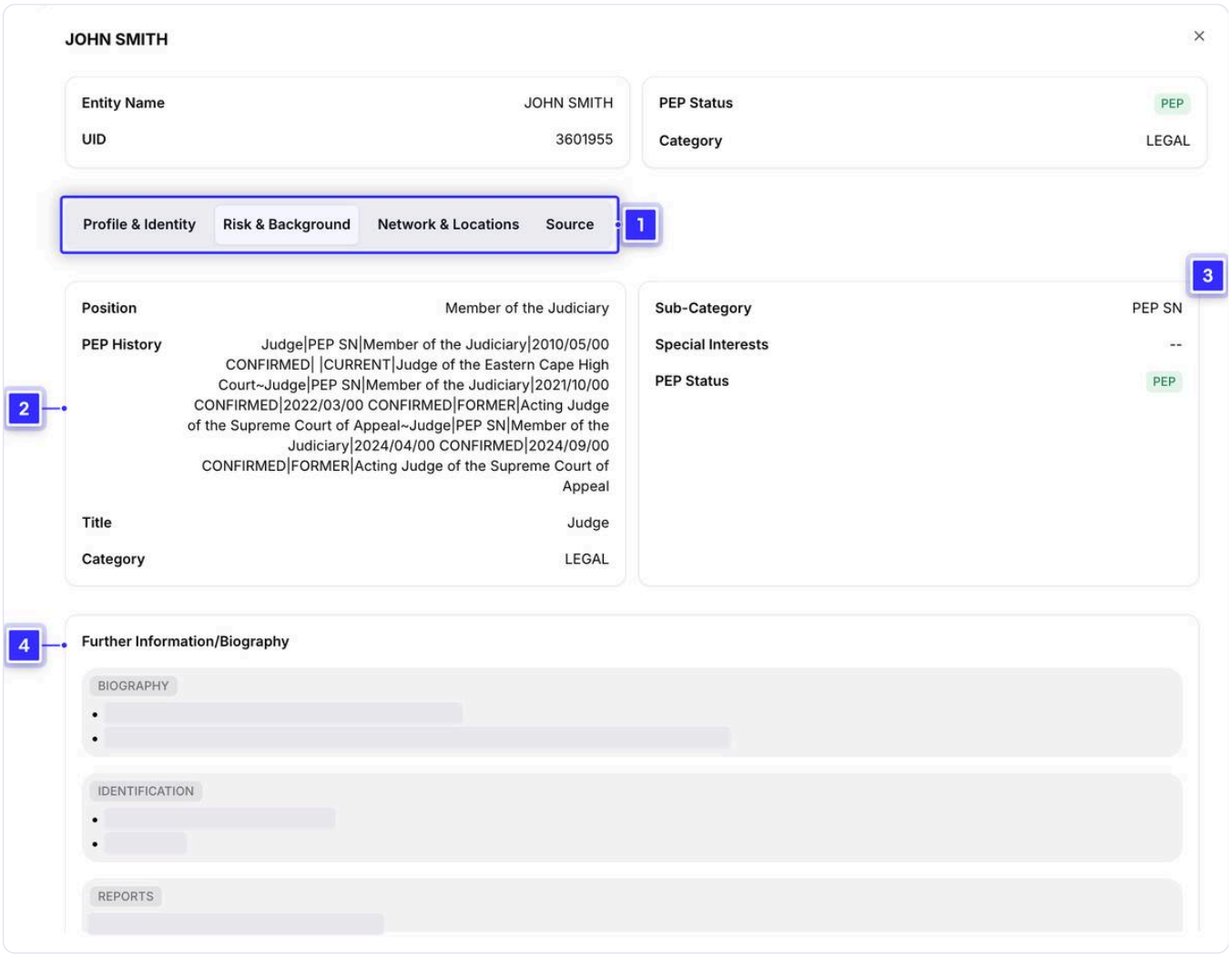


Figure 7.5 Risk & Background tab: the tabs (1), Position, PEP History, Title and Category (2), Sub-Category, Special Interests and PEP Status (3), and the Further Information/Biography panel (4)

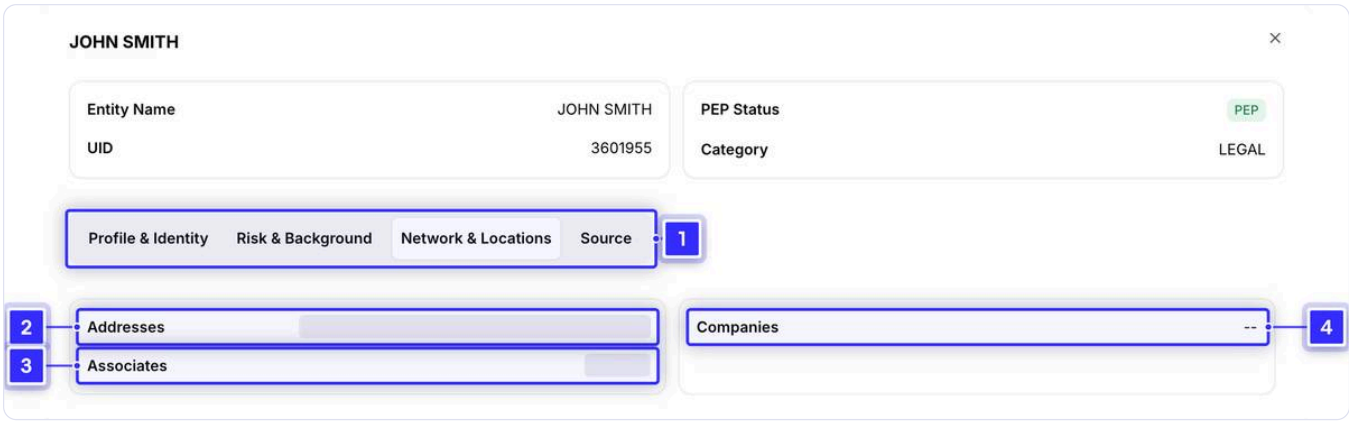


Figure 7.6 Network & Locations tab: the tabs (1), Addresses (2), Associates (3) and Companies (4)

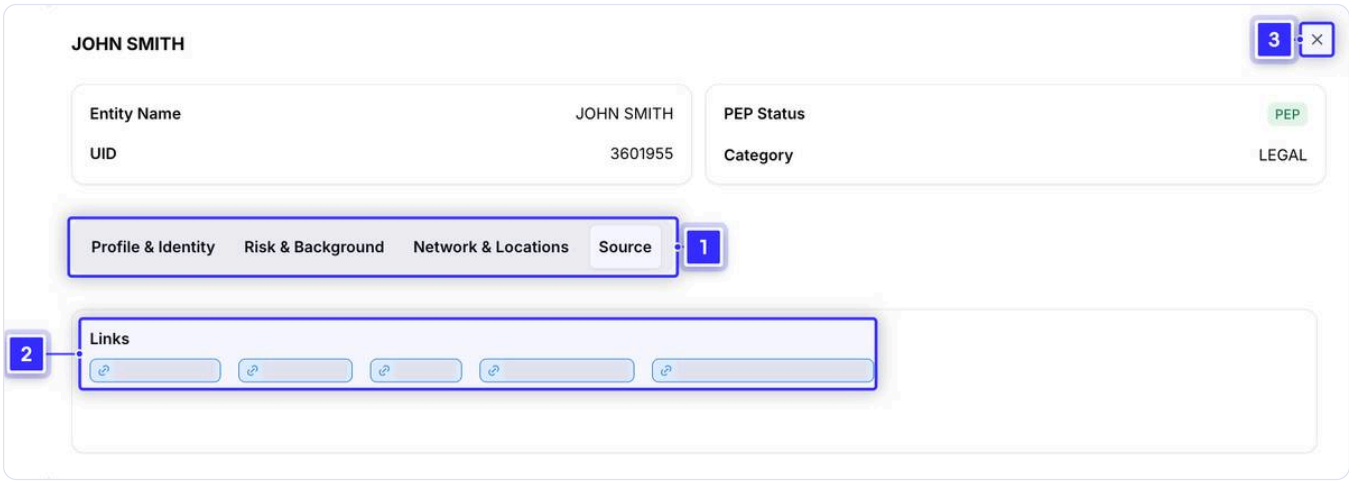


Figure 7.7 Source tab: the tabs (1), the Links (2) and the close button (3)

> **Note**
> The PEP Status filter offers **NON-PEP**, **Unknown** and **Active**, but the results table and this dialog show **PEP**, **NON-PEP** or **-**.

Manual Screening

Fyscal ARCX → Name Screening → Manual Screening

Use Manual Screening to screen one person or company by entering their details yourself. Next to each field the form shows the weightage it carries, taken from the active Screening Configuration.

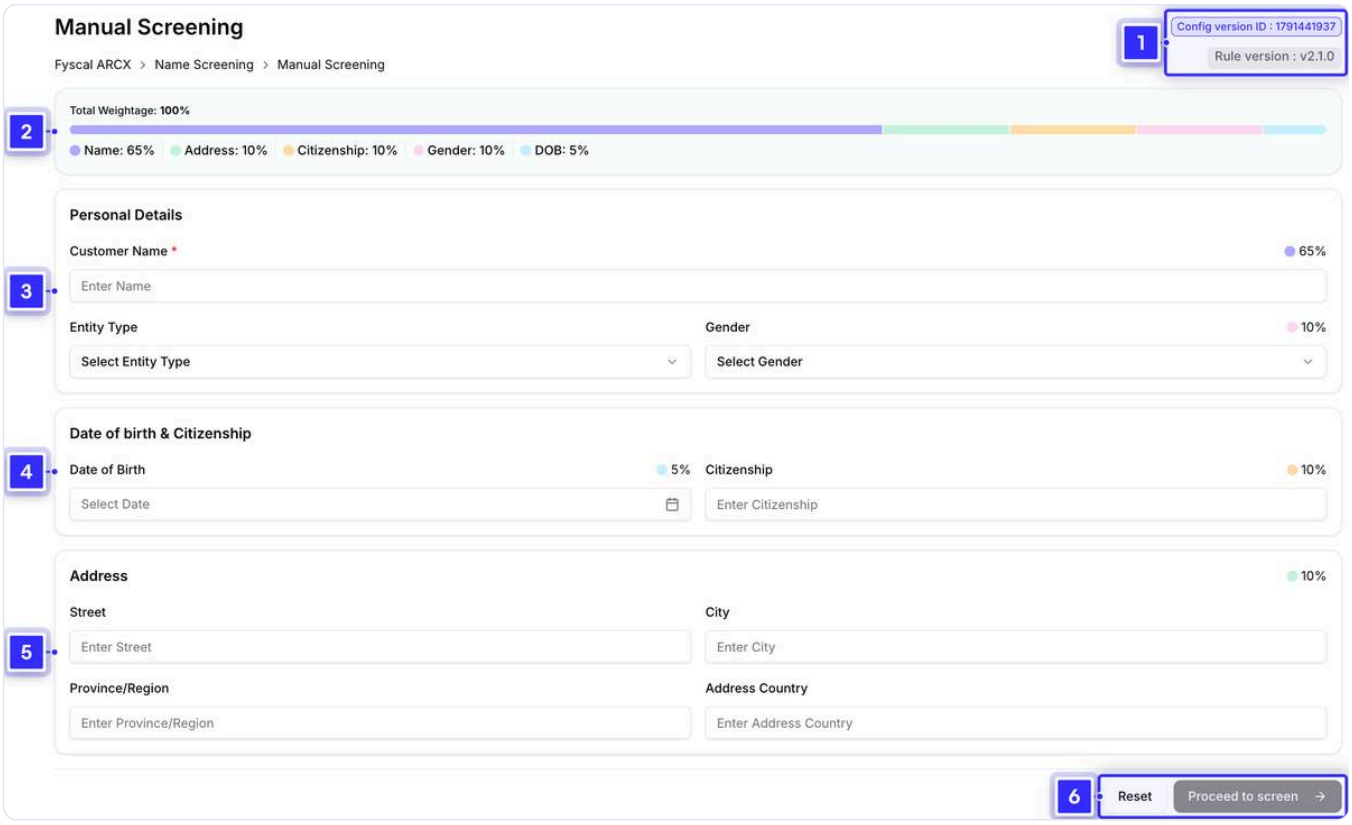


Figure 7.8 The Manual Screening form, empty: the configuration chips (1), the weightage bar (2), Personal Details (3), Date of birth & Citizenship (4), Address (5), and Reset and Proceed to screen (6)

1. Two chips: **Config version ID : 1791441937** and **Rule version : v2.1.0**. The config version ID is the same number as the ACTIVE version on the Screening Configuration page.
2. The weightage bar: **Total Weightage: 100%**, split as **Name: 65%**, **Address: 10%**, **Citizenship: 10%**, **Gender: 10%** and **DOB: 5%**.
3. **Personal Details**: Customer Name, Entity Type and Gender.
4. **Date of birth & Citizenship**: Date of Birth and Citizenship.
5. **Address**: Street, City, Province/Region and Address Country. The section carries a single weightage of 10%.
6. **Reset** and **Proceed to screen**.

Field	Weightage shown	Required	Options or format
Customer Name	65%	Yes (*)	Free text. Placeholder "Enter Name".
Entity Type	None	No	Placeholder "Select Entity Type". Options **Individual** and **Company**.
Gender	10%	No	Placeholder "Select Gender". Options **Male**, **Female** and **Other**.
Date of Birth	5%	No	Placeholder "Select Date". A calendar with month and year selectors. Years run from 1926 to 2026, and dates after today are greyed out.
Citizenship	10%	No	Free text. Placeholder "Enter Citizenship".
Street	10% for the whole Address section	No	Free text. Placeholder "Enter Street".
City		No	Free text. Placeholder "Enter City".
Province/Region		No	Free text. Placeholder "Enter Province/Region".
Address Country		No	Free text. Placeholder "Enter Address Country".

Step 1 **Enter the name**

Type the customer's name in **Customer Name**. This is the only field marked as required (*).

Step 2 **Choose the entity type**

Open **Entity Type** (1) and choose **Individual** or **Company** (2).

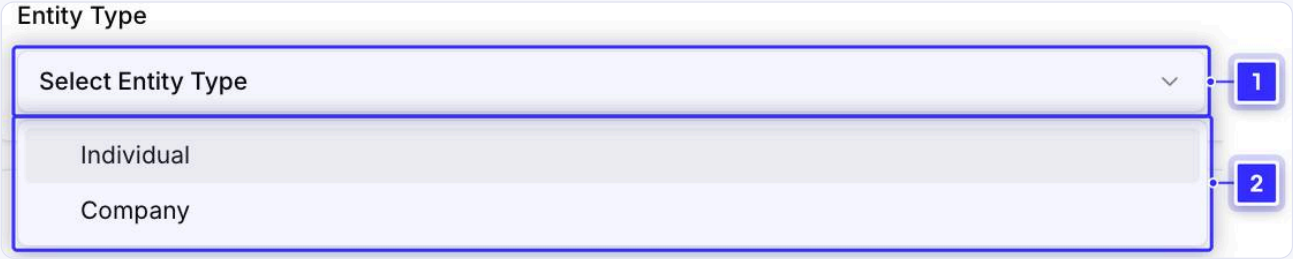


Figure 7.9 The Entity Type field (1) and its list (2): Individual and Company

Step 3 **Choose the gender**

Open **Gender** and choose **Male**, **Female** or **Other**.

Step 4 **Pick the date of birth**

Click **Date of Birth**. In the calendar, choose the month and year from the two lists at the top (2), or move with the arrows (1, 3), then click the day. Today's date is highlighted (4) and dates after it are greyed out.

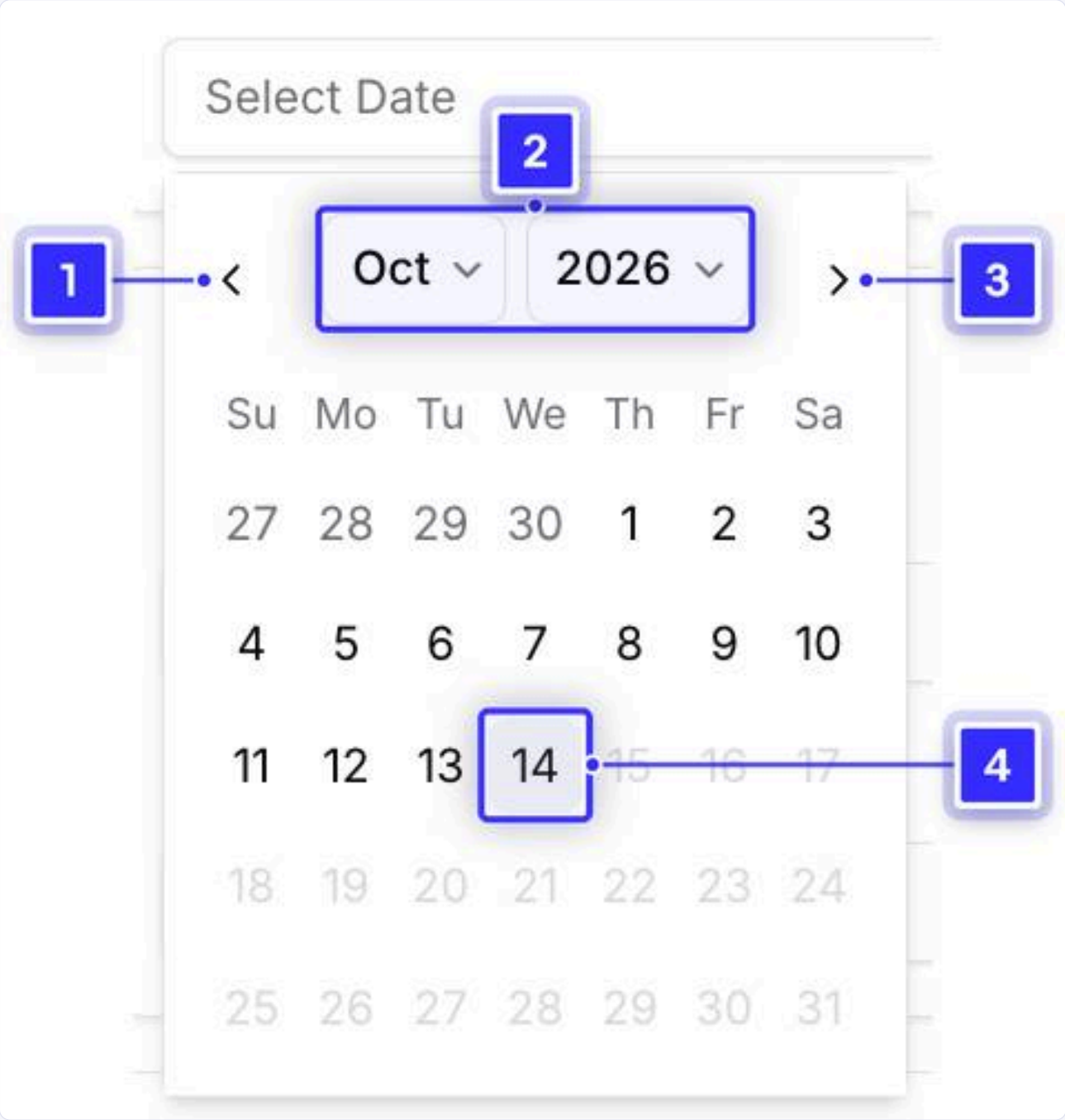


Figure 7.10 The Date of Birth calendar: previous month (1), the month and year lists (2), next month (3) and today's date (4); dates after today are greyed out

Step 5 **Add citizenship and address**

Type **Citizenship**, then fill in whichever address fields you have: **Street**, **City**, **Province/Region** and **Address Country**.

Step 6 **Screen, or start again**

Click **Proceed to screen** to run the screening. To clear the form instead, click **Reset**.

Note

On the empty form, **Proceed to screen** is greyed out.

Batch Screening

Fyscal ARCX → Name Screening → Batch Screening

Use Batch Screening to check whether batch runs succeeded and how many alerts they created. Batch Screening lists the batch screening runs. For each run it shows how many customers were scanned, how many alerts were created, and the run's status and duration. The page has no **Change Schedule** button, and clicking a row does not open a detail view.

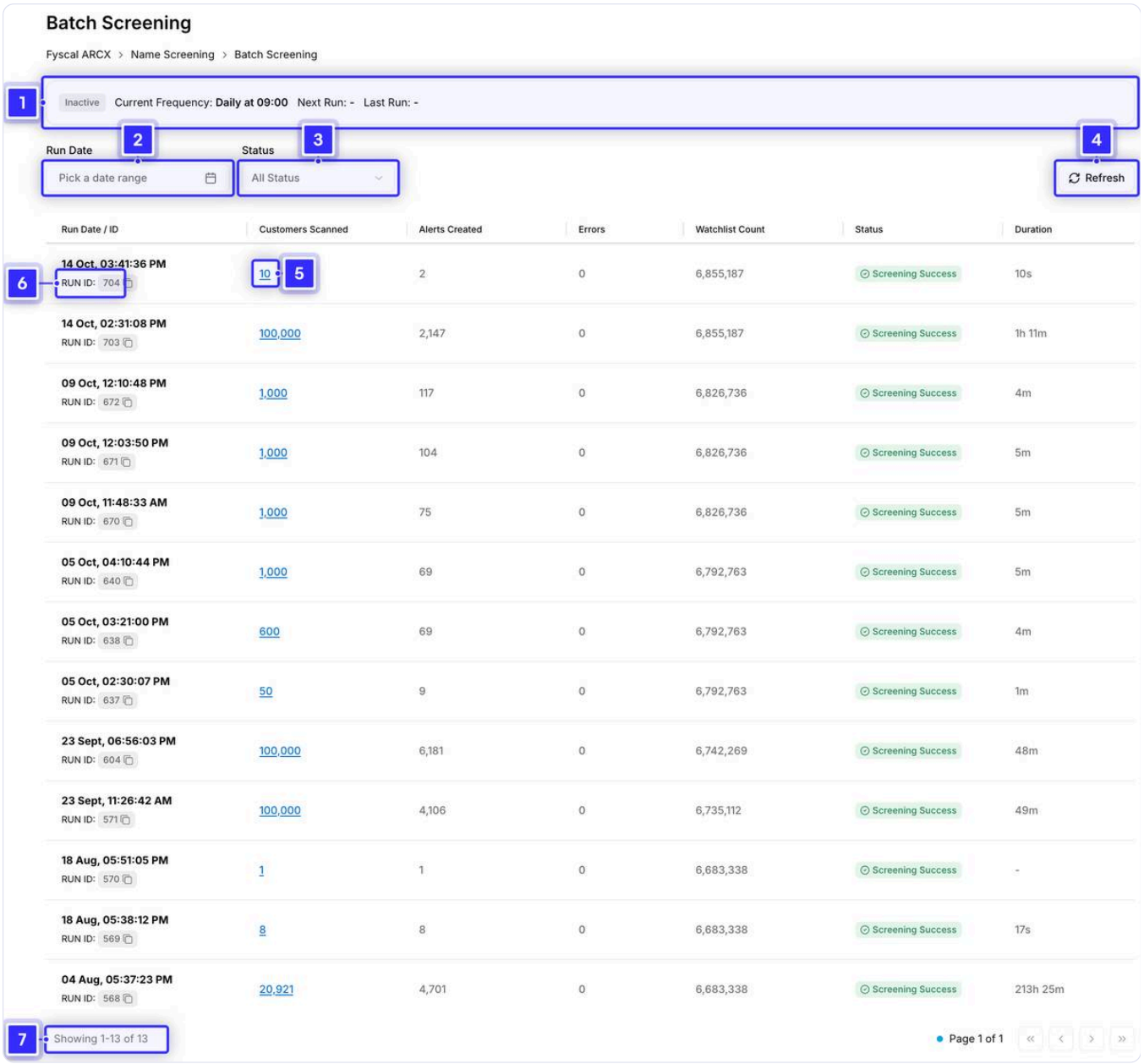


Figure 7.11 Batch Screening: the schedule card (1), Run Date (2), Status (3), Refresh (4), the Customers Scanned figure (5), the run ID (6) and the record count (7)

1. The schedule card. Here it reads **Inactive**, **Current Frequency: Daily at 09:00**, **Next Run: -** and **Last Run: -**.
2. **Run Date**: a date-range field ("Pick a date range").
3. **Status**: the status filter, set to **All Status** by default.
4. **Refresh** reloads the table.
5. The **Customers Scanned** figure, shown underlined in blue.
6. The run ID, with a copy icon next to it.
7. The record count, for example **Showing 1-13 of 13**, with the page controls on the right.

Column	What it shows
Run Date / ID	The run's date and time (for example **14 Oct, 03:41:36 PM**) and, below it, **RUN ID:** with the run number and a copy icon.

Column	What it shows
Customers Scanned	The number of customers the run screened.
Alerts Created	The number of alerts the run created.
Errors	The number of errors in the run.
Watchlist Count	The number of watchlist records at the time of the run, for example **6,855,187**.
Status	The run's status. See the table below.
Duration	How long the run took, for example **10s**, **5m** or **1h 11m**, or **-** when no duration is recorded.

Status	Meaning
Screening In Progress	The run has not finished yet.
Screening Success	The run completed successfully.
Screening Failed	The run failed.

Step 1 **Filter runs by status**

Click **Status** (1) and choose **Screening In Progress**, **Screening Success** or **Screening Failed** (3). You can type in the list's search box (2) to find a status.

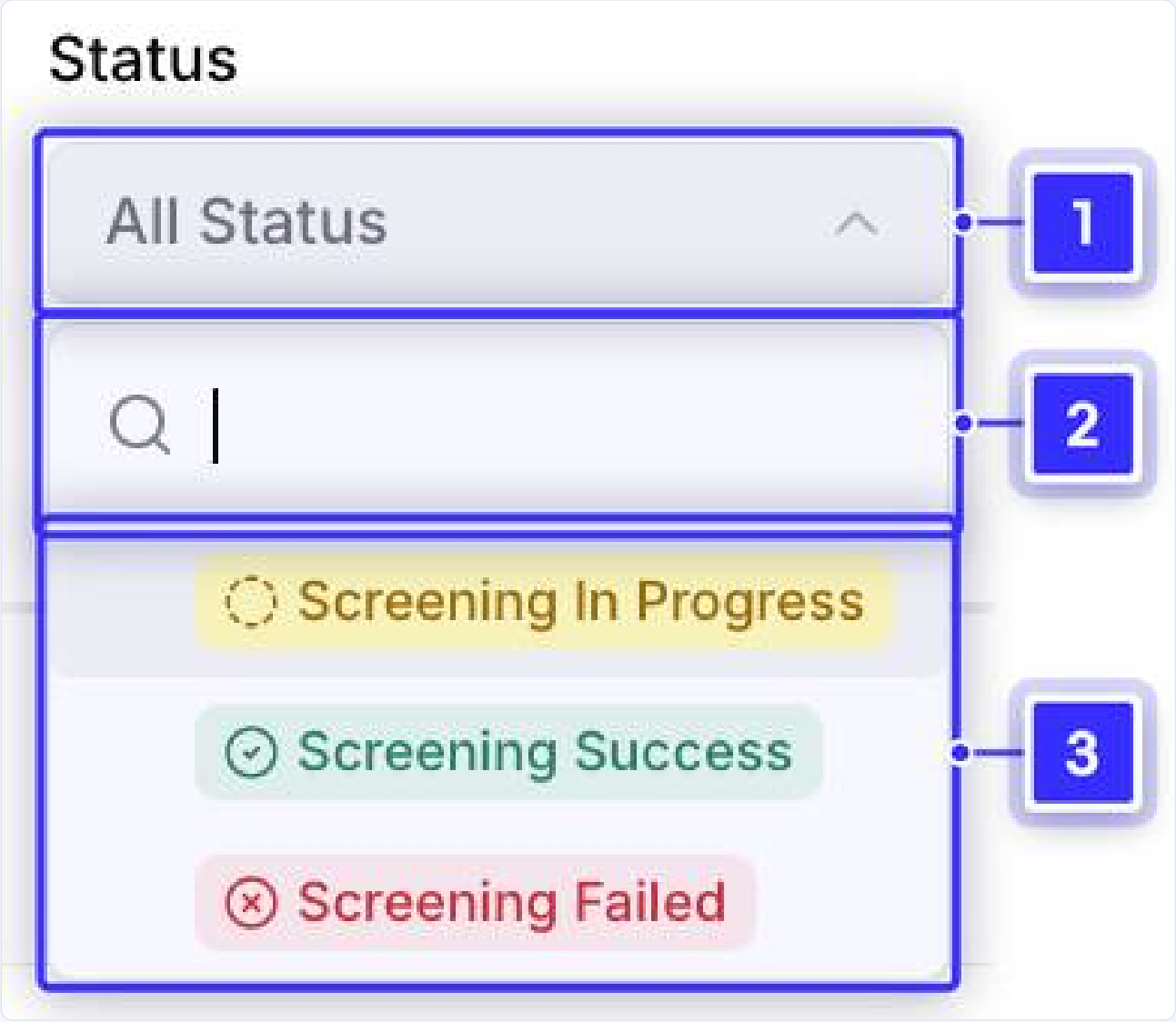


Figure 7.12 The Batch Screening Status filter (1) open: the search box (2) and the options Screening In Progress, Screening Success and Screening Failed (3)

Step 2 **Filter runs by date**

Click **Run Date** ("Pick a date range") and choose the first and last day of the period.

Step 3 **Refresh the list**

Click **Refresh** to reload the table.

Note

In the example list, the three batch runs of 05 Oct each started a few seconds after a **Customers** job in Batch Ingestion and scanned the number of customers that job ingested: run 637 (50 customers) after job 168, run 638 (600) after job 171, and run 640 (1,000) after job 177.

Delta Screening

Fyscal ARCX → Name Screening → Delta Screening

Use Delta Screening to follow the delta runs and to change when they run. Delta Screening shows the delta screening schedule and lists its runs, including the next scheduled run. Unlike Batch Screening, this page has **Resume** and **Change Schedule** buttons.

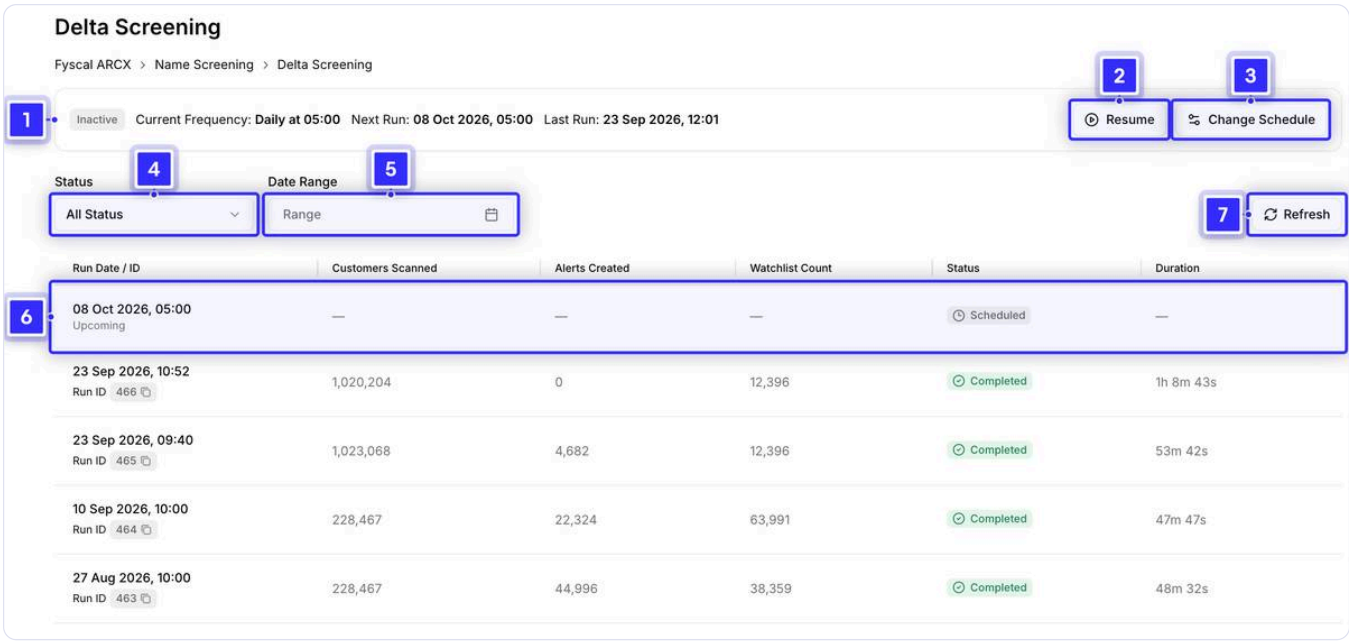


Figure 7.13 Delta Screening: the schedule bar (1), Resume (2), Change Schedule (3), Status (4), Date Range (5), the Upcoming run (6) and Refresh (7)

1. The schedule bar. Here it reads **Inactive**, **Current Frequency: Daily at 05:00**, **Next Run: 08 Oct 2026, 05:00** and **Last Run: 23 Sep 2026, 12:01**. On 14 October the Next Run date shown had already passed, and the Upcoming row still showed it.
2. **Resume**: a button on the schedule bar.
3. **Change Schedule** opens the **Change Screening Schedule** dialog.
4. **Status**: the status filter, set to **All Status** by default.
5. **Date Range**: a date-range field ("Range").
6. The next scheduled run, labelled **Upcoming** with the status **Scheduled**. Its other columns show —.
7. **Refresh** reloads the table.

The two screening pages differ as follows:

On the page	Batch Screening	Delta Screening
Schedule with Current Frequency, Next Run and Last Run	✓ Yes	✓ Yes
Resume button	× No	✓ Yes
Change Schedule button	× No	✓ Yes
Errors column	✓ Yes	× No
Next run listed as **Upcoming**	× No	✓ Yes

The **Watchlist Count** also differs in size: 6,792,763 on the batch runs of 05 Oct, and 12,396 on the delta runs of 23 Sep.

> **AML context**
> In screening generally, a full screen checks customers against the whole list, while a delta screen checks them against the records added or changed since the last run, so that list updates are picked up between full screens.

Column	What it shows
Run Date / ID	The run's date and time (for example **23 Sep 2026, 10:52**) and, below it, **Run ID** with the run number and a copy icon. The next scheduled run shows **Upcoming** in place of the ID.
Customers Scanned	The number of customers the run screened.
Alerts Created	The number of alerts the run created.
Watchlist Count	The watchlist count recorded for the run, for example **12,396**.

Column	What it shows
Status	The run's status. See the table below.
Duration	How long the run took, for example **1h 8m 43s**.

The table shows 20 runs per page (**Showing 1-20 of 30**, **Page 1 of 2**).

Status	Meaning
Scheduled	The next run, not yet started (the **Upcoming** row).
In Progress	The run has not finished yet.
Completed	The run finished.
Failed	The run failed.
Paused	A status offered by the filter.

Step 1 **Filter runs by status**

Click **Status** (1) and choose **All Status**, **Scheduled**, **In Progress**, **Completed**, **Failed** or **Paused** (3). A tick marks the current choice (2).

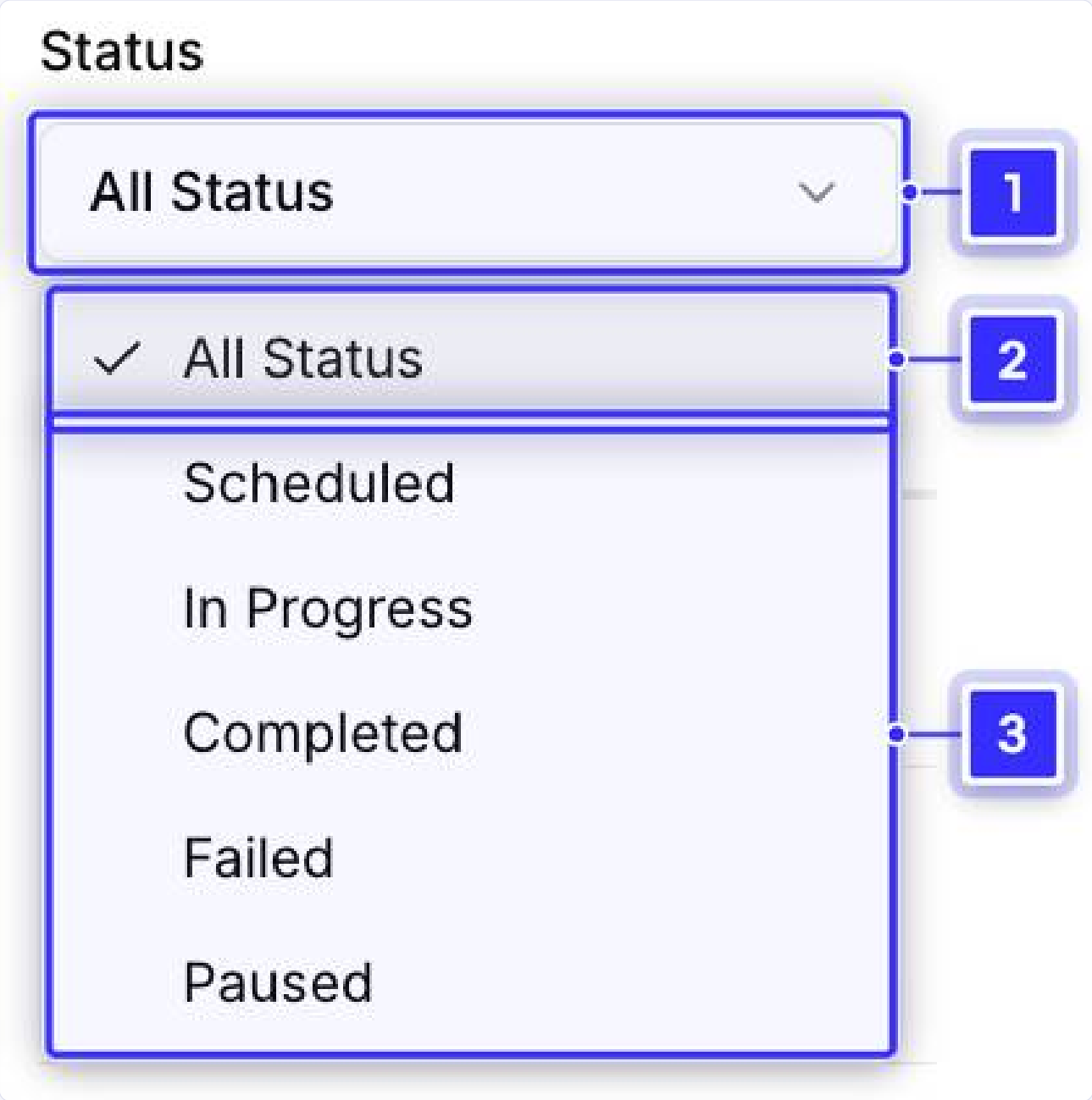


Figure 7.14 The Delta Screening Status filter (1): All Status ticked (2), then Scheduled, In Progress, Completed, Failed and Paused (3)

Step 2 **Filter runs by date**

Click **Date Range**. A two-month calendar opens. Click the first and last day of the period, then click **Apply**. **Clear** removes the range.

Step 3 **Open Change Schedule**

Click **Change Schedule**. The **Change Screening Schedule** dialog opens, headed "Select the new frequency and run time, add a reason, then review before confirming."

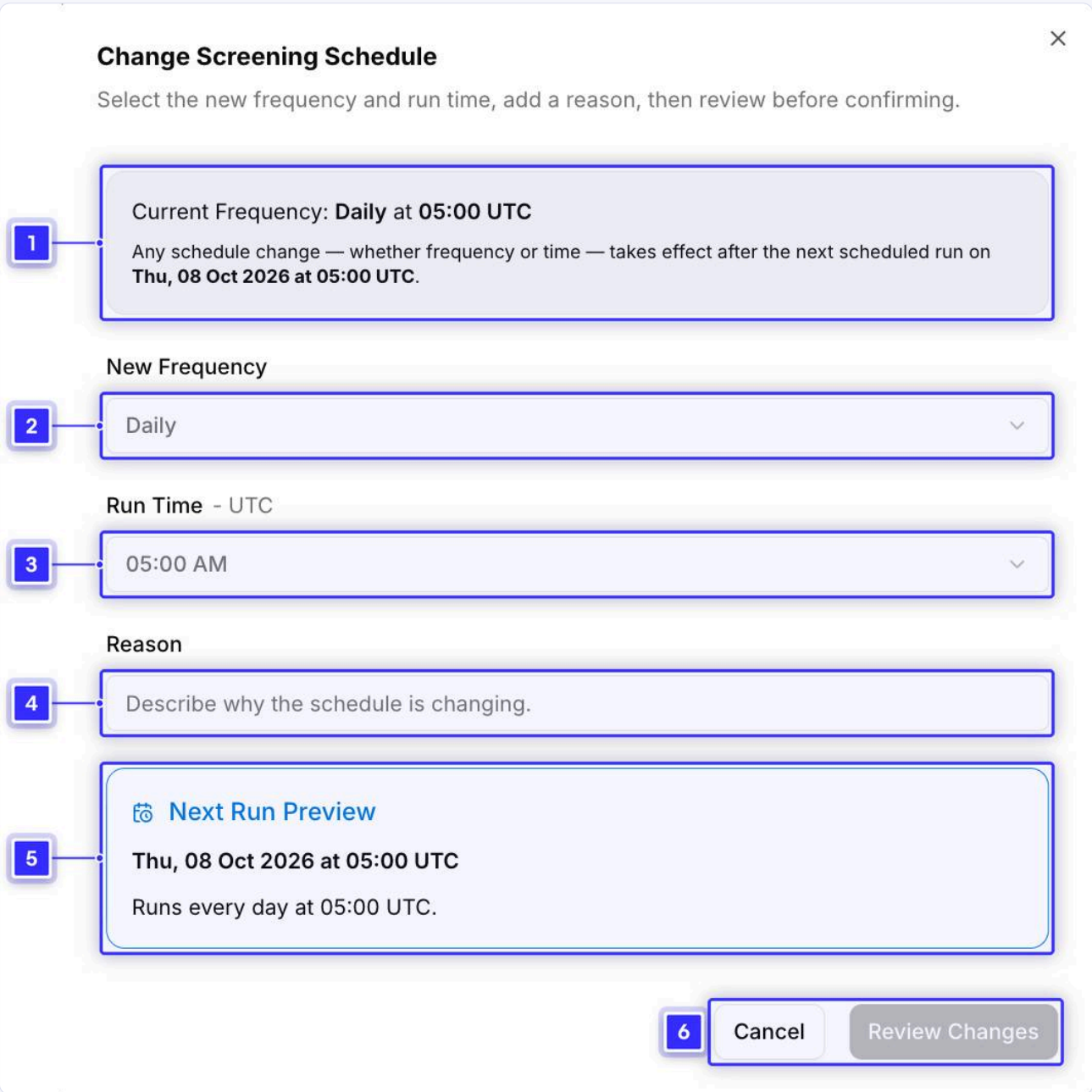


Figure 7.15 The Change Screening Schedule dialog: the current schedule (1), New Frequency (2), Run Time - UTC (3), Reason (4), Next Run Preview (5), and Cancel and Review Changes (6)

Area or field	What it shows or expects
1. Current schedule	**Current Frequency: Daily at 05:00 UTC**, followed by "Any schedule change — whether frequency or time — takes effect after the next scheduled run on Thu, 08 Oct 2026 at 05:00 UTC."
2. New Frequency	A list. Here it shows **Daily**.
3. Run Time - UTC	A list of times in UTC. Here it shows **05:00 AM**.
4. Reason	Free text. Placeholder "Describe why the schedule is changing."

Area or field	What it shows or expects
5. Next Run Preview	The next run and a summary of the schedule, for example **Thu, 08 Oct 2026 at 05:00 UTC** and "Runs every day at 05:00 UTC."
6. Buttons	**Cancel** and **Review Changes**. × at the top right also closes the dialog.

Step 4 **Set the new schedule**

Choose the **New Frequency** and the **Run Time**. Type the **Reason** for the change. Check the **Next Run Preview**, then click **Review Changes**. To leave without changing anything, click **Cancel**.

Note

In the dialog as it opens, with no reason entered, **Review Changes** is greyed out. Run times in the dialog are in UTC.

Alert Configuration

Fyscal ARCX → Name Screening → Configuration → Alerts

Use Alert Configuration to review or change the alert bands that screening uses. Each band has a name, a colour, a Min % to Max % range, a **No Alert** setting, an **SLA Deadline** and an **Auto Hibernate** setting. The page has two tabs: **Active Alert Configuration** and **Alert Configuration History**.

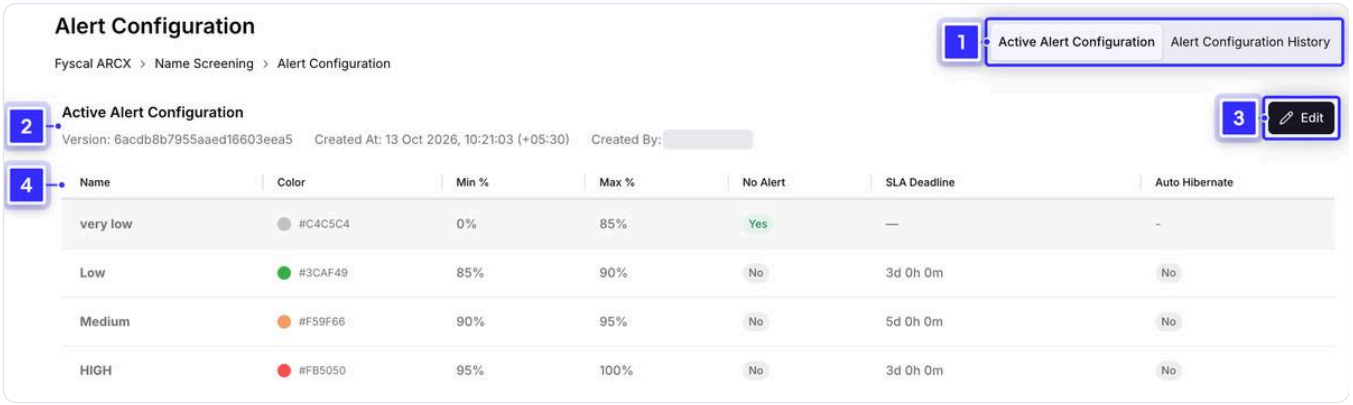


Figure 7.16 Active Alert Configuration: the tabs (1), the version details (2), Edit (3) and the bands table (4)

1. The tabs **Active Alert Configuration** and **Alert Configuration History**.
2. The active version: **Version** (for example 6acdb8b7955aaed16603eea5), **Created At** (13 Oct 2026, 10:21:03 (+05:30)) and **Created By** (hidden in the figure).
3. **Edit** switches the table into the edit form.
4. The bands table.

Column	What it shows
Name	The band's name.
Color	The band's colour, as a swatch and a hex code.
Min %	The lower end of the band's range.
Max %	The upper end of the band's range.
No Alert	**Yes** or **No**.
SLA Deadline	The SLA as days, hours and minutes (for example **3d 0h 0m**), or — where No Alert is Yes.
Auto Hibernate	**Yes** or **No**, or - where No Alert is Yes.

The active configuration in Figure 7.16 (saved on 13 Oct 2026):

Name	Color	Min %	Max %	No Alert	SLA Deadline	Auto Hibernate
very low	#C4C5C4	0%	85%	Yes	—	-

Name	Color	Min %	Max %	No Alert	SLA Deadline	Auto Hibernate
Low	#3CAF49	85%	90%	No	3d 0h 0m	No
Medium	#F59F66	90%	95%	No	5d 0h 0m	No
HIGH	#FB5050	95%	100%	No	3d 0h 0m	No

The SLA does not rise with the band in this configuration: Medium has 5 days, while Low and HIGH have 3 days each. The values are set per band, so check them when you change the bands.

A Name Screening alert shows its band and percentage in its header, for example **LOW 84.29%** on ALT-NS-05102026-000115, and the same band on each match candidate (see Alert Details: Name Screening). The header also shows **Config:** with an Alert Configuration version ID. On that alert it is 6ab3c6efe9d518f3fc6b21d9. That version is not among the 10 listed in Alert Configuration History on 14 October 2026. The alert still shows LOW 84.29%, although 84.29% falls in the current very low band (0% to 85%).

> **AML context**
> Bands let a team review the strongest matches first and give each band a review deadline. An SLA here is the institution's own service level for reviewing an alert, not a regulatory deadline.

Edit the alert configuration

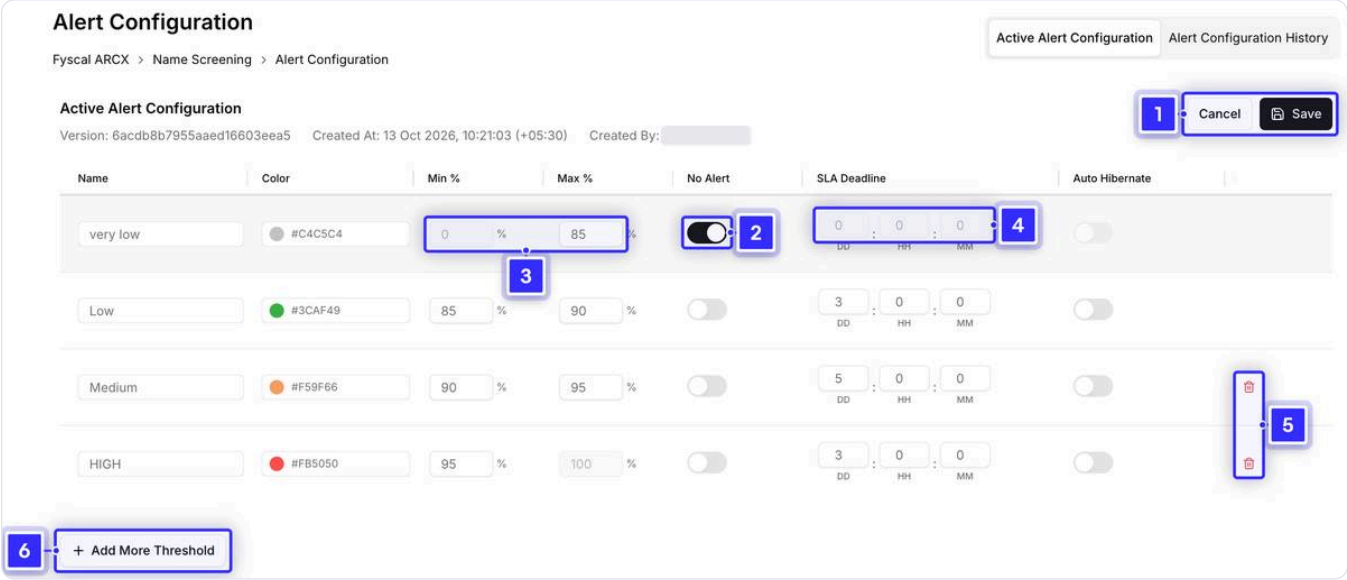


Figure 7.17 Alert Configuration in edit mode: Cancel and Save (1), the No Alert switch (2), Min % and Max % (3), the SLA Deadline fields (4), the delete icons (5) and Add More Threshold (6)

1. **Cancel** and **Save** take the place of **Edit**.
2. **No Alert** is a switch, shown on for the very low band.
3. **Min %** and **Max %** are number fields. The first band's Min % (0) and the last band's Max % (100) are greyed out.
4. **SLA Deadline** has three fields: **DD**, **HH** and **MM**. On the band with No Alert switched on, these fields and the **Auto Hibernate** switch are greyed out.
5. A red delete icon appears at the end of the Medium and HIGH rows.
6. **Add More Threshold** adds a band.

> **Step 1** **Open the edit form**
> On the **Active Alert Configuration** tab, click **Edit**.

> **Step 2** **Change the bands**
> For each band, set the **Name**, the **Color**, **Min %** and **Max %**, the **No Alert** switch, the **SLA Deadline** (DD : HH : MM) and the **Auto Hibernate** switch. Click **Add More Threshold** to add a band, or a band's delete icon to remove it.

> **Step 3** **Save or cancel**
> Click **Save** to keep your changes, or **Cancel** to discard them.

Alert Configuration History

Open the **Alert Configuration History** tab to see every saved version. The table has the columns **Config Version ID** (with a copy icon), **Status**, **Created** and **Created by**. One version is **ACTIVE** and the rest are **INACTIVE**. In Figure 7.18 there are 10 versions (**Showing 1-10 of 10**), newest first.

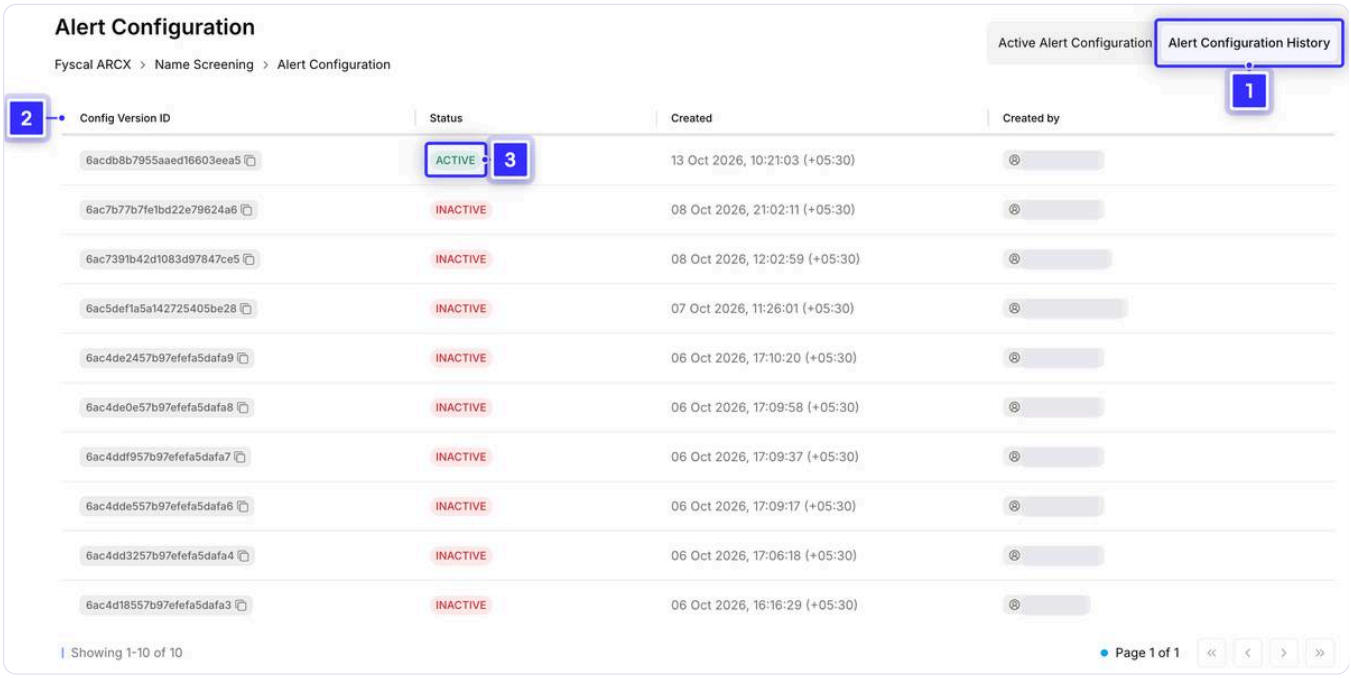


Figure 7.18 Alert Configuration History: the tab (1), the columns (2) and the ACTIVE version (3), followed by nine INACTIVE versions; names hidden

Screening Configuration

Fyscal ARCX → Name Screening → Configuration → Screening

Use Screening Configuration to review or change how much weight each field and sub-field carries in screening. Screening Configuration holds the weightages of the screening fields and of their sub-fields. The Manual Screening form shows the active version's ID and weightages. The page has two tabs: **Active Configuration** and **Configuration History**.

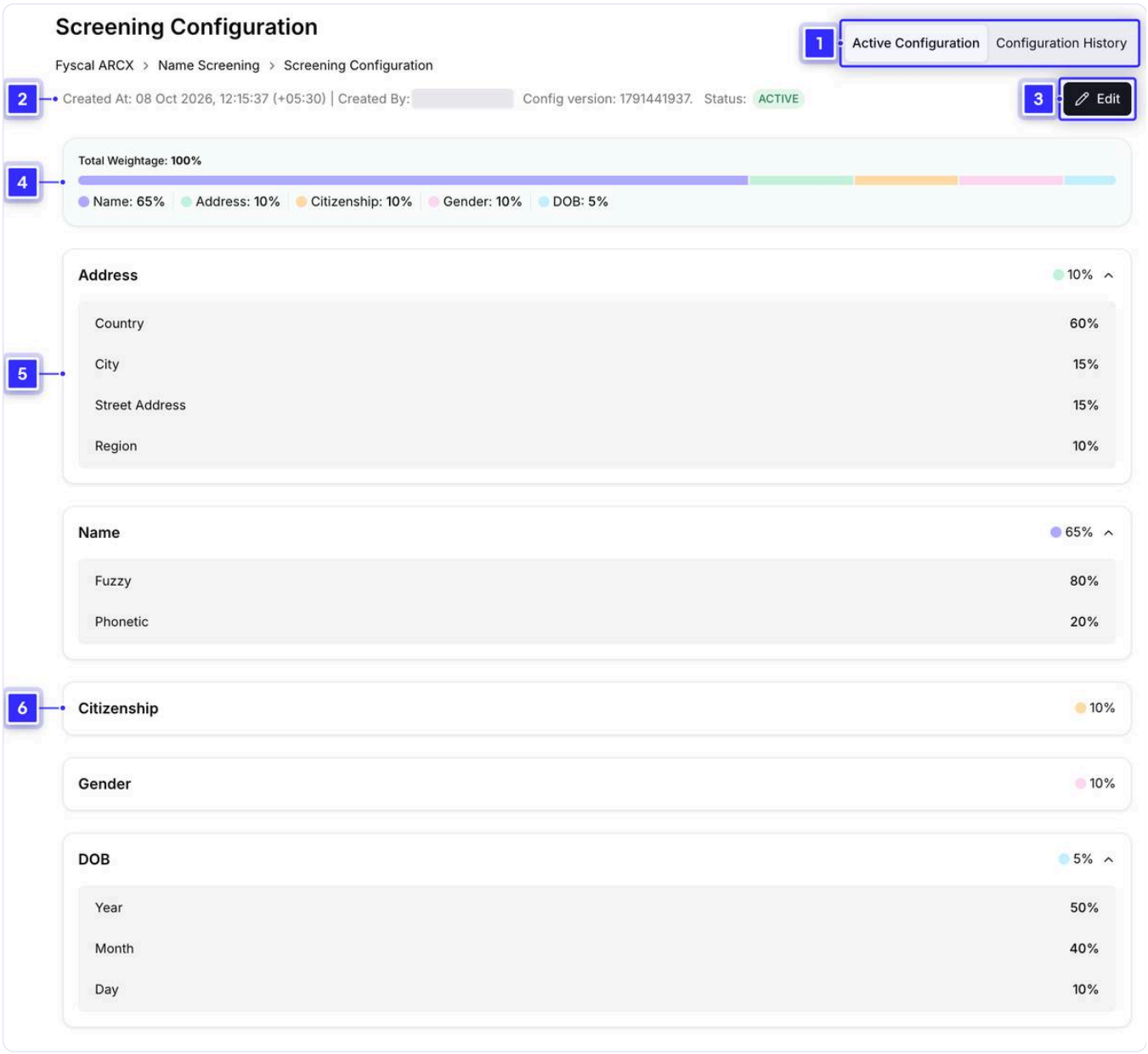


Figure 7.19 Active Configuration: the tabs (1), the version details (2), Edit (3), the Total Weightage bar (4), a field card with sub-fields, Address (5), and a field with no sub-fields, Citizenship (6)

1. The tabs **Active Configuration** and **Configuration History**.
2. The active version: **Created At** (08 Oct 2026, 12:15:37 (+05:30)), **Created By** (hidden in the figure), **Config version** (1791441937) and **Status ACTIVE**.
3. **Edit** switches the page into the edit form.
4. **Total Weightage: 100%**: a bar showing each field's share in its own colour.
5. A field card. **Address**, **Name** and **DOB** have a chevron and list their sub-fields below.
6. **Citizenship** and **Gender** have no sub-fields.

The active configuration in Figure 7.19:

Field	Weightage	Sub-fields
Name	65%	Fuzzy 80%, Phonetic 20%
Address	10%	Country 60%, City 15%, Street Address 15%, Region 10%
Citizenship	10%	None
Gender	10%	None
DOB	5%	Year 50%, Month 40%, Day 10%

In this configuration, the field weightages add up to 100%. Within each of Address, Name and DOB, the sub-field weightages also add up to 100%.

AML context

Fuzzy matching finds names that are spelled differently, and phonetic matching finds names that sound alike, for example after transliteration from another script. Both widen the net, so common names produce many candidates. Date of birth, nationality and address are what tell those candidates apart.

Note

The weightages shown on an alert's match candidates can differ from the ones on this page (see Review a name-screening match).

Edit the screening configuration

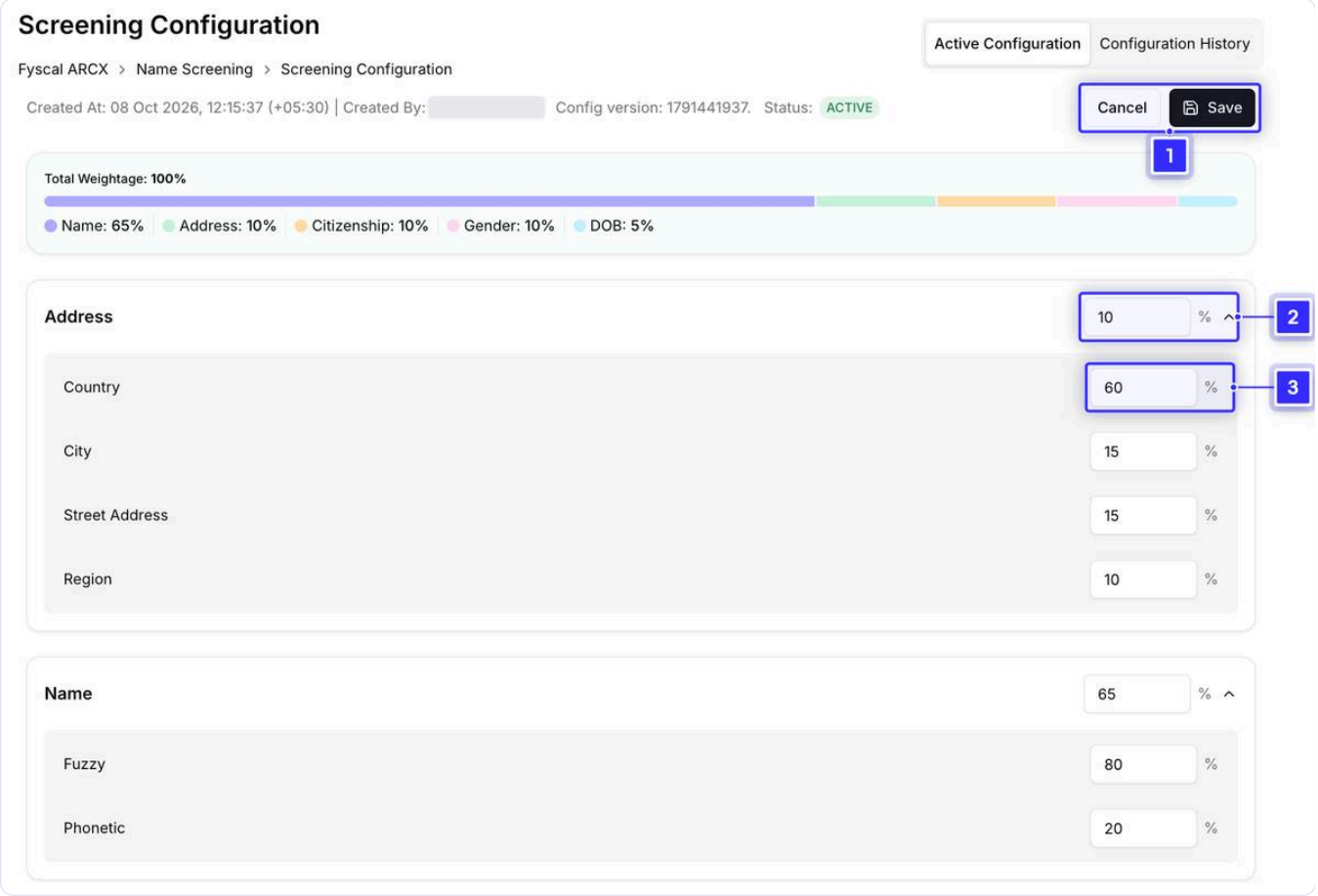


Figure 7.20 Screening Configuration in edit mode: Cancel and Save (1), a field's weightage field, Address (2), and a sub-field's weightage field, Country (3)

1. **Cancel** and **Save** take the place of **Edit**.
2. Each field's weightage becomes a number field with a **%** sign.
3. Each sub-field's weightage becomes a number field too.

Step 1 Open the edit form

On the **Active Configuration** tab, click **Edit**.

Step 2 Change the weightages

Type the new percentages for **Address**, **Name**, **Citizenship**, **Gender** and **DOB**, and for the sub-fields of Address (Country, City, Street Address, Region), Name (Fuzzy, Phonetic) and DOB (Year, Month, Day).

Step 3 Save or cancel

Click **Save** to keep your changes, or **Cancel** to discard them.

Configuration History

Open the **Configuration History** tab to see every saved version. The table has the columns **Config Version ID** (with a copy icon), **Status** (**ACTIVE** or **INACTIVE**), **Created** and **Created by**, newest first. The example environment holds 105 versions, 20 per page (**Showing 1-20 of 105**, **Page 1 of 6**).

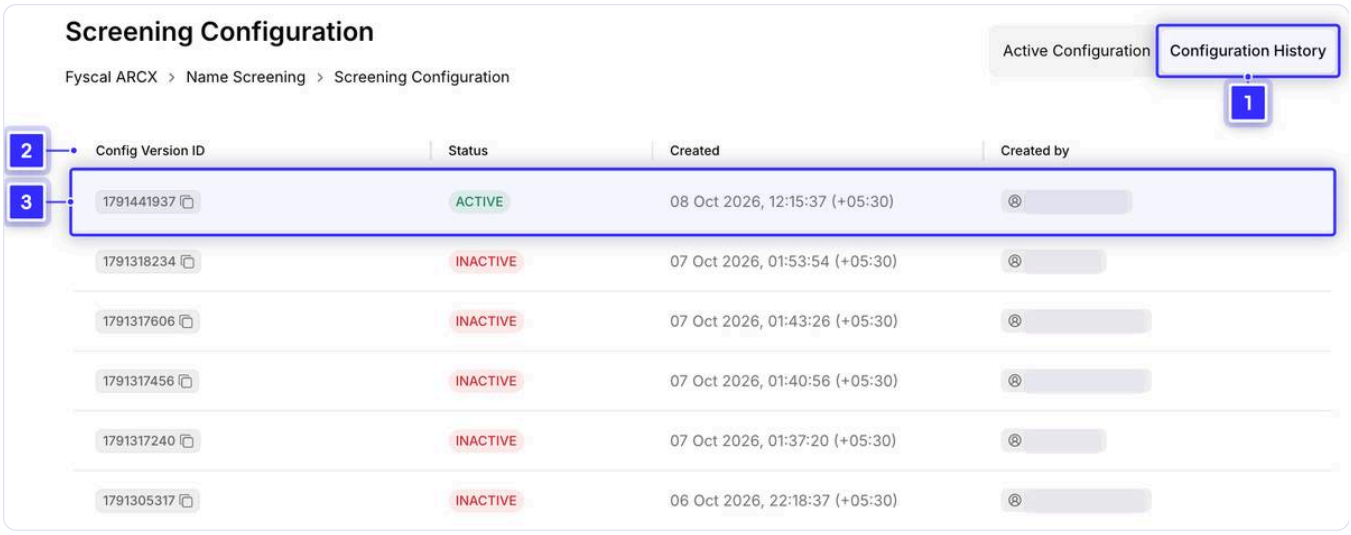


Figure 7.21 Configuration History: the tab (1), the columns (2) and the ACTIVE version 1791441937 (3), followed by INACTIVE versions; names hidden

Review a name-screening match

Fyscal ARCX → Case Manager → Alerts → a Name Screening alert → Matches

WHO	WHERE	DECISION	RECORDED WITH
The analyst working the alert or case	Alert Details or Case Details → Matches	True Match, False Match or Potential Match	A Rationale Code and Rationale Details (at least 10 characters)

Screening finds watchlist records that may be your customer. The analyst decides whether each one is. The **Matches** panel puts the customer's values next to each watchlist candidate's values, field by field, with a **Weightage** and a **Score** for each field and a band and percentage for the candidate. The panel is described in Customer, accounts and matches, and the decision is recorded with **Dispose Alert** (see Dispose alerts and close a case).

What the dispositions mean for you

The **Disposition** list offers three values. The screen does not define them; the table gives their usual meaning in screening review. Your institution's procedures set what each one requires.

Disposition	Usual meaning in screening review
True Match	The watchlist record is your customer: the name matches and the other identifiers agree. In the examples, a Closed case with this disposition shows **File STR** (see File an STR).
False Match	The watchlist record is someone else: the names are only alike, or an identifier such as date of birth or nationality clearly conflicts.
Potential Match	The record may be your customer, but the evidence is not enough to confirm or rule it out, for example because the record has no date of birth.

Decide on a match

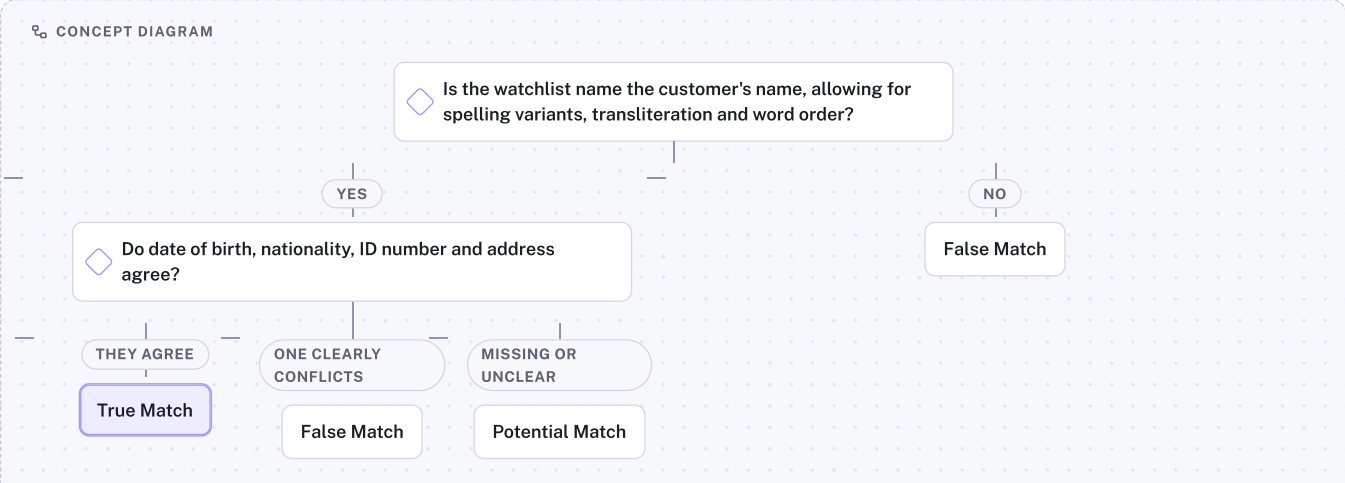


Diagram 7.2 — Deciding a name-screening match

Diagram 7.2 is a general review aid, not product logic. Start with the name. If it is not the customer's name, the candidate is a False Match. If it is, compare the secondary identifiers. Agreement points to a True Match and a clear conflict to a False Match. When identifiers are missing on either side, look for more evidence in the **Identity** and **Additional Information** tabs, such as aliases and ID numbers, before you settle on Potential Match.

Example: reading a candidate

Alert ALT-NS-05102026-000115 for Ramon Michael Castillo Tan is banded **LOW 84.29%** and has two candidates (see Alert Details: Name Screening). The first candidate, UID 4880431, shows:

Field	Customer	Candidate (UID 4880431)	Weightage	Score
Name	Ramon Michael Castillo Tan	MICHAEL TAN	73%	90%
Nationality	Philippines	PHILIPPINES	11%	100%
Date of Birth	Provided	-	0%	0%
Address	Provided	A different city	12%	27%
Entity Type	INDIVIDUAL (MALE)	M (M)	0%	0%

Read with Diagram 7.2: the name is close and the nationality agrees, but the record has no date of birth to compare and the address is in a different city. The identifiers are partly missing and partly different, so this candidate cannot be confirmed from the Matches panel alone. The second candidate, RAMON TAN (UID 7134045, **LOW 82.6%**), needs the same review. The alert in the example is **Not Started** and has no disposition yet.

> **Note**
> The field weightages shown on this alert (Name 73%, Nationality 11%, Address 12%) differ from the active Screening Configuration (Name 65%, Address 10%, Citizenship 10%, Gender 10%, DOB 5%), and the weightages and scores on screen do not by themselves give 84.29%. Use the per-field scores to see where the candidate agrees and differs, not to recalculate the percentage.

RELATED IN DETECTION & MONITORING

Transaction Monitoring | Typology Library | Data Ingestion

DETECTION & MONITORING

8 Transaction Monitoring

Fyscal ARCX → Transaction Monitoring

Transaction Monitoring is where you build and run the rules that scan transactions for suspicious patterns. A rule is called a **typology**; it is made of conditions on reusable calculations called **variables**, and it runs on a **schedule**. Compliance analysts and rule owners use the three pages under the menu: **Typology**, **Variables** and **Schedules**.

FOR	IN THE MENU	READING TIME
Compliance analysts and rule owners	Fyscal ARCX → Transaction Monitoring	About 43 min

The main example in this chapter is the typology **High volume and Value outgoing Remittances** (**TMR-01072026-000463**). For ready-made rules you can build with the same screens, see the Typology Library.

- **Typologies**: Typology list, Filter and sort the list, Typology detail, Schedule Details and the Create Typology form.
- **Variables**: Variables list, View Variable and Create a variable.
- **Schedules**: Run History and Schedule List.
- **Build a typology from scratch**: the walkthrough in seven parts (1, 2, 3, 4, 5, 6, 7), then How conditions are evaluated.

Typology list

Fyscal ARCX → Transaction Monitoring → Typology

The **Transaction Monitoring Typologies** page lists every typology (rule) with its status and category. Start here to find a rule, open it, or create a new one.

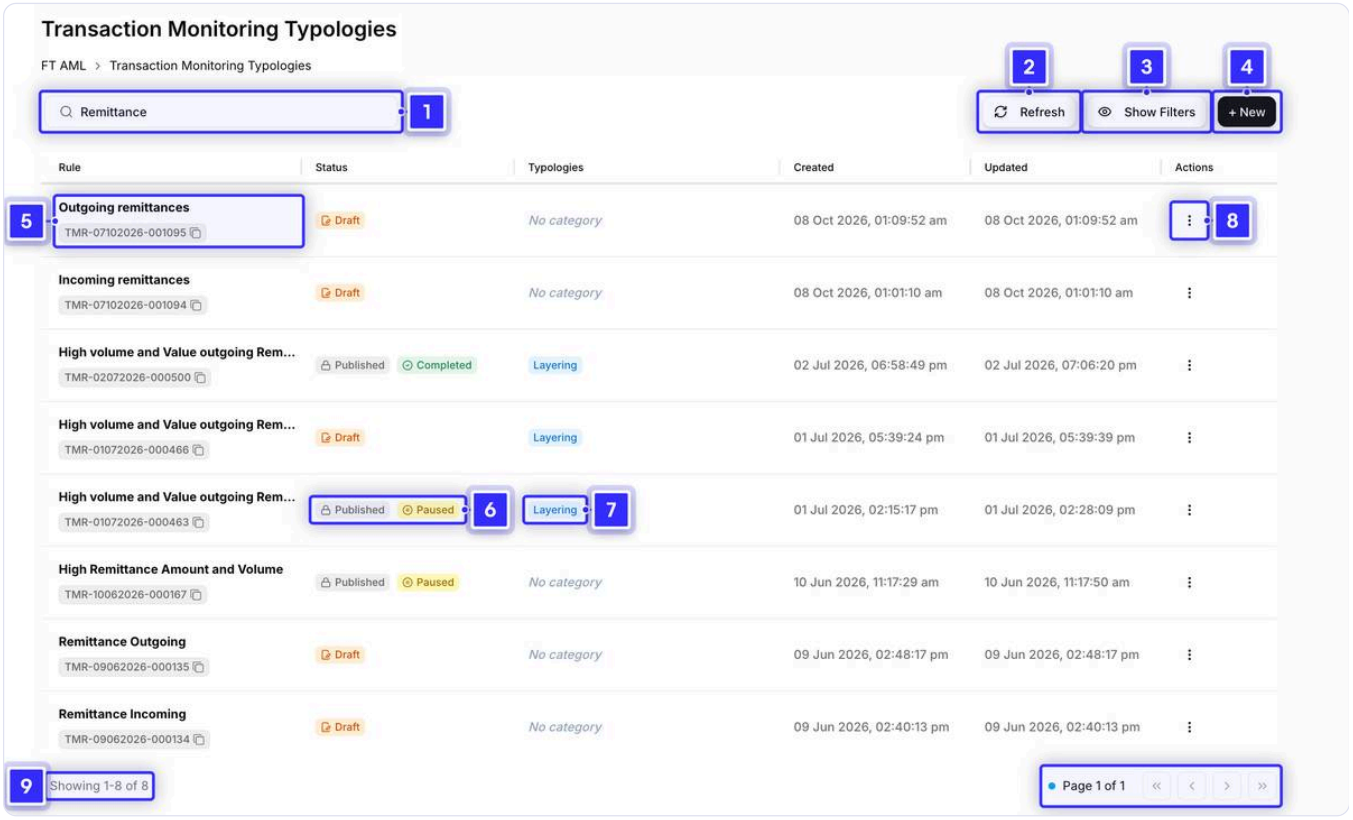


Figure 8.1 The typology list searched for Remittance: search (1), Refresh (2), Show Filters (3), + New (4), a rule and its ID (5), status chips (6), typology type (7), the row menu (8) and the count (9)

1 **Search by rule name and id**: type part of a rule name or a rule ID such as TMR-01072026-000463. Here “Remittance” finds 8 rules.

2. **Refresh**: reloads the list.
3. **Show Filters**: opens the filter bar (the button then reads **Hide Filters**). See Filter and sort the list.
4. **+ New**: opens **Create Typology** (see Create Typology form).
5. **Rule**: the rule name, with its rule ID in a chip below it. The chip has a copy icon.
6. **Status**: Draft, Published or Shadow, with a run-state chip such as **Paused** or **Completed** beside it.
7. **Typologies**: the typology type chosen for the rule, or *No category* when none was chosen.
8. **Actions**: the ⋮ menu for the row.
9. Pagination: **Showing 1-8 of 8** and **Page 1 of 1**, with first, previous, next and last buttons. Without a search the list shows 10 rules per page.

Column	What it shows
Rule	Rule name (long names are shortened with ...) and rule ID, for example TMR-06102026-001090.
Status	The rule's status chip: Draft, Published or Shadow.
Typologies	The typology type, for example Anomaly, Structuring, Cardinality, Velocity, Large Transaction, SMURFING; *No category* if none.
Created	Date and time the rule was created, for example 06 Oct 2026, 10:55:47 am.
Updated	Date and time of the last change.
Actions	⋮ menu with row actions.

Statuses and run state

Value	Where it appears	Meaning as shown on screen
Draft	Status	A saved rule that has not been activated. New rules are saved as Draft.
Shadow	Status	Activated in Shadow Mode: “Alert generated against live data will be shown in rule detail page.”
Published	Status	Activated in Published Mode: “Alert from this rule will flow into Alert Manager.”
Paused	Chip beside the status, in the list and on the rule's page	The rule is not currently running; the page offers **Resume**.
Completed	Chip beside the status, in the list	The rule's schedule has passed its **End Time**, so no further runs are planned.

> **Note**
> Some Transaction Monitoring screens use other names than the rest of Fyscal ARCX. The breadcrumb of the typology pages reads **FT AML** → **Transaction Monitoring Typologies**, and the Variables page breadcrumb reads **Transaction Monitoring Rules**. The **Activation Mode** dialog describes Published Mode as “Alert from this rule will flow into Alert Manager.” This guide quotes those labels as they appear.

> **AML context**
> A typology is a known pattern of money-laundering or terrorist-financing behaviour, such as structuring, rapid movement of funds or use of mule accounts, written as conditions that can be measured on transactions. Institutions usually set the thresholds from their own risk assessment, test a rule before it raises alerts, and review it periodically.

Filter and sort the list

Fyscal ARCX → Transaction Monitoring → Typology → Show Filters

The filter bar has two filters and a sort control.

Step 1 **Open the filter bar**

Click **Show Filters**. Three controls appear below the search box: **All Typologies** (1), **All Statuses** (2) and **Sort By** (3). The button now reads **Hide Filters** (4).

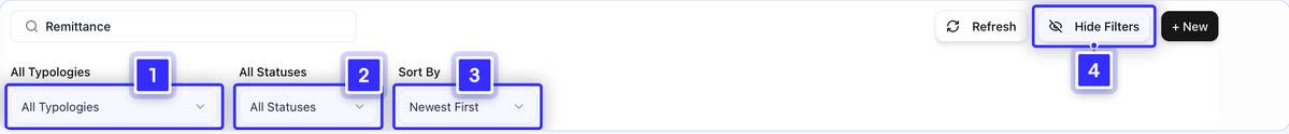


Figure 8.2 The filter bar: All Typologies (1), All Statuses (2) and Sort By (3), with Hide Filters (4)

Step 2 **Filter by typology type**

Open **All Typologies** (1) and choose a type from the list (2). The list shows the types in use, for example SMURFING, Mule Networks, Layering, High Value, High Value Transfer, Support, Structuring and identical transactions; some names appear twice because two types were created with the same name. Scroll the list with the arrow at the bottom (3) for more, such as Anomaly, Cardinality, Large Transaction and Velocity.

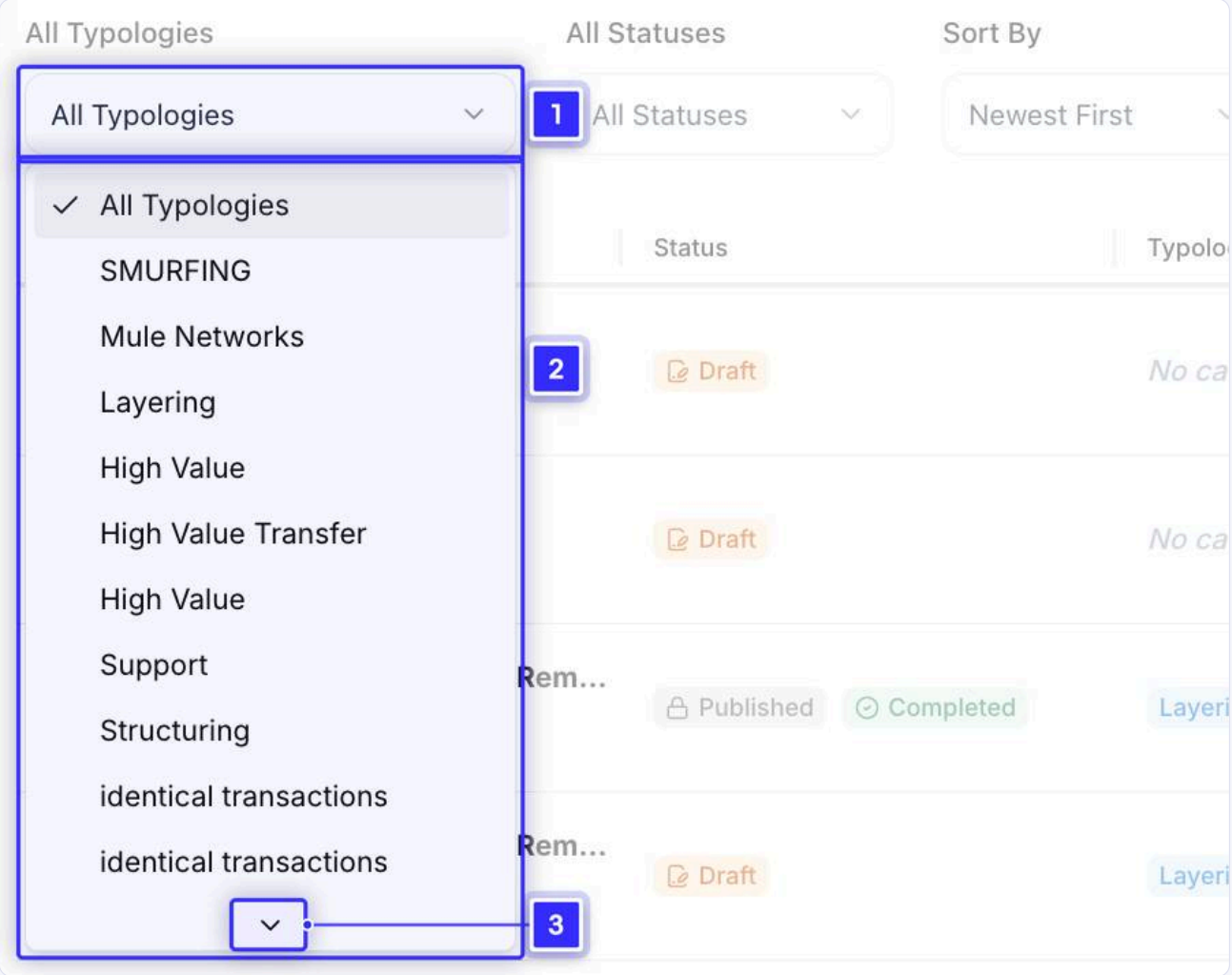


Figure 8.3 All Typologies (1) open: the list of typology types (2) and the scroll arrow (3)

Step 3 **Filter by status**

Open **All Statuses** (1) and choose **Draft**, **Published** or **Shadow** from the list (2). Choose **All Statuses** to clear the filter.

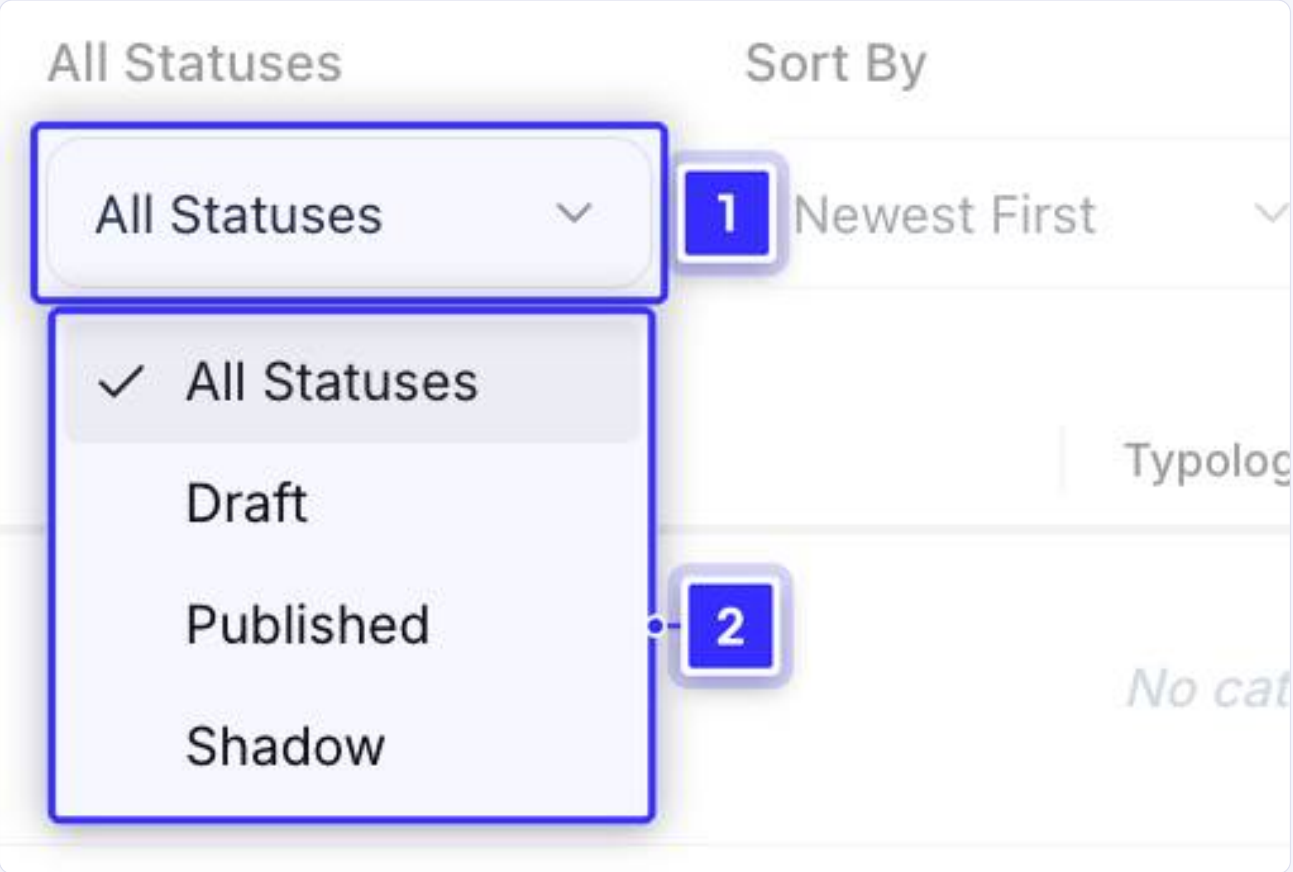


Figure 8.4 All Statuses (1) open: All Statuses, Draft, Published and Shadow (2)

Step 4 **Sort the list**

Open **Sort By** and choose **Newest First** (the default) or **Oldest First**.

Step 5 **Use the row menu**

Click ⋮ (2) in the **Actions** column. On a **Draft** rule (1) the **Actions** menu offers **Duplicate** (3), which makes a copy of the rule.



Figure 8.5 The Actions menu (2) on a Draft rule (1): Duplicate (3)

Typology detail

Fyscal ARCX → Transaction Monitoring → Typology → (click a row)

Click a row to open the typology's page. It shows the rule read-only: its status, timing, condition groups and the variables it uses. The example below is a Published rule that is currently Paused.

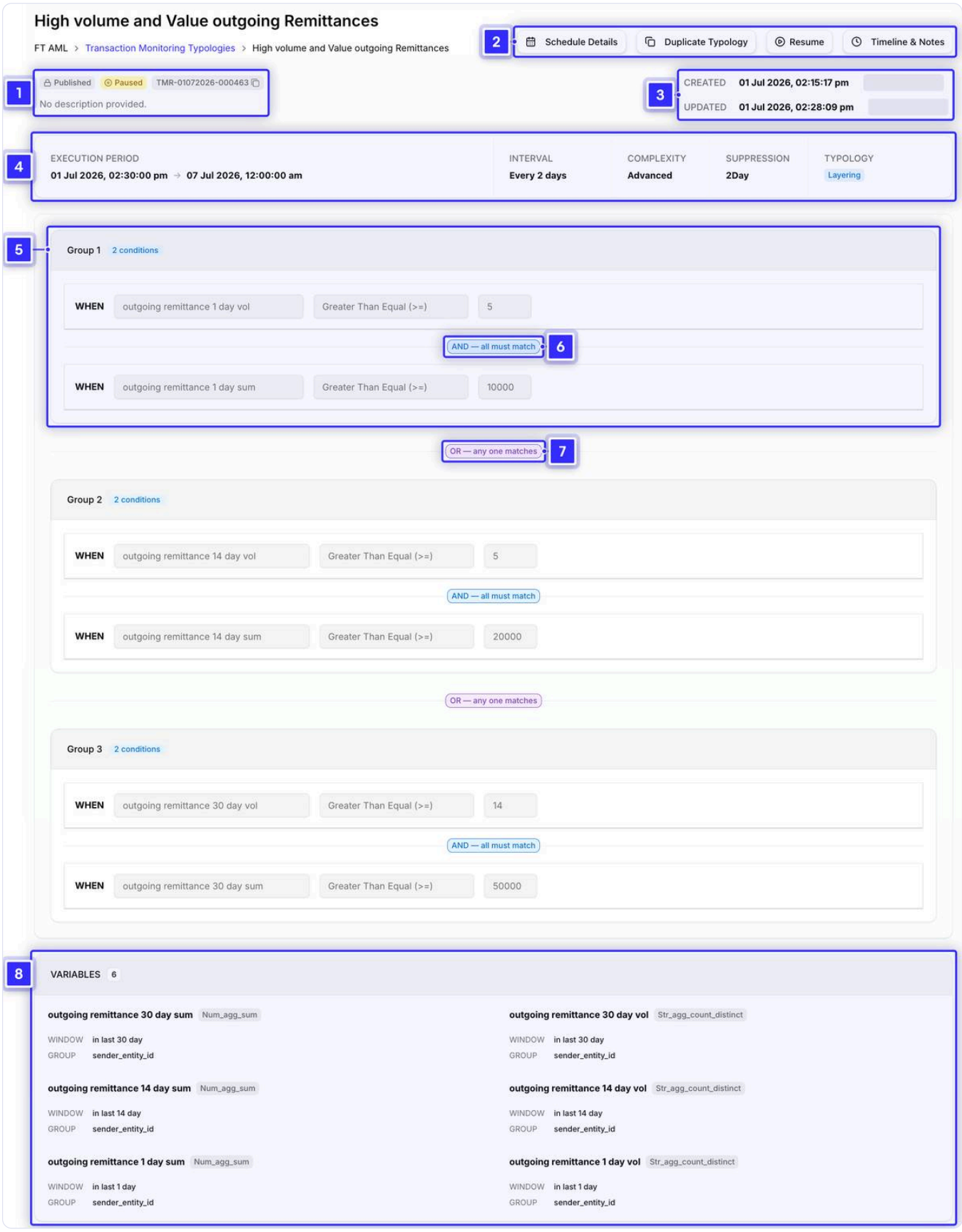


Figure 8.6 Typology detail for High volume and Value outgoing Remittances (TMR-01072026-000463): Published, Paused, three condition groups and six variables

1. Status chips (**Published**, **Paused**), the rule ID with a copy icon, and the description (here “No description provided.”).
2. Page actions: **Schedule Details** (the rule's run history, see Schedule Details), **Duplicate Typology**, **Resume** (shown because the rule is paused) and **Timeline & Notes**.
3. **CREATED** and **UPDATED**: date, time and the user.

4. Summary strip: **EXECUTION PERIOD** (01 Jul 2026, 02:30:00 pm → 07 Jul 2026, 12:00:00 am), **INTERVAL** (Every 2 days), **COMPLEXITY** (Advanced), **SUPPRESSION** (2Day) and **TYPOLOGY** (Layering).
5. A condition group, with its number of conditions (**2 conditions**). Each row reads **WHEN** variable, operator, value.
6. **AND — all must match**: the link between conditions inside a group.
7. **OR — any one matches**: the link between groups.
8. **VARIABLES** with a count (6): one card per variable, showing its type, **WINDOW** and **GROUP**.

The three groups of the example read as follows. The rule alerts on a sender when any one group is fully true.

Group	Condition 1		Condition 2
1	outgoing remittance 1 day vol **Greater Than Equal (>=)** 5	AND	outgoing remittance 1 day sum **Greater Than Equal (>=)** 10000
2	outgoing remittance 14 day vol **Greater Than Equal (>=)** 5	AND	outgoing remittance 14 day sum **Greater Than Equal (>=)** 20000
3	outgoing remittance 30 day vol **Greater Than Equal (>=)** 14	AND	outgoing remittance 30 day sum **Greater Than Equal (>=)** 50000

Variable	Type	WINDOW	GROUP
outgoing remittance 30 day sum	Num_agg_sum	in last 30 day	`sender_entity_id`
outgoing remittance 30 day vol	Str_agg_count_distinct	in last 30 day	`sender_entity_id`
outgoing remittance 14 day sum	Num_agg_sum	in last 14 day	`sender_entity_id`
outgoing remittance 14 day vol	Str_agg_count_distinct	in last 14 day	`sender_entity_id`
outgoing remittance 1 day sum	Num_agg_sum	in last 1 day	`sender_entity_id`
outgoing remittance 1 day vol	Str_agg_count_distinct	in last 1 day	`sender_entity_id`

Step 1 **See how a variable is calculated**

Click a variable card. A popup shows the variable's name, its type (1), a **DESCRIPTION** (2) of the calculation, its **WINDOW** (3) and its **GROUP** (4). For **outgoing remittance 30 day sum** the description reads *NUM_AGG_SUM(amount), type STR_EQ REMITTANCE, grouped by sender_entity_id, window: (now() - INTERVAL 30 DAY, now())*: the sum of `amount` for transactions whose type equals REMITTANCE, per sender, over the last 30 days. Click × (5) to close.

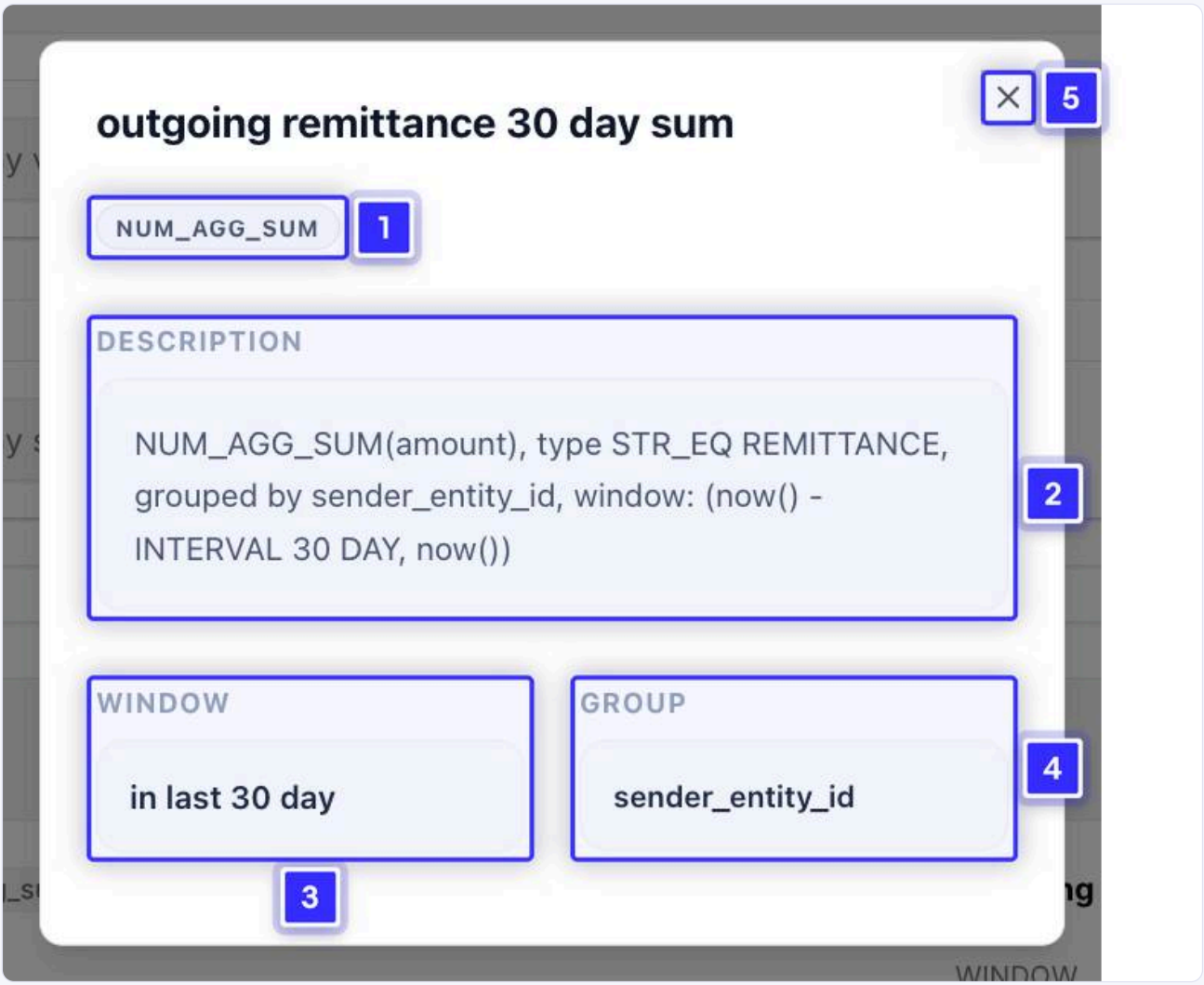


Figure 8.7 Variable popup for outgoing remittance 30 day sum: type (1), description (2), window (3), group (4) and close (5)

Step 2 **Read or add notes**

Click **Timeline & Notes**. The **Activity Timeline** panel opens with the rule ID, an **ADD A NOTE** box (1), **Attach File** (2) and **Add note** (3). Events for the rule are listed below (4); for this rule the panel shows *No activity found.* Click × (5) to close.

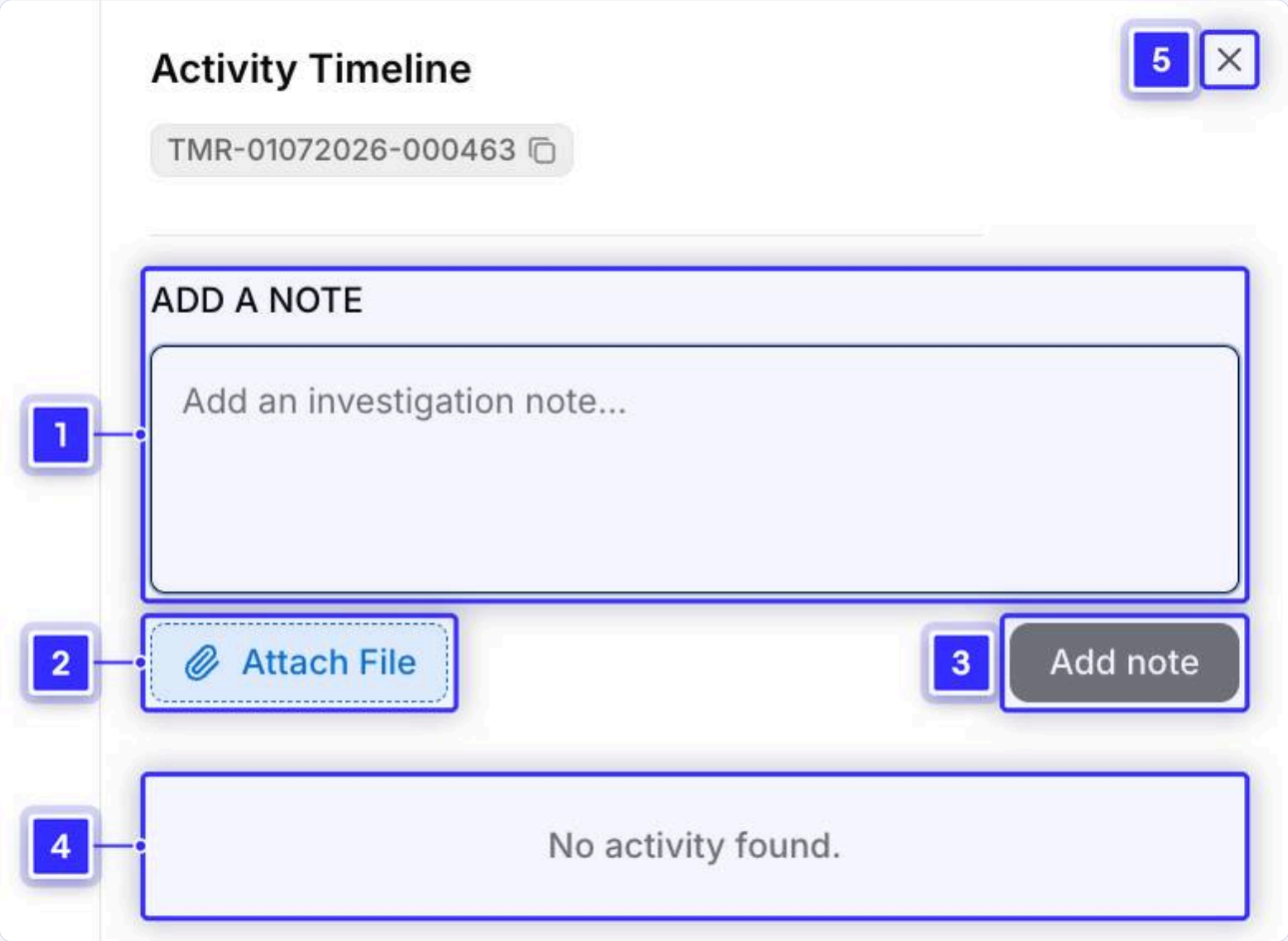


Figure 8.8 Activity Timeline for TMR-01072026-000463: note box (1), Attach File (2), Add note (3), events (4) and close (5)

Note

The buttons at the top depend on the rule's state. On this Paused, Published rule they are **Schedule Details**, **Duplicate Typology**, **Resume** and **Timeline & Notes**. A Draft rule's page offers **Delete**, **Update**, **Duplicate Typology**, **Activate** and **Timeline & Notes**. The condition fields are read-only on this page.

Schedule Details (a typology's run history)

Fyscal ARCX → Transaction Monitoring → Typology → (rule) → Schedule Details

Schedule Details lists every run of one typology. The breadcrumb links back to the list and to the rule.

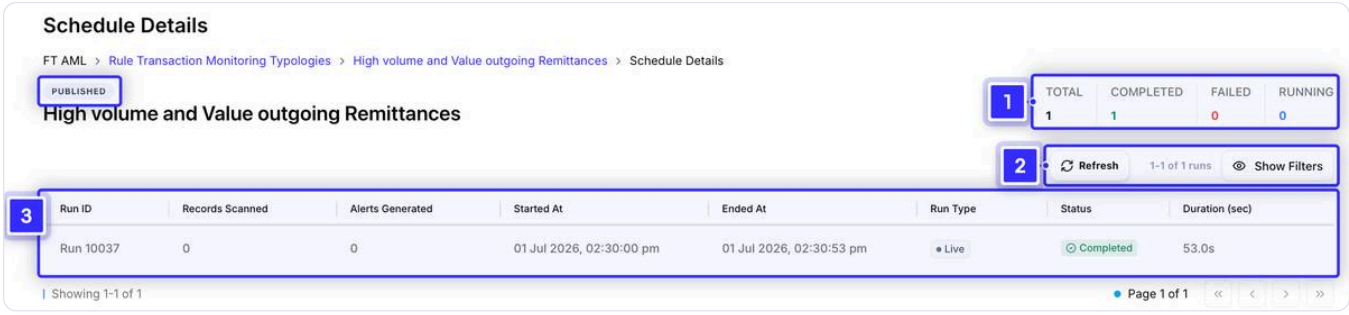


Figure 8.9 Schedule Details for High volume and Value outgoing Remittances: run totals and one completed live run

1. Totals: **TOTAL**, **COMPLETED**, **FAILED** and **RUNNING** runs (1, 1, 0, 0 here). The rule's status (**PUBLISHED**) is shown above its name.
2. **Refresh**, the run count (**1-1 of 1 runs**) and **Show Filters**.

3 The runs table.

Column	What it shows	Example
Run ID	Identifier of the run	Run 10037
Records Scanned	Records the run read	0
Alerts Generated	Alerts the run raised	0
Started At / Ended At	Start and end date and time	01 Jul 2026, 02:30:00 pm / 02:30:53 pm
Run Type	How the rule ran	Live
Status	Outcome of the run	Completed
Duration (sec)	Run length	53.0s

> **Note**
> A run with **Records Scanned** 0 had no transaction data to read in its window. Check data ingestion for that period before judging the rule.

Create Typology form

Fyscal ARCX → Transaction Monitoring → Typology → + New

+ New opens **Create Typology**. The first page holds the rule's details and its conditions; **Next Step** goes to the schedule page (Part 5 of the walkthrough).

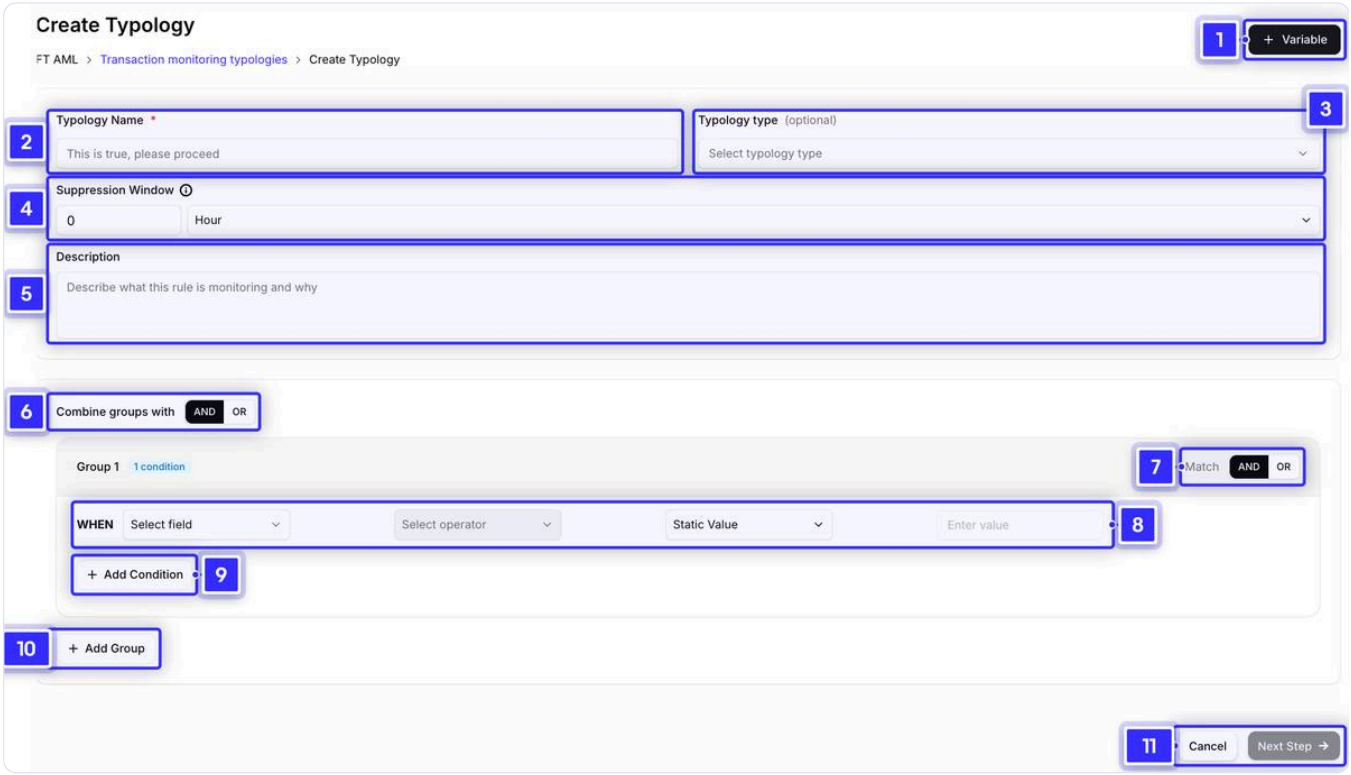


Figure 8.10 Create Typology, first page: details, Combine groups with, Group 1 and its first condition row

1. **+ Variable**: creates a variable without leaving the form (opens **Create Variables**).
2. **Typology Name** (required).
3. **Typology type** (optional).
4. **Suppression Window**: a number and a unit.
5. **Description**.
6. **Combine groups with**: **AND** or **OR**.
7. **Match**: **AND** or **OR** for the conditions inside this group.
8. A condition row: **WHEN**, field, operator, value type and value.

9. **Add Condition**: adds a row to this group.
10. **Add Group**: adds another group.
11. **Cancel** and **Next Step**. **Next Step** stays greyed out until the required details and conditions are complete.

Field	What it expects	Required	Options or format
Typology Name	The rule's name as it will appear in the list	Yes (*)	Free text
Typology type	The category the rule is filed under; it is what the **All Typologies** filter uses	No (optional)	**Select typology type**; each type shows a short code, for example Structuring (TP100), Anomaly (TP103), Large Transaction (LT-01). The chosen type shows as a chip with ×.
Suppression Window	A time period set on the rule. An information icon (ⓘ) next to the label holds the field's help text.	No	A number (default 0) and a unit (default **Hour**; Day is also used, for example 30 Day)
Description	What the rule monitors and why	No	Free text; placeholder “Describe what this rule is monitoring and why”
Combine groups with	How groups combine	—	**AND** (default) or **OR**
Group Match	How conditions inside the group combine	—	**AND** (default) or **OR**
WHEN field	The variable to test	Yes	**Select field**: lists your variables
Operator	The comparison	Yes	**Select operator** (greyed until a field is chosen). Twelve operators, from Equal to Is Not Null; the full list is in the Part 3 field reference.
Value type	What the field is compared with	Yes	**Static Value** (default) or **Variable**; a third entry, **Ingested Data**, is shown greyed out
Value	The threshold	Yes	With **Static Value**: a number in **Enter value**. With **Variable**: a variable picker and a **THAN MULTIPLIER** box.

With **Variable** as the value type, the condition compares two variables, scaled by the multiplier. For example, in Rule 9 of the Typology Library the condition `sent_sum_7d_spike` **Greater Than Equal (>=)** Variable `sent_sum_90d` with **THAN MULTIPLIER** 0.5 means “the 7-day total is at least 0.5 × the 90-day total”. The rule page shows the compared variable as “sent_sum_90d (multiplied by 0.5)”.

When a group has more than one condition, the form shows **AND — all must match** or **OR — any one matches** between rows, following the group's **Match** setting. The same labels appear between groups, following **Combine groups with**. Each extra group has a **Remove** button and each extra row an ×. A worked example is in How conditions are evaluated.

Variables list

Fyscal ARCX → Transaction Monitoring → Variables

A variable is a named calculation, such as the number of transactions a sender made in the last 7 days. Typology conditions test variables, and one variable can be used by many typologies. The **Variables** page lists them all.

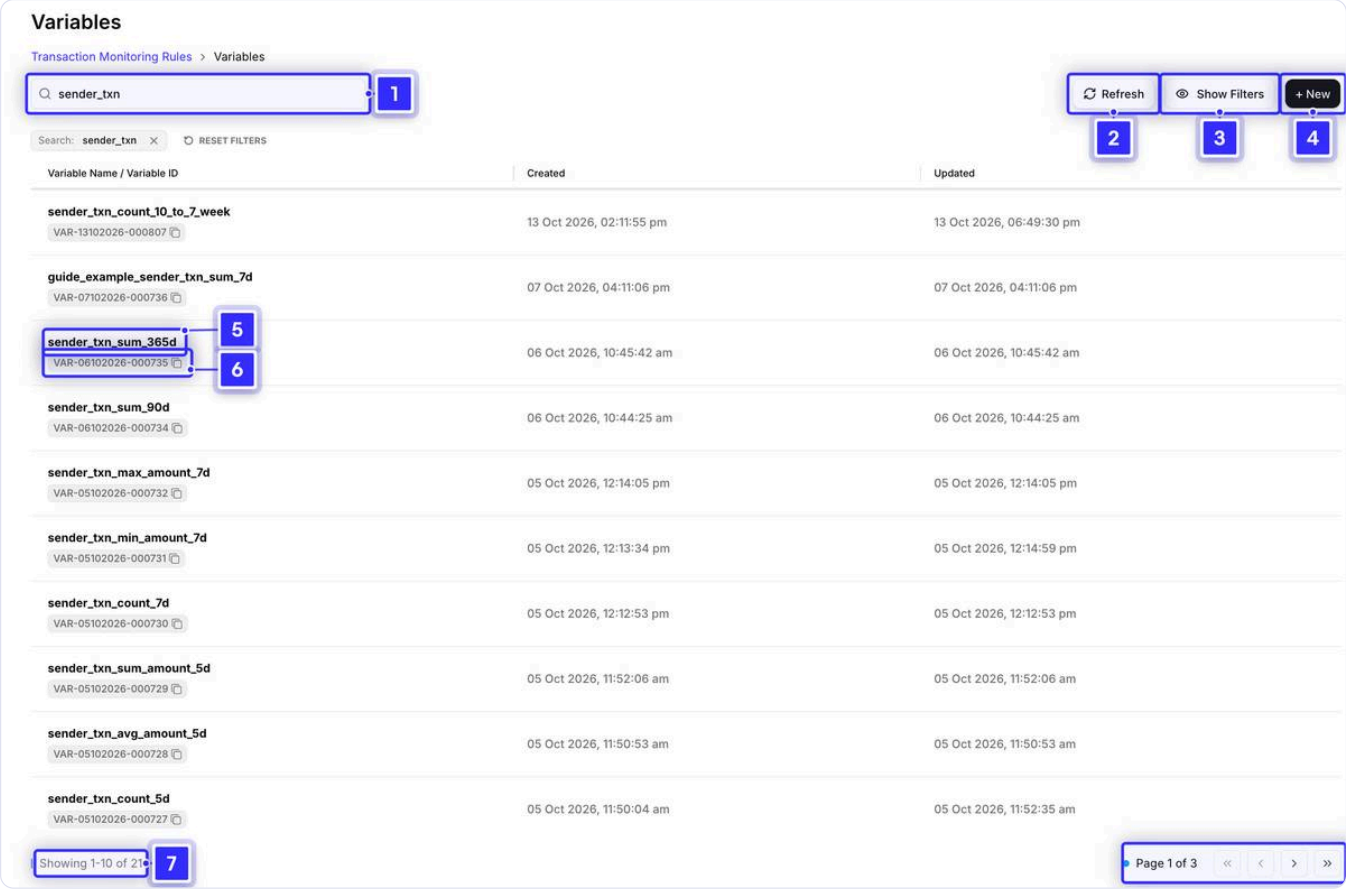


Figure 8.11 The Variables list searched for sender_txn: search (1), Refresh (2), Show Filters (3), + New (4), a variable name (5) and ID (6), and the count (7)

1. Search box (*variable name*). Here “sender_txn” finds 21 variables; the search also shows as a **Search:** chip with **RESET FILTERS** below the box.
2. **Refresh**.
3. **Show Filters**.
4. **+ New**: opens **Create Variables**.
5. **Variable Name / Variable ID**: the name, for example `sender_txn_sum_365d`, and its ID, for example VAR-06102026-000735.
6. The Variable ID chip, with a copy icon.
7. Pagination (**Showing 1-10 of 21**, **Page 1 of 3**).

Column	What it shows
Variable Name / Variable ID	Name and VAR-identifier
Created	Date and time created
Updated	Date and time last changed

Variable names in the product follow a pattern of subject, measure and window, for example `sender_txn_count_7d`, `sender_txn_sum_90d`, `sender_txn_max_amount_7d`, `sender_txn_avg_amount_5d`. Use the same pattern so variables are easy to find and reuse.

Step 1 **Sort the list**

Click **Show Filters**. A single **Sort By** control (1) appears (placeholder **Select Sort By**), and the button reads **Hide Filters** (2).

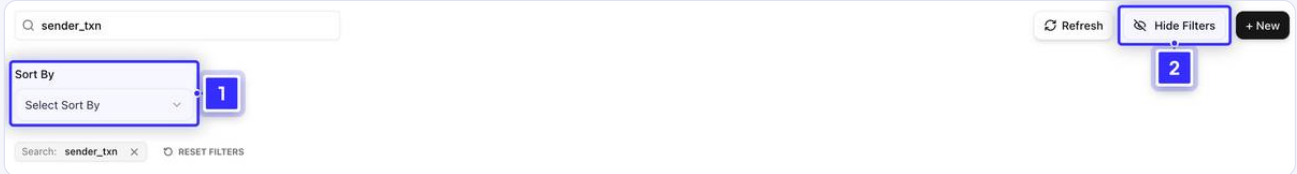


Figure 8.12 Variables with filters shown: Sort By (1) and Hide Filters (2)

View Variable

Fyscal ARCX → Transaction Monitoring → Variables → (click a row)

Click a variable to open **View Variable**. It shows the variable's definition and every rule that uses it.

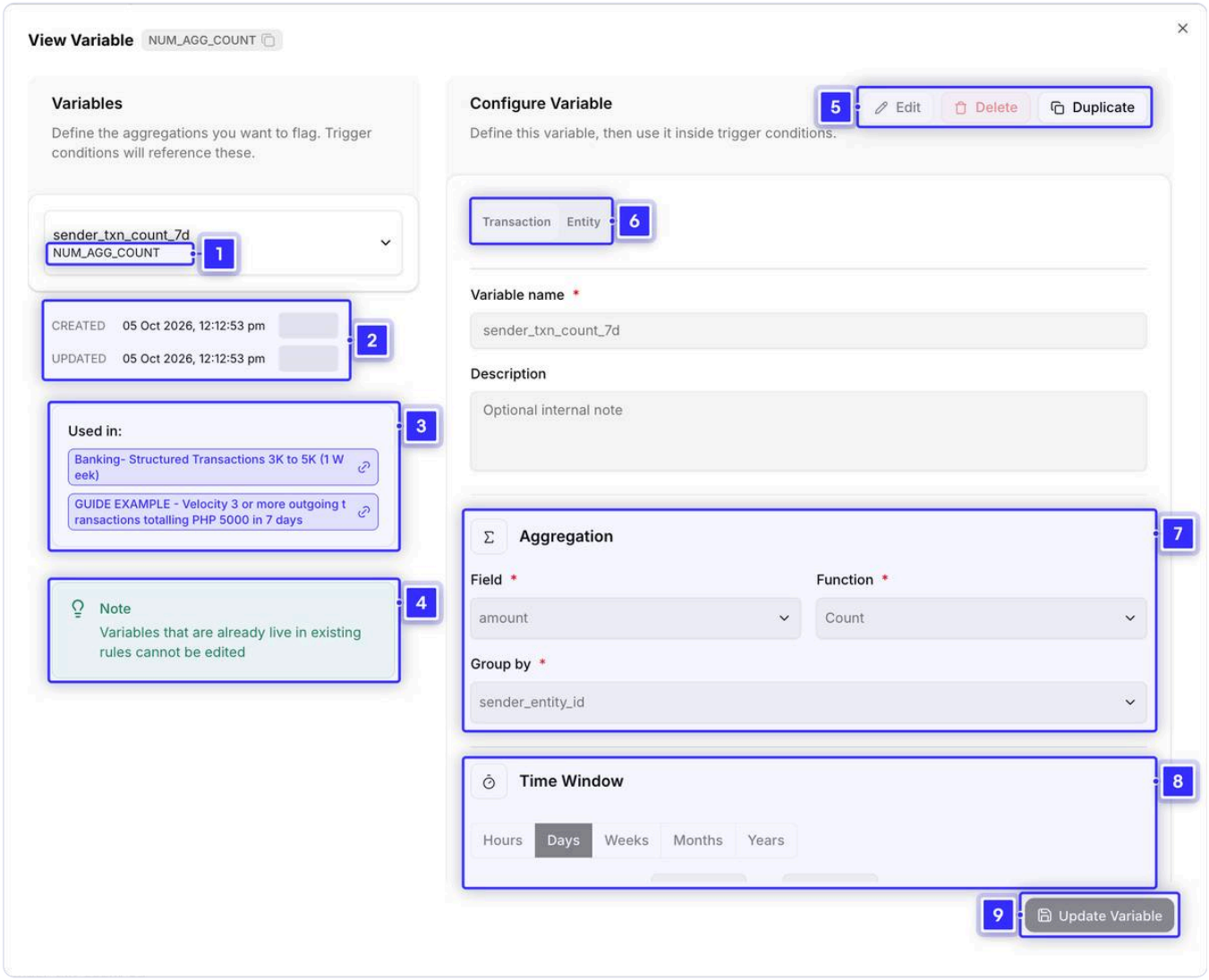


Figure 8.13 View Variable for sender_txn_count_7d (NUM_AGG_COUNT): used in two rules, so it cannot be edited

1. The variable type tag, here **NUM_AGG_COUNT**.
2. **CREATED** and **UPDATED**, with date, time and user.
3. **Used in:** each typology that uses the variable, as a link. Here: Banking- Structured Transactions 3K to 5K (1 Week), and the walkthrough's rule GUIDE EXAMPLE -Velocity (see Build a typology from scratch).
4. **Note:** "Variables that are already live in existing rules cannot be edited".
5. **Edit**, **Delete** and **Duplicate**. For this variable **Edit** and **Delete** are greyed out; **Duplicate** is available.
6. **Transaction** / **Entity**.
7. **Aggregation**: **Field** (`amount`), **Function** (Count), **Group by** (`sender_entity_id`).
8. **Time Window** (scroll down for the window and **Filters**).
9. **Update Variable** (greyed out).

> **Note**
> A variable that is used in a live rule cannot be changed in place. To change the calculation, click **Duplicate**, adjust the copy, save it under a new name, and point the rule at the new variable.

Create a variable

Fyscal ARCX → Transaction Monitoring → Variables → + New

+ New on the Variables page, or **+ Variable** on Create Typology, opens **Create Variables**.

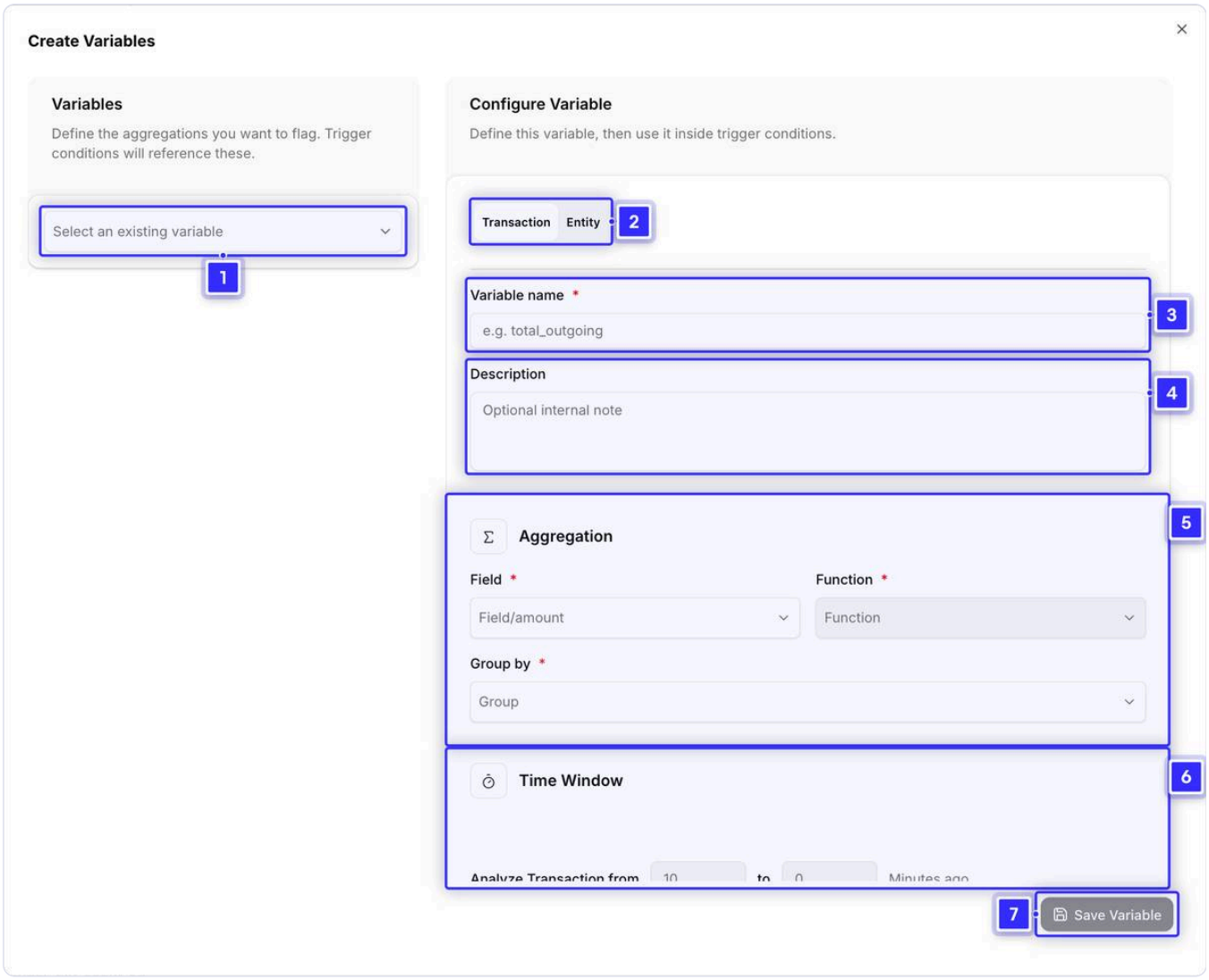


Figure 8.14 Create Variables: the empty form, with Select an existing variable on the left and Configure Variable on the right

1. **Select an existing variable**: pick a variable that already exists instead of creating a duplicate.
2. **Transaction** / **Entity**: whether the calculation is on transactions or entity data.
3. **Variable name** (required; placeholder “e.g. total_outgoing”).
4. **Description** (optional internal note).
5. **Aggregation**: **Field**, **Function** and **Group by**, all required.
6. **Time Window**, with **Filters** below it.
7. **Save Variable**.

Field	What it expects	Required	Options or format
Transaction / Entity	Data the variable is calculated from	—	Two tabs; **Transaction** is selected by default
Variable name	Unique name	Yes (*)	Free text, for example `sender_txn_sum_90d`
Description	Internal note	No	Free text
Field	The data field to calculate on	Yes (*)	Dropdown (placeholder Field/amount), for example `amount`, `receiver_amount`
Function	The calculation	Yes (*)	Depends on the field. A numeric field such as `amount` offers **Count**, **Count Distinct**, **Sum**, **Average**, **Minimum**, **Maximum**. An ID or text field such as `id` or `receiver_entity_id` offers only **Count**, **Count Distinct**, **Minimum**, **Maximum**. The variable's type tag follows the field and function, for example NUM_AGG_SUM, NUM_AGG_COUNT, STR_AGG_COUNT, STR_AGG_COUNT_DISTINCT.

Field	What it expects	Required	Options or format
Group by	Calculate separately for each value of this field	Yes (*)	Dropdown, for example `sender_entity_id` (one result per sender)
Time Window unit	Unit of the window	—	**Hours**, **Days**, **Weeks**, **Months**, **Years**
Analyze Transaction from … to … ago	Start and end of the window, counted back from the trigger time	—	Two number boxes followed by the unit and “ago”, for example from 90 to 0 Days ago
Filters (optional)	Restricts the calculation to matching transactions	No	**Add Filter** adds a row: **Field**, an operator (**Select field first**), a value, and **Static** or **Dynamic**. The heading counts the rows, for example **Filters (1)**.

Below the window boxes the form draws a timeline labelled, for example, **0 days ago** and **Triggered at T (00:00)**, with the sentence “This variable will be triggered time 00:00:00 on day T.” The window is measured back from T. The second box is the end of the window: **0** ends the window at T, so *from 90 to 0 Days ago* is the last 90 days. The end can also be above 0: *from 100 to 1 Days ago* covers the 100 days up to one day before T, and the form's timeline then reads **1 day ago**. The variable card on a typology page shows only the start (“in last 100 day”), so check the end on **View Variable**. The Typology Library's building blocks draw the windows side by side.

Filters are how a variable counts only some transactions. The variable **outgoing remittance 30 day sum** in the main example is a Sum of `amount` with a filter on type equal to REMITTANCE (its description reads *type STR_EQ REMITTANCE*).

Schedules: Run History

Fyscal ARCX → Transaction Monitoring → Schedules → Run History

A schedule sets when rules run: a name, an execution interval, a start time and an optional end time. One schedule can drive several rules. The **Schedules** page has two views, **Run History** and **Schedule List**. **Run History** logs every run of every schedule.

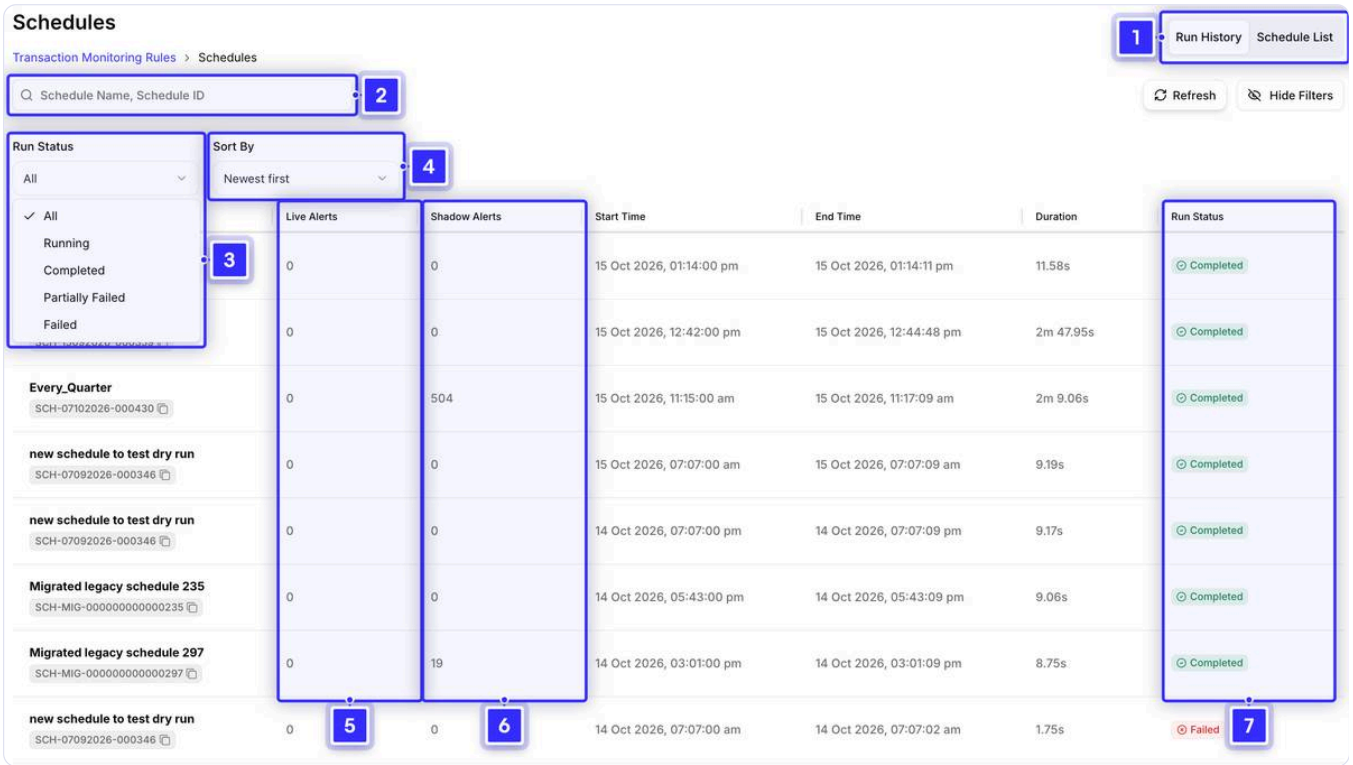


Figure 8.15 Schedules, Run History view, with the Run Status filter open

1. View switch: **Run History** / **Schedule List**.
2. Search (*Schedule Name, Schedule ID*).
3. **Run Status** filter: **All**, **Running**, **Completed**, **Partially Failed**, **Failed**.
4. **Sort By**: **Newest first** by default.

5. **Live Alerts**: alerts raised by Published rules in the run.
6. **Shadow Alerts**: alerts raised by Shadow rules in the run (for example 504 for Every_Quarter, 19 for Migrated legacy schedule 297).
7. **Run Status** of each run.

Column	What it shows
Schedule Name / Schedule ID	Schedule name and SCH-identifier
Live Alerts	Alerts from Published rules in this run
Shadow Alerts	Alerts from Shadow rules in this run
Start Time / End Time	When the run started and ended
Duration	Run length, for example 3.75s
Run Status	Running, Completed, Partially Failed or Failed

> **Tip**
> To see the runs of one rule, use Schedule Details on the rule's page.

Schedules: Schedule List

Fyscal ARCX → Transaction Monitoring → Schedules → Schedule List

Schedule List shows every schedule and how many rules use it. Schedules are created from the Create Typology schedule page (Part 5 of the walkthrough); this page has no create button.

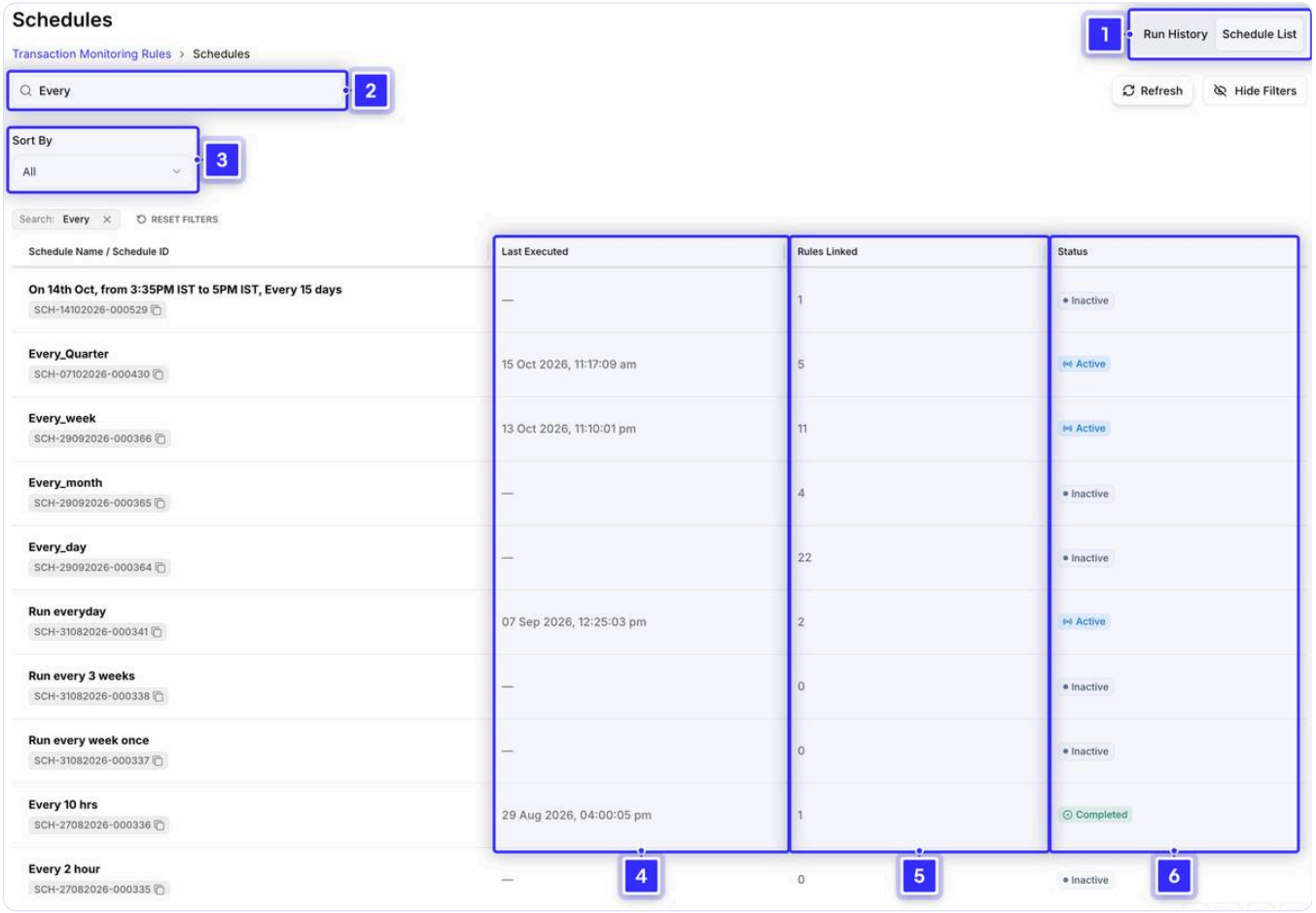


Figure 8.16 Schedule List searched for Every: view switch (1), search (2), Sort By (3), Last Executed (4), Rules Linked (5) and Status (6)

1. View switch.
2. Search (*Schedule Name*). Here “Every” finds 12 schedules.

3. **Sort By** (shows **All**).
4. **Last Executed**: date and time of the last run, or — if it has not run.
5. **Rules Linked**: how many rules reference the schedule (Every_day: 22).
6. **Status**: **Active**, **Inactive**, or **Completed** once the schedule has passed its End Time.

Step 1 **Open a schedule**

Click a row. The **View** dialog shows the schedule's ID (1), **CREATED BY** (2), **Edit** (3) and the **Schedule** fields (4): **Name**, **Execution Interval** (a number and a unit), **Start Time** and **End Time (optional)**, followed by a summary sentence (5) such as "This rule will run every 1 day starting 07 Oct 2026, 12:00:00 am". **Live in:** (6) names the active rule the schedule drives, or "Not used in any active rule". **Used in:** (7) lists every rule that references it, each as a link.

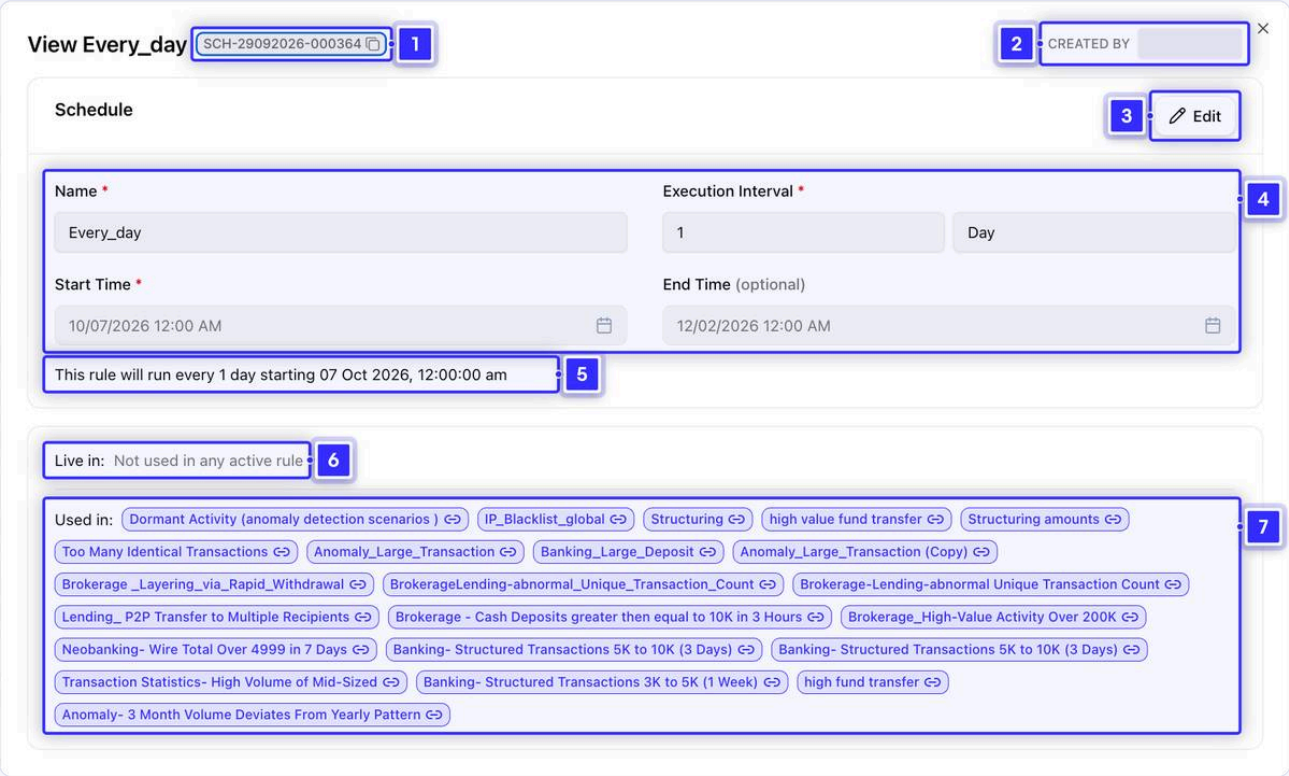


Figure 8.17 View Every_day: ID (1), CREATED BY (2), Edit (3), schedule fields (4), summary (5), Live in (6) and Used in (7)

Step 2 **Edit a schedule**

Click **Edit** (3) in the dialog to change the fields.

Note

A schedule can be linked to many rules (Every_day is used in 22). A change to its interval or times applies to every rule in its **Used in** list, so check that list before you edit.

Build a typology from scratch: walkthrough

Fyscal ARCX → Transaction Monitoring → Variables / Typology

WHERE	SAVED AS	MAKER CHECKER	OUTPUT
Transaction Monitoring → Variables and Typology	A **Draft** rule	Yes, for activation (Part 7)	An **Activate Typology** request, Pending a checker

This walkthrough builds a complete rule, screen by screen, from a new variable to a saved draft. The worked example is a Velocity rule: **flag a sender who makes 3 or more outgoing transactions totalling ₱5,000 or more within 7 days**. Follow the parts in order; each step is one action, and the figure under it shows the screen after that action.

Part	Screen	What you do
1	—	Plan the rule: the variables, conditions, type, suppression and schedule it needs

Part	Screen	What you do
2	Variables → **Create Variables**	Create the 7-day sum variable
3	Typology → **Create Typology**	Name the rule, choose its type, set suppression and a description
4	**Create Typology**, conditions	Add the two conditions in Group 1
5	**Review & schedule rule**	Choose an existing schedule or create a new one
6	**Review & schedule rule** → **Update Typology**	Save the rule as a Draft and check it
7	Dry run, **Activate**, Maker Checker Approval	Test the rule and request activation

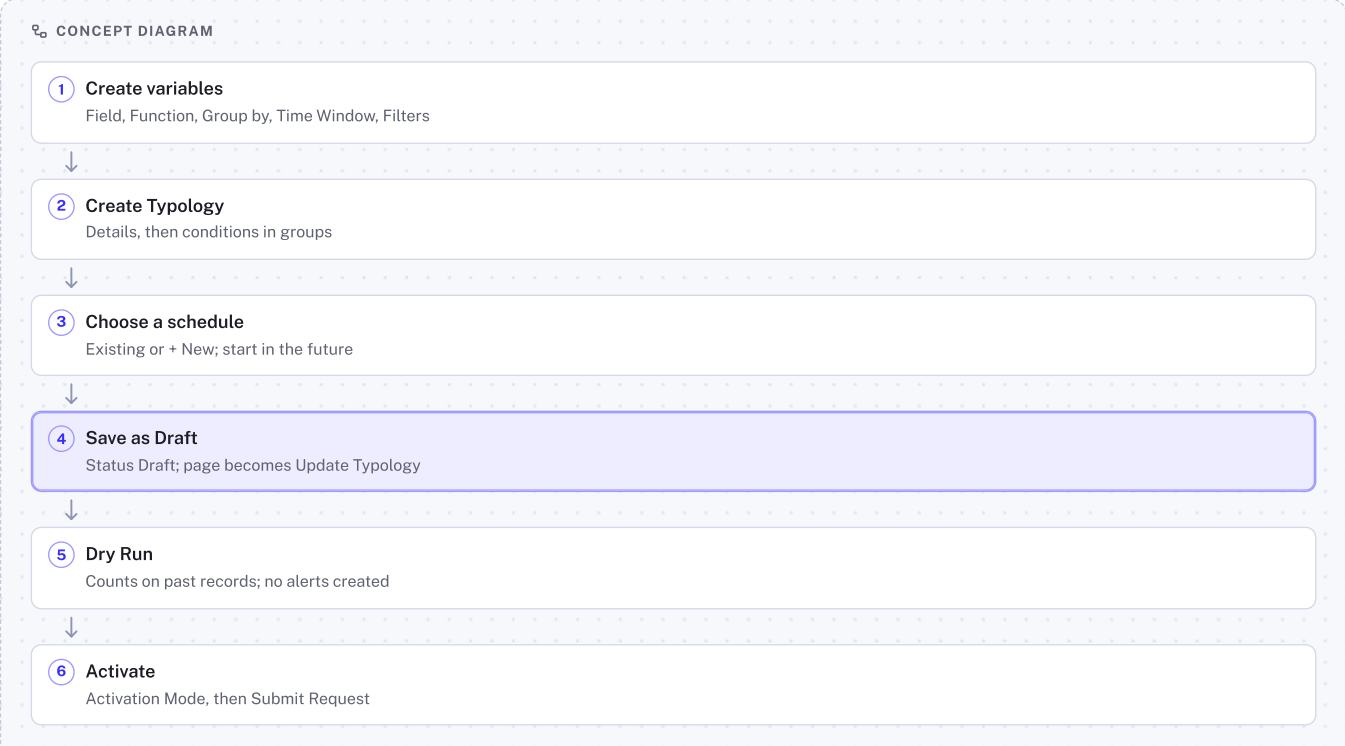


Diagram 8.1 — Building a typology, from variable to activation request

Diagram 8.1 shows the order the screens impose. A typology's conditions can only pick variables that already exist, so variables come first. **Save as Draft** needs a schedule, and **Dry Run** needs a saved draft. **Activate** does not switch the rule on: it sends a request to Maker Checker Approval (Diagram 8.2 in Part 7).

> **Note**
> In the screenshots the example objects carry a *GUIDE EXAMPLE* prefix so they are easy to find on the test system: the rule is named **GUIDE EXAMPLE - Velocity 3 or more outgoing transactions totalling PHP 5000 in 7 days**, the new variable `guide_example_sender_txn_sum_7d` and the new schedule `guide_example_schedule`. The steps below give the values without the prefix. Use your own names.

Part 1: Plan the rule

Before you open a form, write the rule down as variables and conditions. A **variable** calculates one number per sender; a **condition** compares that number with a threshold. The example needs two numbers per sender over the last 7 days: how many transactions they sent, and the total amount they sent.

Item	Value in the example	Where you set it
Count of transactions per sender, last 7 days	Variable `sender_txn_count_7d` : **Field** `amount` , **Function** Count, **Group by** `sender_entity_id` , window 7 days. It already exists, so it is reused.	View Variable (Figure 8.13)
Total amount per sender, last 7 days	New variable `sender_txn_sum_7d` : **Field** `amount` , **Function** Sum, **Group by** `sender_entity_id` , from 7 to 0 Days ago, no filters	Part 2
Condition 1	`sender_txn_count_7d` **Greater Than Equal (>=)** 3	Part 4

Item	Value in the example	Where you set it
Condition 2	`sender_txn_sum_7d` **Greater Than Equal (>=)** 5000	Part 4
How the conditions combine	Both in Group 1, **Match AND** (both must be true)	Part 4
Typology type	Velocity (V-01)	Part 3
Suppression Window	7 Day	Part 3
Schedule	Every 1 Day, starting at 09:00 AM on a future date, no end time	Part 5

Check for variables you can reuse before creating new ones: open **Select an existing variable** in **Create Variables**, or search the Variables list. Here the count variable exists and the 7-day sum does not, so Part 2 creates only the sum.

Part 2: Create the variable

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 1 **Open Create Variables**

Go to **Transaction Monitoring → Variables** and click **+ New** (1) at the top right.



Figure 8.18 + New (1), at the top right of the Variables page, opens Create Variables

Step 2 **Read the empty form**

The **Create Variables** dialog opens. **Select an existing variable** (1) is on the left; **Configure Variable** is on the right, with **Transaction** / **Entity** (2), **Variable name** (3), **Description** (4), **Field** (5), **Function** (6), **Group by** (7) and **Time Window** (8) further down. **Function** stays greyed out until you choose a **Field**, and **Save Variable** (9) stays greyed out until the required fields are filled.

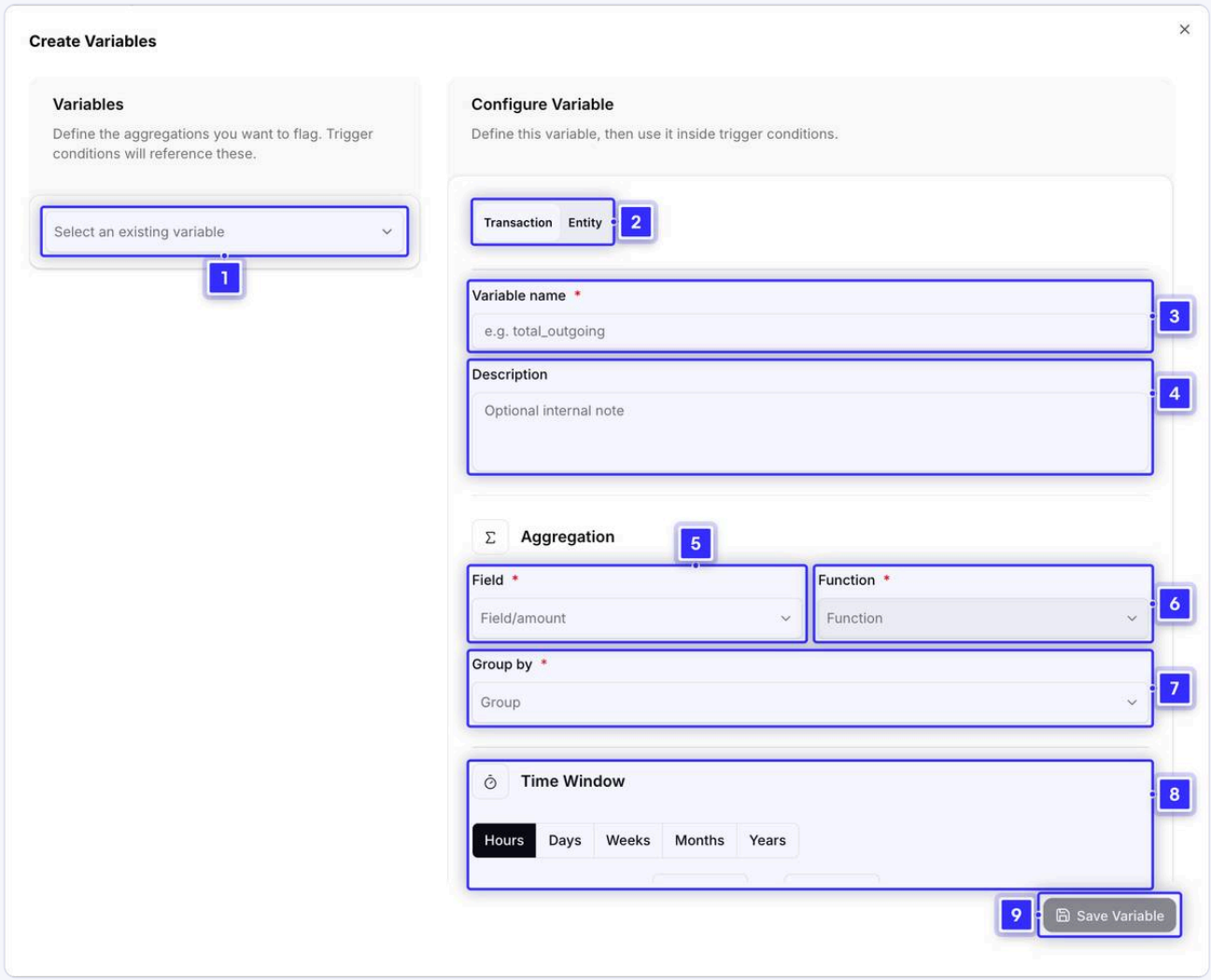


Figure 8.19 Create Variables, empty: Select an existing variable (1), Transaction / Entity (2), Variable name (3), Description (4), Field (5), Function (6), Group by (7), Time Window (8) and Save Variable (9)

Step 3 **Name and describe the variable**

Leave **Transaction** (1) selected. In **Variable name** (2) type `sender_txn_sum_7d`. In **Description** (3) type a note such as "Total amount sent per sender over the last 7 days."

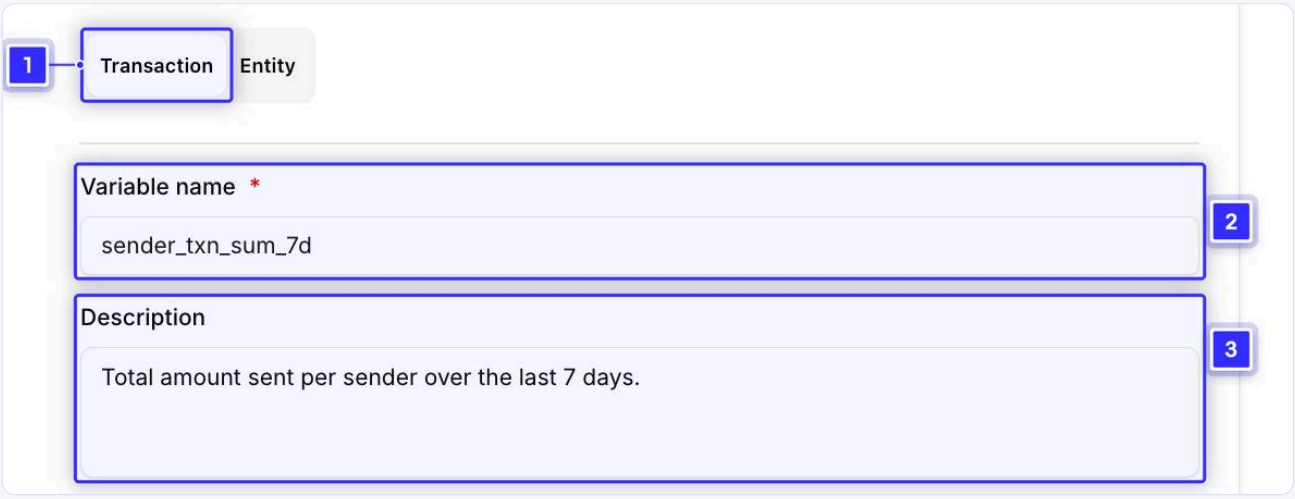


Figure 8.20 Transaction selected (1), Variable name (2) and Description (3) filled in

Step 4 **Choose the Field**

Open **Field** (1) (placeholder **Field/amount**). The list has a **Search Fields** box (2) and the 51 transaction fields. Choose `amount` (3).

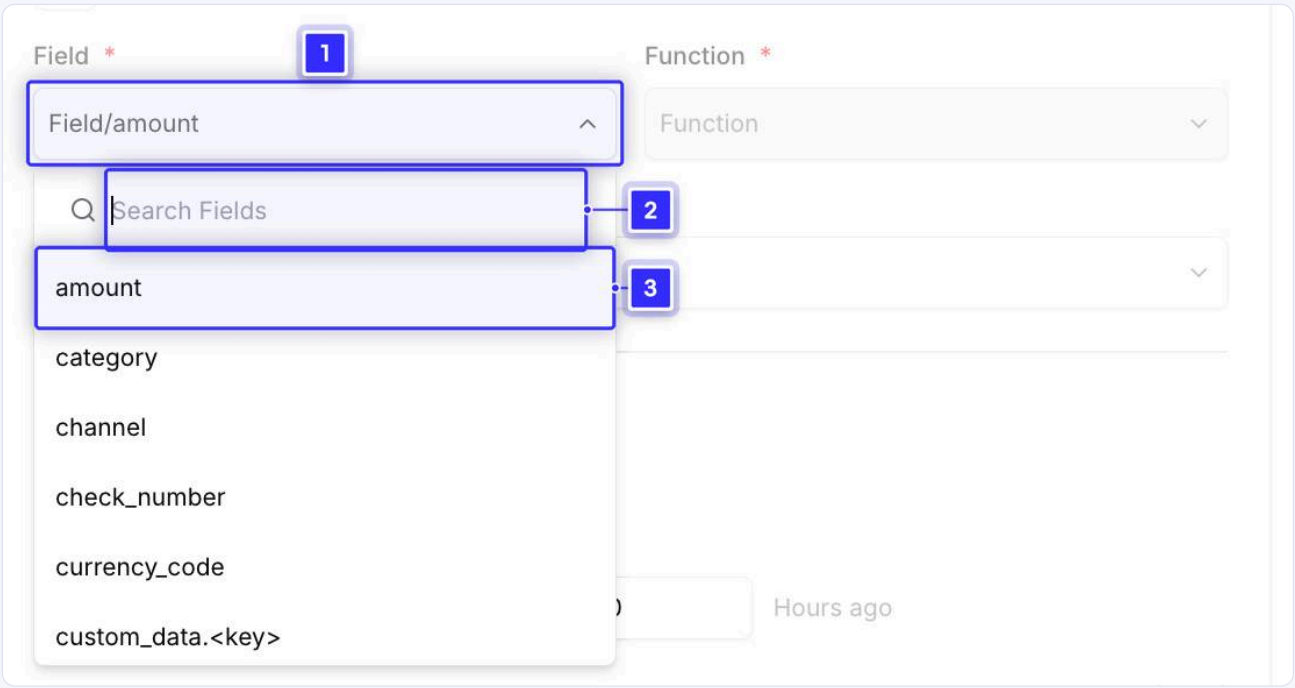


Figure 8.21 The Field list (1) open: Search Fields (2) and amount (3) at the top

Step 5 **Choose the Function**

With **Field** set to `amount` (1), open **Function** (2), now available. The options are **Count**, **Count Distinct**, **Sum**, **Average**, **Minimum** and **Maximum**. Choose **Sum** (3).

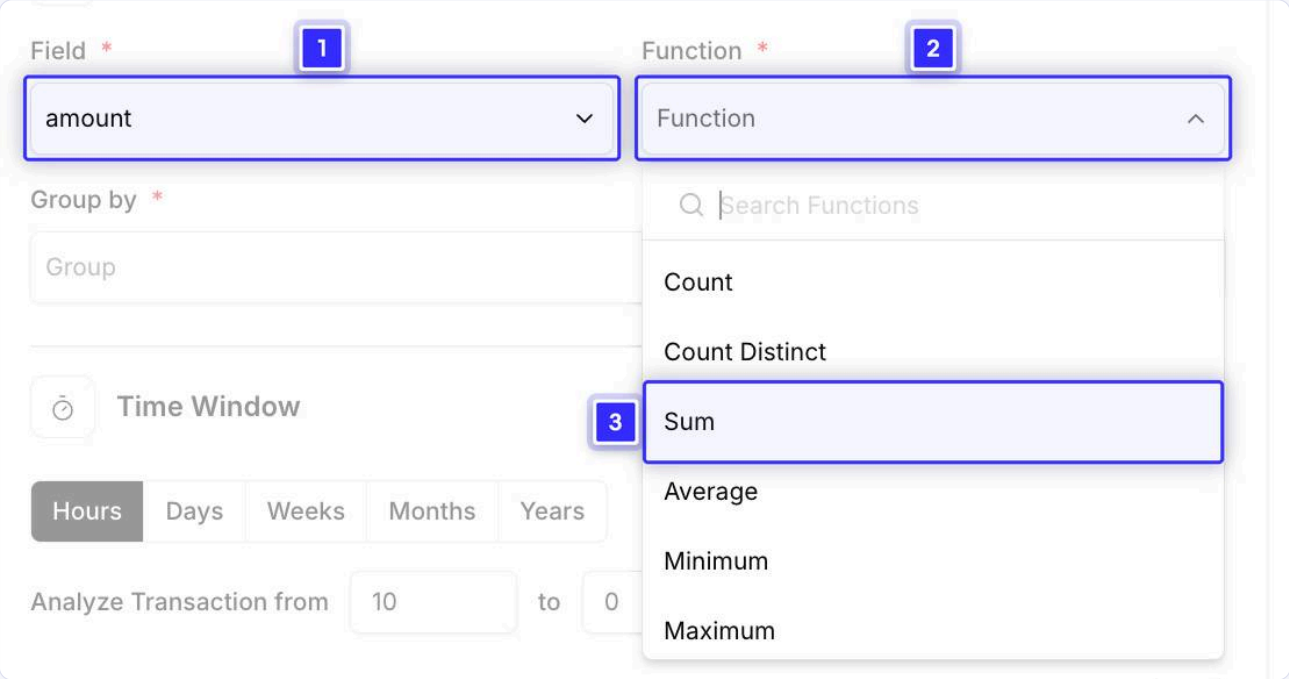


Figure 8.22 Field amount (1); the Function list (2): Count, Count Distinct, Sum (3), Average, Minimum, Maximum

Step 6 **Choose Group by**

Open **Group by** (1). It lists the same fields as **Field** without `amount`. Type `sender_entity` in **Search Fields** (2): two fields remain, `sender_entity_id` and `sender_entity_name`. Choose `sender_entity_id` (3), so the sum is calculated separately for each sender.

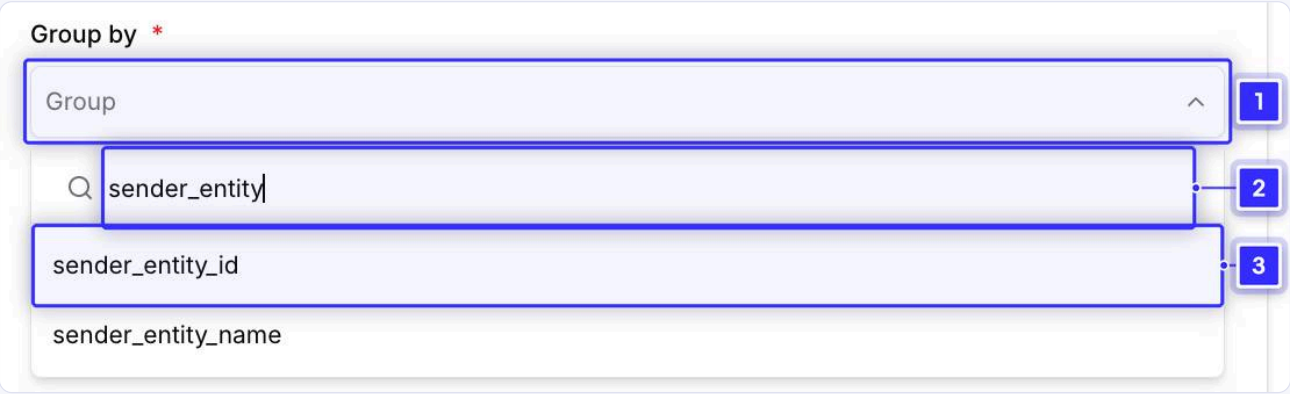


Figure 8.23 Group by (1) searched for sender_entity (2): choose sender_entity_id (3)

Step 7 **Set the time window**

Scroll down to **Time Window**. Click **Days** (1); the default is **Hours**. In **Analyze Transaction from** enter **7** and in **to** enter **0** (2). The line reads “from 7 to 0 Days ago”: the last 7 days up to the trigger time T. The form starts with one blank filter row under **Filters (1)** (3). Leave it empty: this variable sums every transaction the sender made. The blank row is dropped when you save.

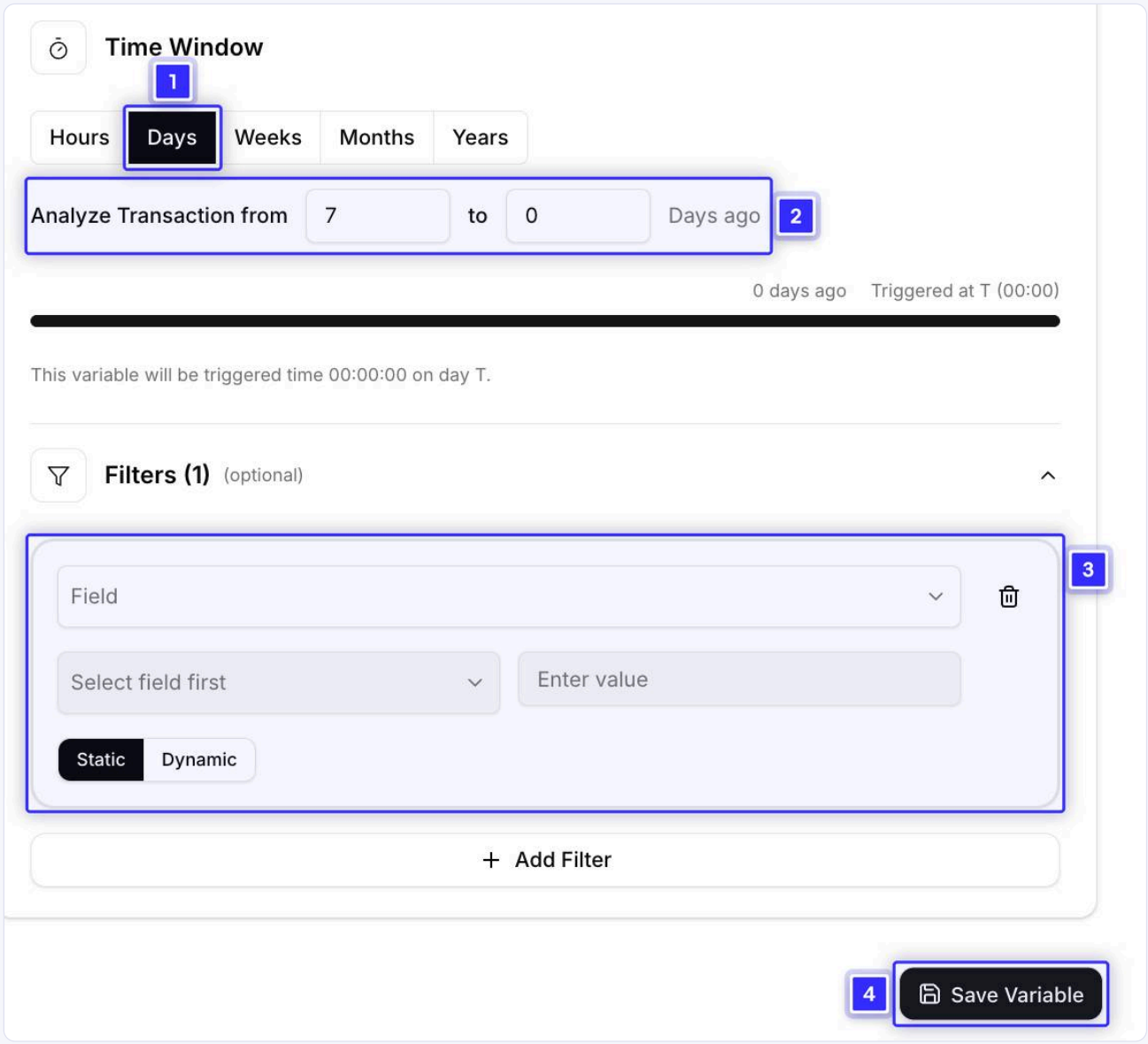


Figure 8.24 Time Window: Days (1), from 7 to 0 Days ago (2); the blank filter row (3); Save Variable (4)

Step 8 **Save the variable**

Click **Save Variable** (4 in Figure 8.24). The button shows **Saving...** and the fields grey out. The dialog then closes, and the new variable is the first row of the list with its ID, here VAR-07102026-000736. No confirmation message is shown. To find it again later, type its name in the search box (1): the row shows the name (2) and the Variable ID (3).

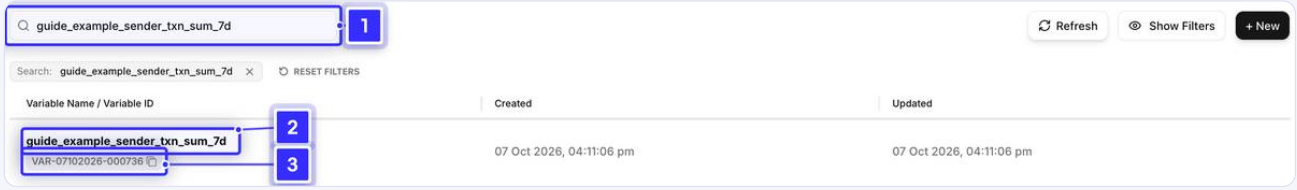


Figure 8.25 The saved variable found by name (1): its name (2) and Variable ID (3)

Step 9 **Check the saved variable**

Click the row to open **View Variable**. The type tag (1) reads **NUM_AGG_SUM**, and the form shows `amount`, **Sum** and `sender_entity_id`. **CREATED** and **UPDATED** (2) show the date and time and the user. **Edit**, **Delete** and **Duplicate** (3) are at the top of **Configure Variable**; **Update Variable** (4) is greyed out. Scroll down (Figure 8.27): **Days** (1) is selected, the window reads 7 to 0 **Days** ago (2) and the heading reads **Filters (0)** (3). Close the dialog with ×.

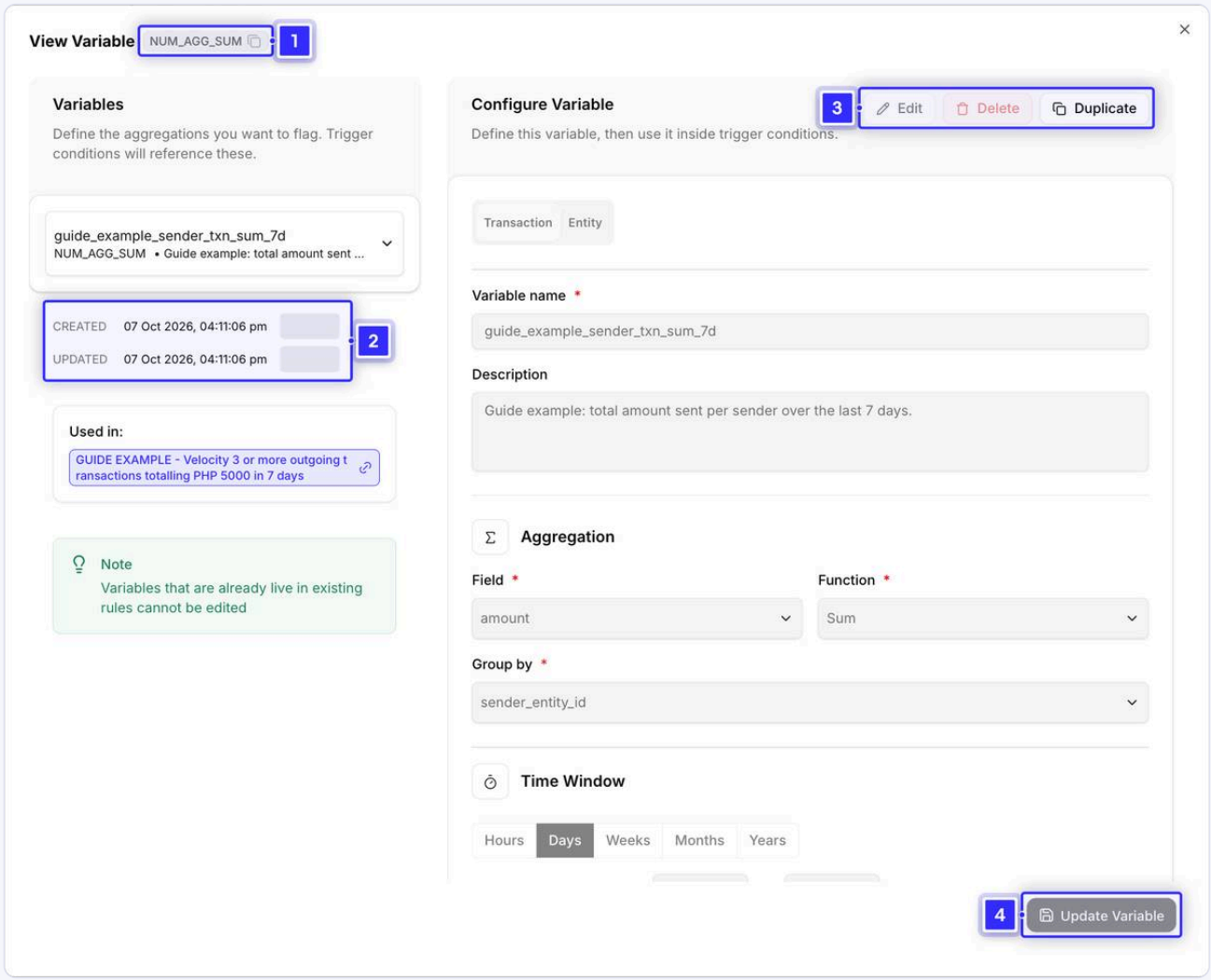


Figure 8.26 View Variable for the new variable: type tag (1), created and updated (2), Edit, Delete and Duplicate (3), Update Variable (4)

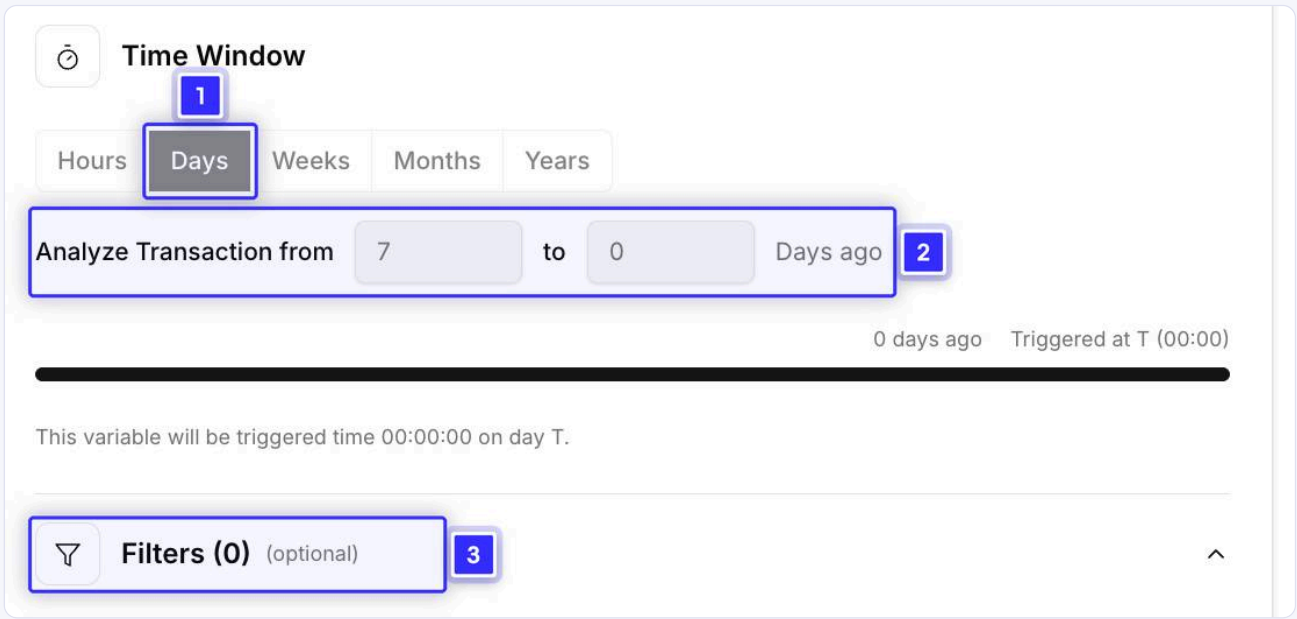


Figure 8.27 View Variable, lower part: Days (1), 7 to 0 Days ago (2) and Filters (0) (3)

Create Variables: field reference

Field	Required	What to enter / options
Select an existing variable	No	Opens a list of existing variables. Use it to check whether the calculation already exists.
Transaction / Entity	—	Two tabs. **Transaction** is selected by default. The example uses **Transaction**.
Variable name	Yes (*)	Free text; placeholder “e.g. total_outgoing”. Example: `sender_txn_sum_7d`.
Description	No	Free text; placeholder “Optional internal note”. It is shown on the variable card on the typology page (Figure 8.51).
Field	Yes (*)	A searchable list of 51 transaction fields (listed below). Example: `amount`.
Function	Yes (*)	**Count**, **Count Distinct**, **Sum**, **Average**, **Minimum**, **Maximum**. Greyed out until a **Field** is chosen. Example: **Sum**.
Group by	Yes (*)	A searchable list: the same fields as **Field**, without `amount`. Example: `sender_entity_id`.
Time Window unit	—	Buttons: **Hours** (default), **Days**, **Weeks**, **Months**, **Years**. Example: **Days**.
Analyze Transaction from … to … ago	—	Two numbers, counted back from the trigger time T. The empty form shows 10 and 0. Example: 7 and 0.
Filters (optional)	No	One blank row at the start: **Field**, an operator (**Select field first**), **Enter value**, and **Static** / **Dynamic**. **Add Filter** adds rows; the bin icon removes one. A blank row is not saved. Example: none.

The 51 fields offered under **Field** are: `amount`, `category`, `channel`, `check_number`, `currency_code`, `custom_data.<key>`, `id`, `ingested_at`, `merchant_category_code`, `mode_of_transaction`, `occurred_at`, `orig_currency_amount`, `orig_currency_code`, `product_type`, `purpose_of_remittance`, `receiver_address`, `receiver_amount`, `receiver_bank_city_code`, `receiver_bank_swift_code`, `receiver_currency_code`, `receiver_device_id`, `receiver_entity_id`, `receiver_entity_name`, `receiver_geo_coordinates.latitude`, `receiver_geo_coordinates.longitude`, `receiver_instrument_id`, `receiver_instrument_subtype`, `receiver_instrument_type`, `receiver_ip`, `receiver_provider_country`, `receiver_provider_name`, `regulatory_transaction_code`, `remarks`, `sender_address`, `sender_amount`, `sender_bank_city_code`, `sender_bank_swift_code`, `sender_currency_code`, `sender_device_id`, `sender_entity_id`, `sender_entity_name`, `sender_geo_coordinates.latitude`, `sender_geo_coordinates.longitude`, `sender_instrument_id`, `sender_instrument_subtype`, `sender_instrument_type`, `sender_ip`, `sender_provider_country`, `sender_provider_name`, `status`, `type`.

Part 3: Create the typology

Fyscal ARCX → Transaction Monitoring → Typology → + New

Step 1 **Open Create Typology**

Go to **Transaction Monitoring → Typology** and click **+ New** (1).



Figure 8.28 + New (1), at the top right of the Typologies page, opens Create Typology

Step 2 **Read the details card**

Create Typology opens on its first page. The top card holds **Typology Name** (2), **Typology type** (3), **Suppression Window** (4) and **Description** (5). **+ Variable** (1) creates a variable without leaving the form. The conditions are below the card (Part 4). The page has no **Save as Draft** button: you save on the next page.



Figure 8.29 Create Typology, empty details card: + Variable (1), Typology Name (2), Typology type (3), Suppression Window (4), Description (5)

Step 3 **Enter the name**

In **Typology Name** type **Velocity 3 or more outgoing transactions totalling PHP 5000 in 7 days**. A name may contain only letters, digits, spaces, hyphens, underscores and parentheses. Any other character turns the field red (1) with the message (2) “Rule name can only include letters, digits, spaces, hyphens, underscores, and parentheses”. The name in Figure 8.30 contains a colon, a plus sign, commas, an en dash and ₱, none of which is in that list. That is why the example name spells the amount as “PHP 5000”.

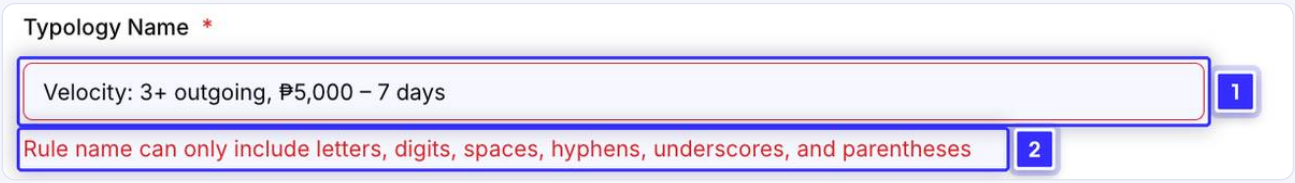


Figure 8.30 A name with characters outside the allowed set (1), and the validation message (2)

Step 4 **Open Typology type**

Open **Typology type** (1) (marked optional). The list has a **Search typology type** box (2) and shows each type with its code (3): SMURFING (TP01), Mule Networks (ML01), Layering (LA01), High Value (HV01), High Value Transfer (HV02), High Value (HV03), Support (TP00), Structuring (TP100), identical transactions (TP101), identical transactions (TP102), Anomaly (TP103), banking threshhold (TP104), Cardinality (C-01), Large Transaction (LT-01), Velocity (V-01), Transactions (T-01) and Anamoly (A01). The list ends with **+ New**.

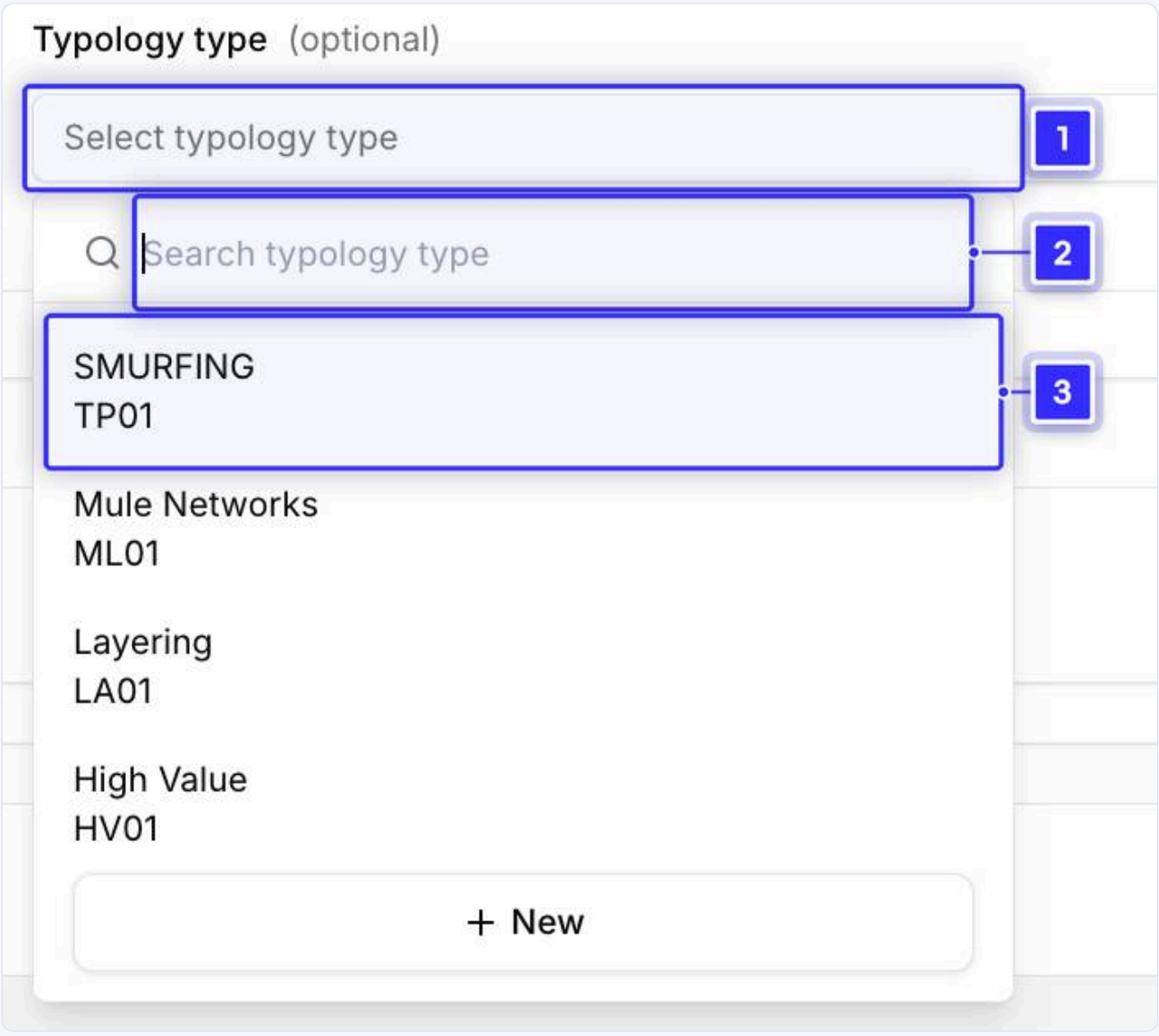


Figure 8.31 The Typology type list (1), with its search box (2) and each type with its code (3)

Step 5 **Choose Velocity**

Type `Velo` in the search box (1). Only **Velocity** (V-01) (2) remains. Click it. It appears in the field as a chip, **Velocity (V-01)**, with × to remove it.

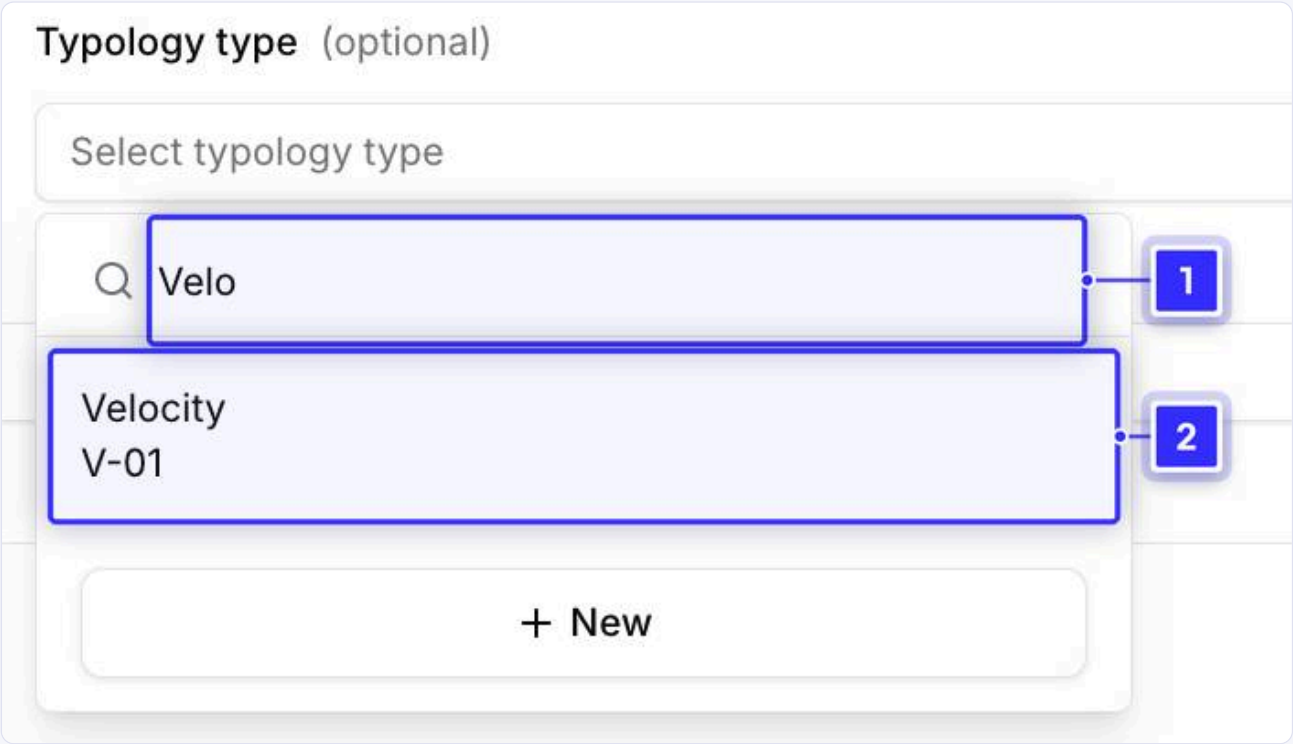


Figure 8.32 Typology type searched for Velo (1): Velocity, V-01 (2)

Step 6 **Set the suppression window**

In **Suppression Window** type **7** in the number box (2) (default 0). Open the unit list (3) (default **Hour**): **Hour**, **Day**, **Week**, **Month**, **Year**. Choose **Day** (4). The **Velocity (V-01)** chip (1) is in **Typology type** above. The example uses the same length as the variables' 7-day window (see Create Typology form).

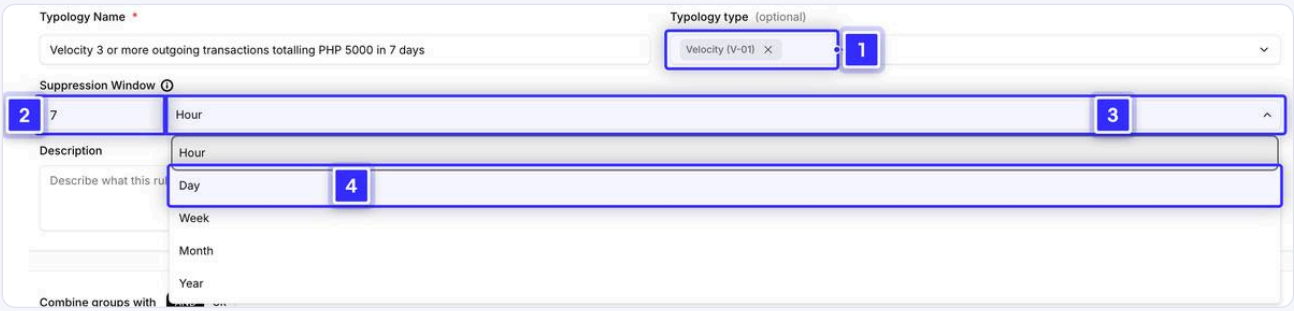


Figure 8.33 The Velocity (V-01) chip (1); Suppression Window 7 (2) and the unit list (3): Hour, Day (4), Week, Month, Year

Step 7 **Write the description**

In **Description** (placeholder “Describe what this rule is monitoring and why”) state the rule in words, for example “Flags a sender with 3 or more outgoing transactions totalling ₱5,000 or more within 7 days.” The description is shown under the rule ID on the typology page. The completed card is shown in Figure 8.40.

Create Typology, details: field reference

Field	Required	What to enter / options
Typology Name	Yes (*)	3 to 100 characters (a longer name is rejected after **Next Step** with “Rule name must be 3-100 characters”). Letters, digits, spaces, hyphens, underscores and parentheses only. Placeholder “This is true, please proceed”. Example: Velocity 3 or more outgoing transactions totalling PHP 5000 in 7 days.
Typology type	No (optional)	A searchable list of types with codes (see step 4); the choice shows as a chip with ×. Example: Velocity (V-01).

Field	Required	What to enter / options
Suppression Window	No	A number (default 0) and a unit: **Hour** (default), **Day**, **Week**, **Month**, **Year**. Example: 7 Day.
Description	No	Free text. Example: what the rule flags and why.
Combine groups with	—	**AND** (default) or **OR**. Applies when there is more than one group.
Group Match	—	**AND** (default) or **OR**, for the conditions inside the group. Example: **AND**.
WHEN field	Yes	**Select field**: a searchable list headed **VARIABLES**, newest first.
Operator	Yes	**Select operator**, greyed out until a field is chosen: **Equal**, **Not Equal**, **Greater Than**, **Greater Than Equal**, **Less Than**, **Less Than Equal**, **Between**, **Not Between**, **In**, **Not In**, **Is Null**, **Is Not Null**.
Compare to	Yes	**Static Value** (default) or **Variable**. A third entry, **Ingested Data**, is shown greyed out.
Value	Yes	With **Static Value**: a number in **Enter value** (greyed out until an operator is chosen).

Part 4: Add the conditions

Fyscal ARCX → Transaction Monitoring → Typology → + New (conditions)

Below the details card, **Combine groups with** is set to **AND** and **Group 1** has one empty row with **Match** set to **AND**. The example uses one group, so leave both settings as they are.

Step 1 **Open the field picker in row 1**

In Group 1 click **Select field** (1) next to **WHEN**. A list opens with a **Search..** box (2) and the heading **VARIABLES** (3); the newest variable is first. Type part of a name to narrow the list, for example `sender_txn` .

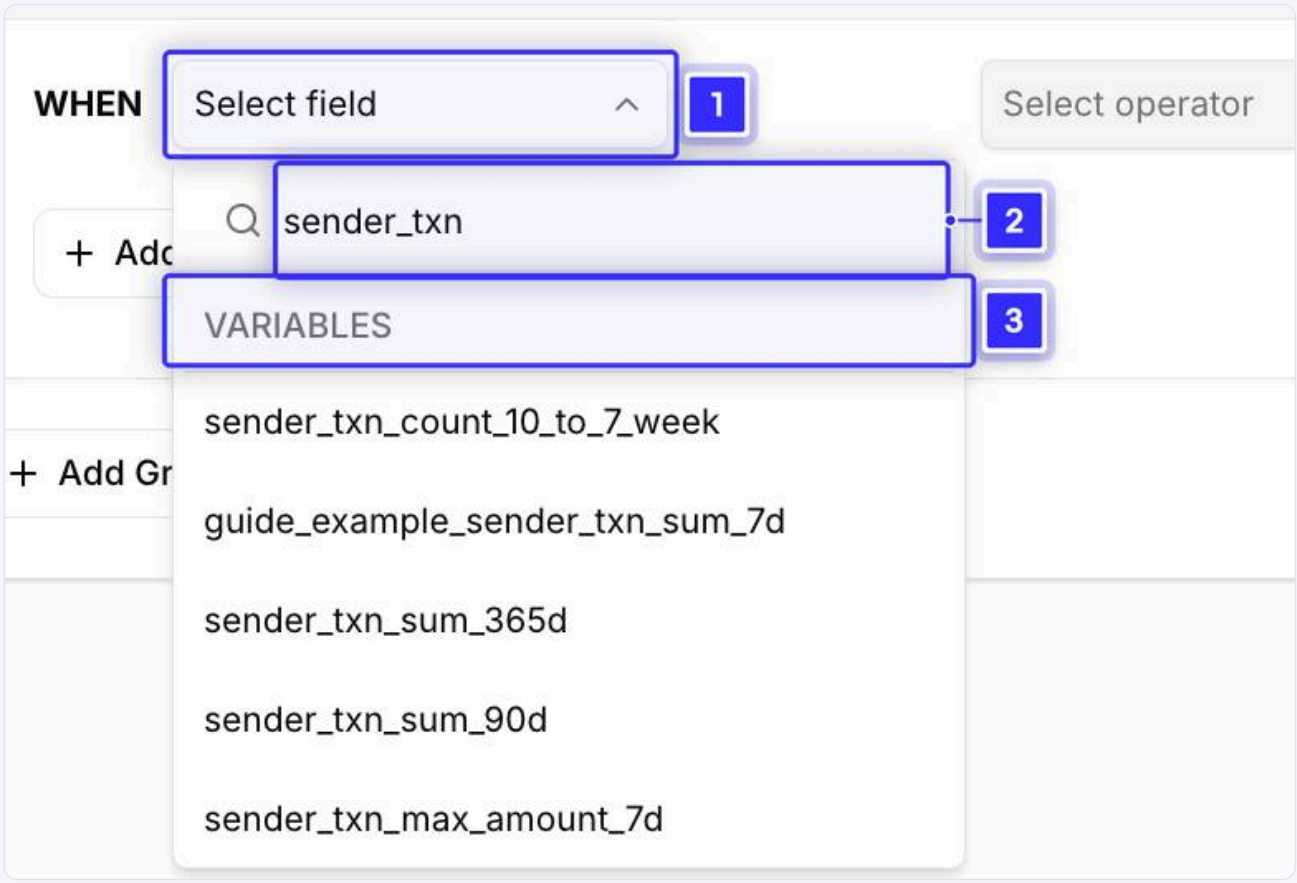


Figure 8.34 Group 1, row 1: Select field (1), the Search.. box (2) and the VARIABLES list (3), narrowed to sender_txn

Step 2 **Choose the count variable**

Type `sender_txn_count_7d` in the search box (1). One match remains (2). Click it.

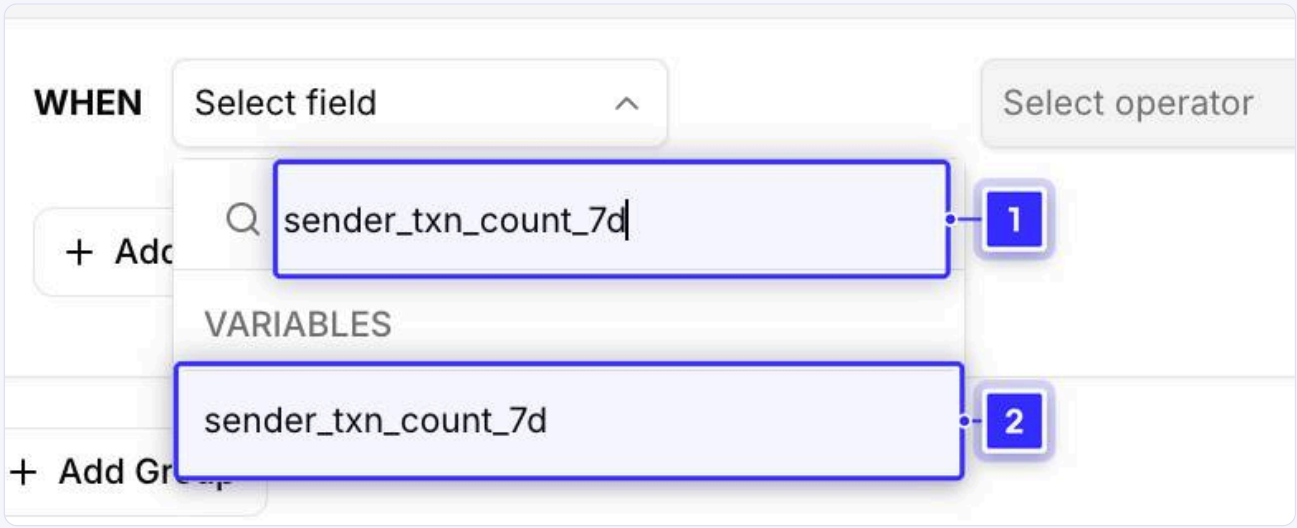


Figure 8.35 The variable list searched for sender_txn_count_7d (1): one match (2)

Step 3 **Choose the operator**

With the variable chosen (1), open **Select operator** (2), now available. The list shows **Equal**, **Not Equal**, **Greater Than**, **Greater Than Equal**, **Less Than** and **Less Than Equal**; scroll for **Between**, **Not Between**, **In**, **Not In**, **Is Null** and **Is Not Null**. Choose **Greater Than Equal** (3). The field then reads **Greater Than Equal (>=)**, shortened to "Greater Than Equal (>..." in the row.

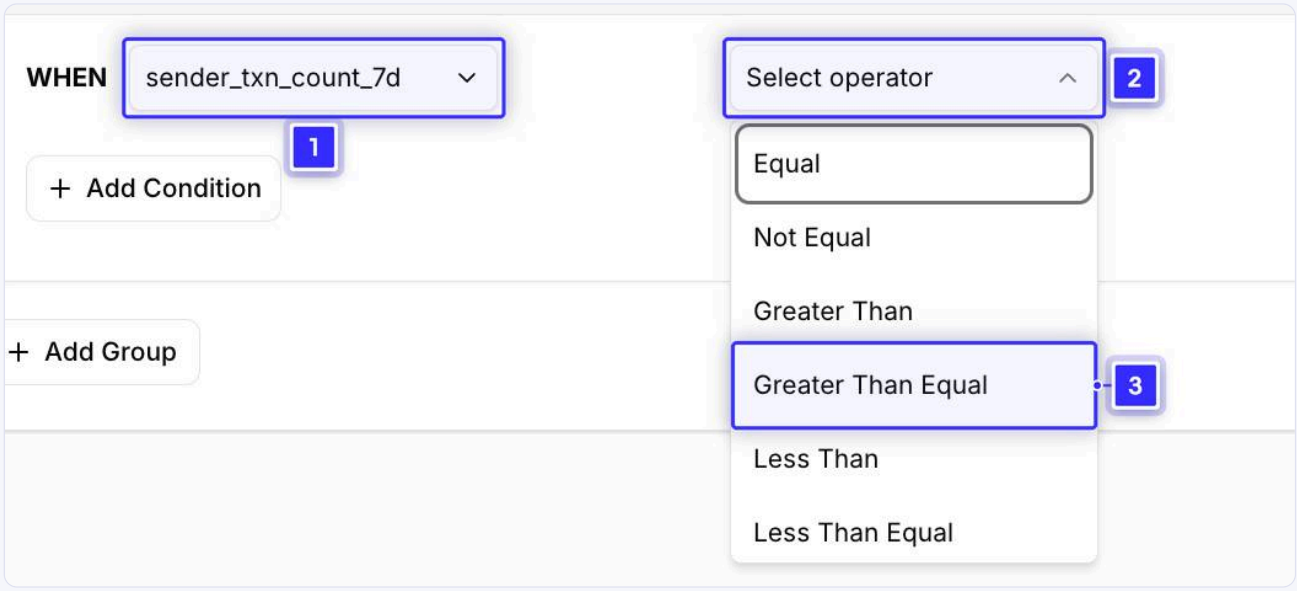


Figure 8.36 Row 1: the variable (1) and the operator list (2): choose Greater Than Equal (3)

Step 4 **Keep Static Value**

Open the compare-to list (1). It offers **Static Value** (2) (selected) and **Variable** (3); **Ingested Data** (4) is greyed out. Keep **Static Value**, because the threshold is a fixed number.

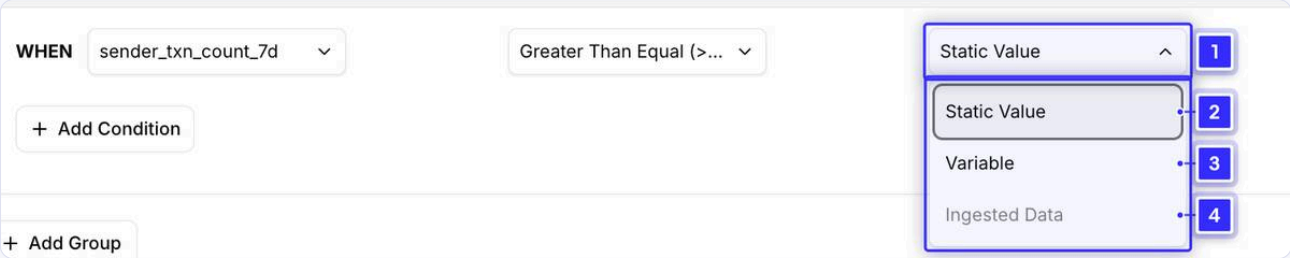


Figure 8.37 The compare-to list (1): Static Value (2), Variable (3), and Ingested Data (4) greyed out

Step 5 **Enter the threshold**

In **Enter value** type **3**. Row 1 is complete: the variable (1), **Greater Than Equal** (2), **Static Value** (3) and 3 (4). **Next Step** (5) becomes available.

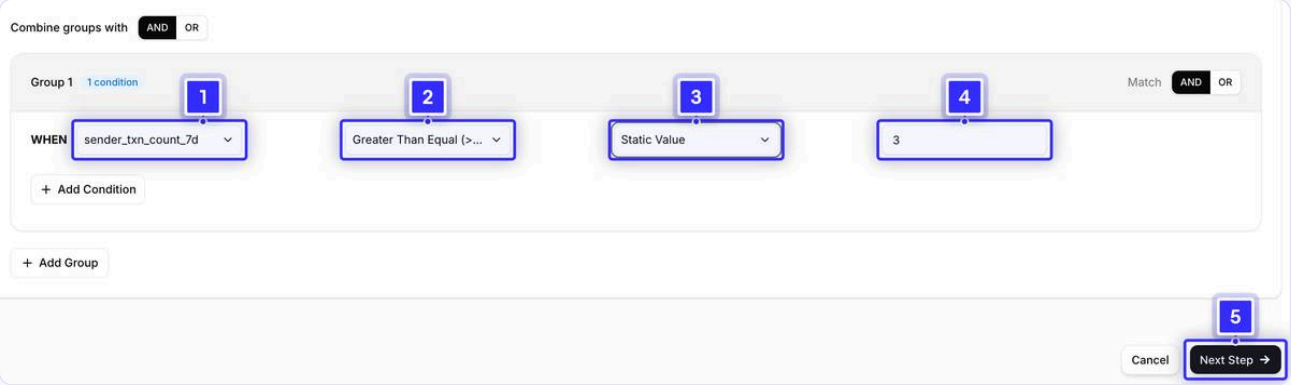


Figure 8.38 Row 1 complete: sender_txn_count_7d (1), Greater Than Equal (2), Static Value (3), 3 (4); Next Step available (5)

Step 6 **Add the second row**

Click **Add Condition**. A second **WHEN** row appears, the group heading changes to **2 conditions** (1), and the label **AND — all must match** (2) appears between the rows. Click **Select field** (3) in row 2, type the name of the variable from Part 2 in the search box (4) (the screenshot searches for `guide_example_sender`) and click it (5).

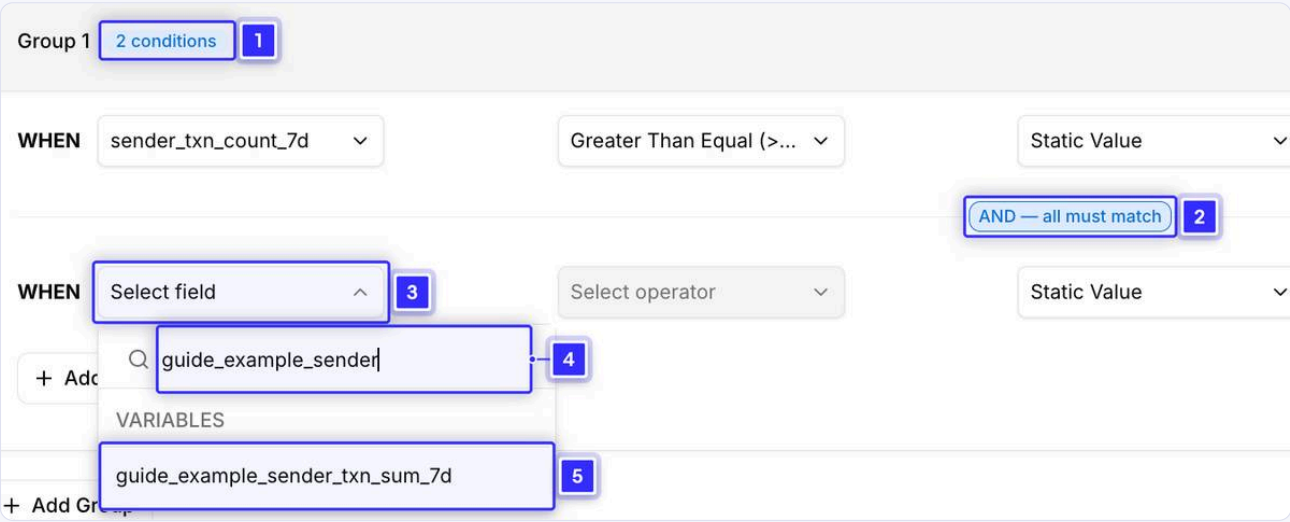


Figure 8.39 Row 2 added: 2 conditions (1), the AND — all must match label (2), Select field (3), the search (4) and the variable from Part 2 (5)

Step 7 **Complete row 2**

Choose **Greater Than Equal** from the same operator list as in step 3, keep **Static Value**, and type **5000** in **Enter value**.

Step 8 **Check the whole form**

The first page is complete: name (1), **Velocity (V-01)** (2), **Suppression Window** 7 **Day** (3), description (4), Group 1 with **Match AND** (5), row 1 (6) and row 2 (7). Each extra row has an × to remove it. Click **Next Step** (8).

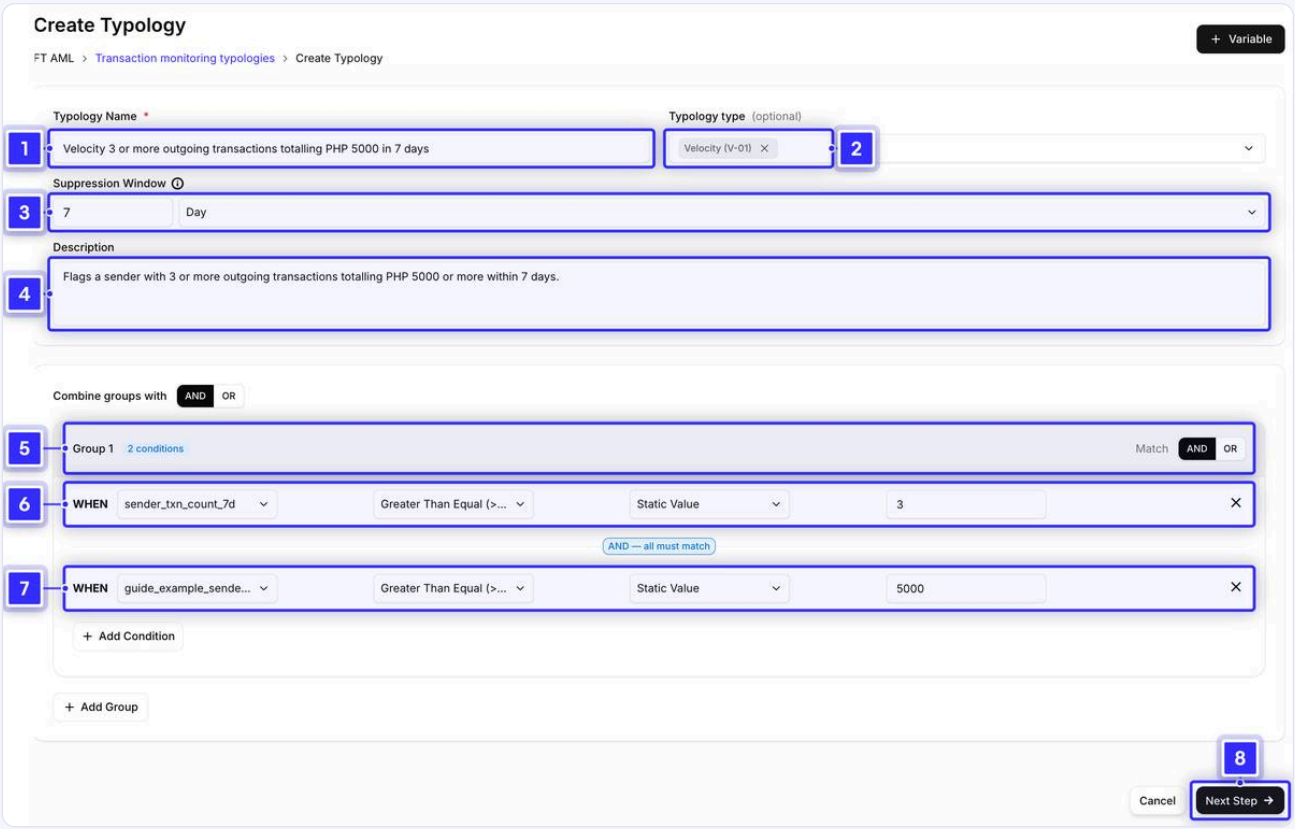


Figure 8.40 Create Typology, first page complete: name (1), Velocity (2), Suppression Window (3), description (4), Group 1 (5), row 1 (6), row 2 (7) and Next Step (8)

Note

Both conditions are in one group with **Match AND**, so the rule flags a sender only when the 7-day count is at least 3 *and* the 7-day total is at least 5000. To flag a sender when either is true, set **Match** to **OR**. See How conditions are evaluated.

Part 5: Choose or create a schedule

Fyscal ARCX → Transaction Monitoring → Typology → + New → Next Step

Step 1 **Read the Review & schedule rule page**

Next Step opens **Review & schedule rule** (“Validate your rule, run it on historical data, then schedule and activate.”). The **Schedule** card has **Select Schedule** (1), placeholder “Select from schedule list”. **Dry Run** (2) is greyed out, with the note “Please add execution interval and save this rule as a draft to dry run the results.” **Previous Step** (3) returns to the conditions. **Save as Draft** (4) is greyed out until a schedule is chosen.

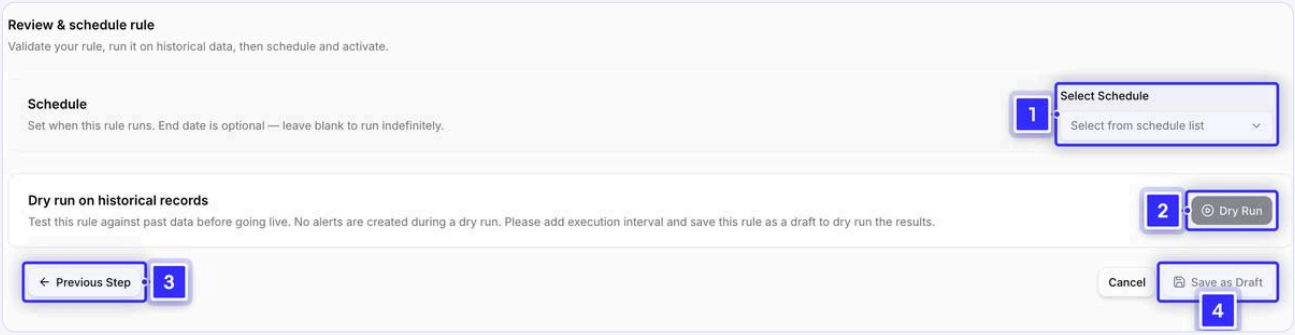


Figure 8.41 Review & schedule rule: Select Schedule (1), Dry Run (2), Previous Step (3) and Save as Draft (4)

Step 2 **Open Select Schedule**

Open **Select Schedule**. The list has a **Search Schedule** box (1) and shows each existing schedule with its name and SCH-ID (2), for example Every_Quarter (SCH-07102026-000430), Every_week, Every_month and Every_day; the screenshot searches for “Every”. **+ New** (3) is at the bottom.

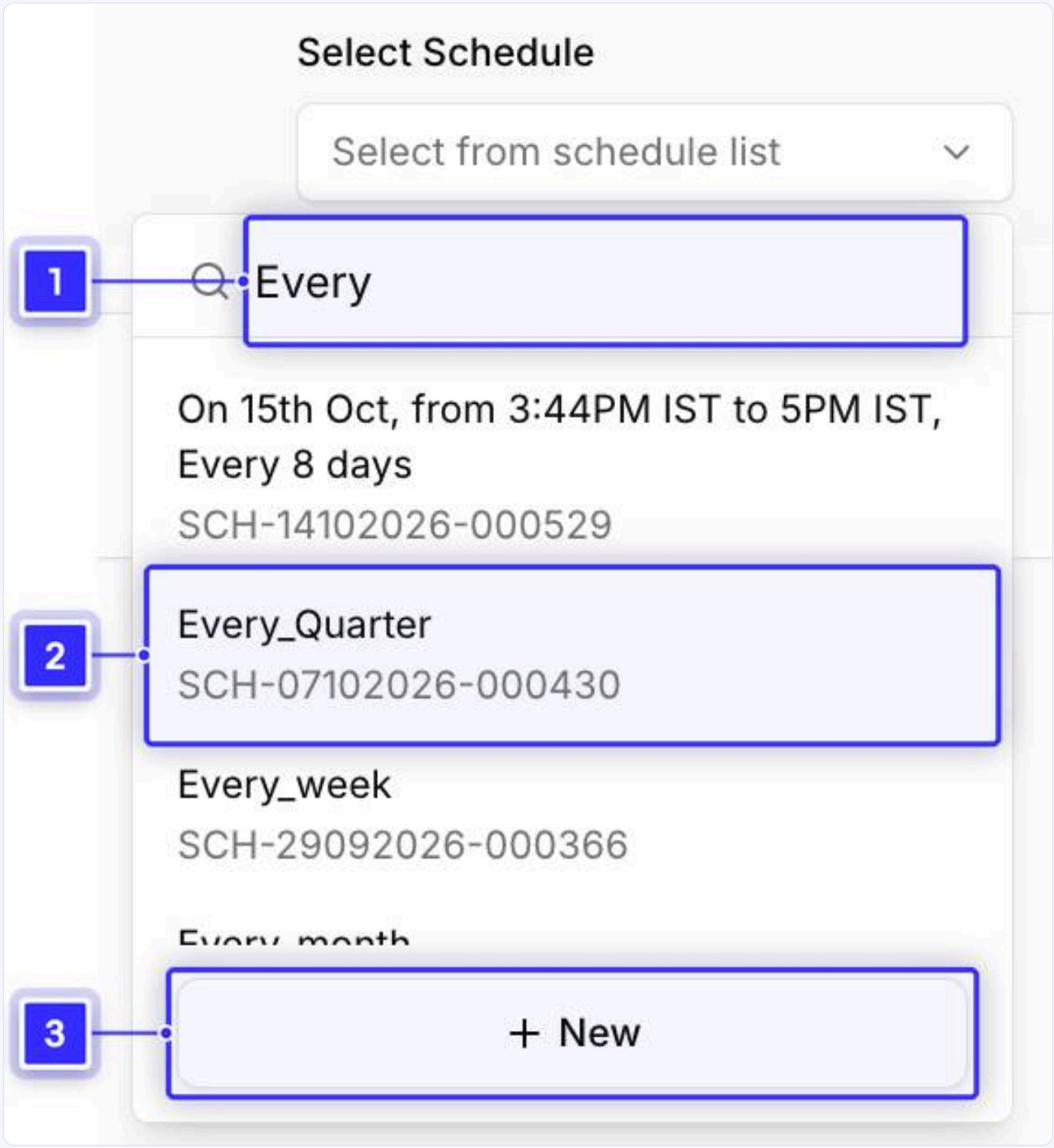


Figure 8.42 The Select Schedule list: search (1), an existing schedule with its ID (2) and + New (3)

Using an existing schedule. When you choose an existing schedule (1), its fields appear in the card and can be edited. If its **Start Time** is in the past, the field turns red with “Start time cannot be in the past” (2) and **Save as Draft** (3) stays greyed out. Every_day (start 10/07/2026 12:00 AM) and Every_week (start 10/06/2026 12:10 AM) both showed this message. These fields belong to the existing schedule, and one schedule can drive many rules (see Schedule List). The example therefore creates a new schedule instead.

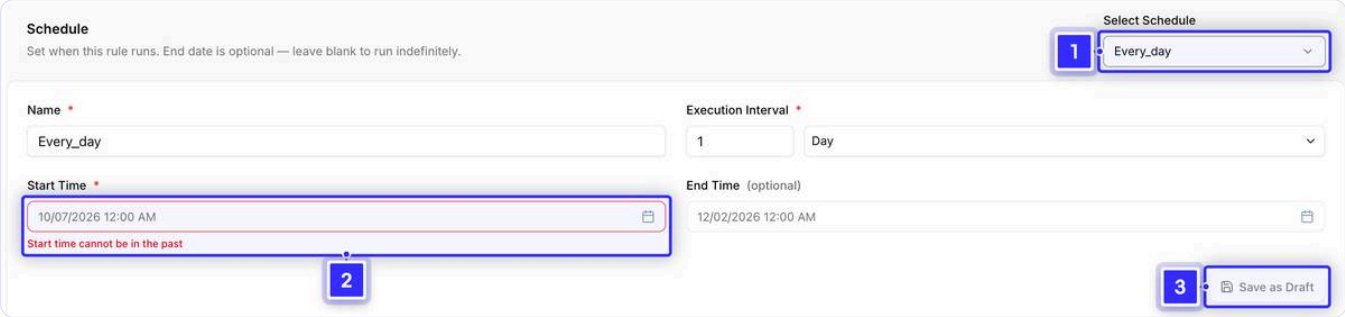


Figure 8.43 Every_day chosen (1): “Start time cannot be in the past” (2), and Save as Draft greyed out (3)

Step 3 **Start a new schedule**

Open **Select Schedule** again and click **+ New**. Empty schedule fields appear: **Name** (1), **Execution Interval** (2) with a **Unit** list (3), **Start Time** (4), filled with the current date and time, and **End Time** (5), marked optional. A **Save as Draft** button (6) appears in the card, greyed out.

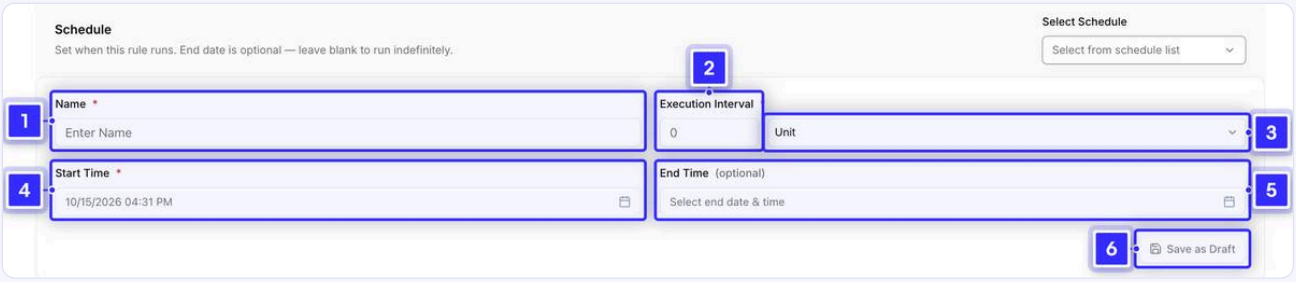


Figure 8.44 + New: Name (1), Execution Interval (2), Unit (3), Start Time (4), End Time (5) and Save as Draft (6)

Step 4 **Name the schedule and set the interval**

Type a **Name** (1) (the screenshots use `guide_example_schedule`). In **Execution Interval** (2) type **1**. Open **Unit** (3): **Hour**, **Day**, **Week**, **Month**, **Year**. Until you choose a unit, a red message under the field says “Interval unit is mandatory when interval is selected”. Choose **Day** (4).

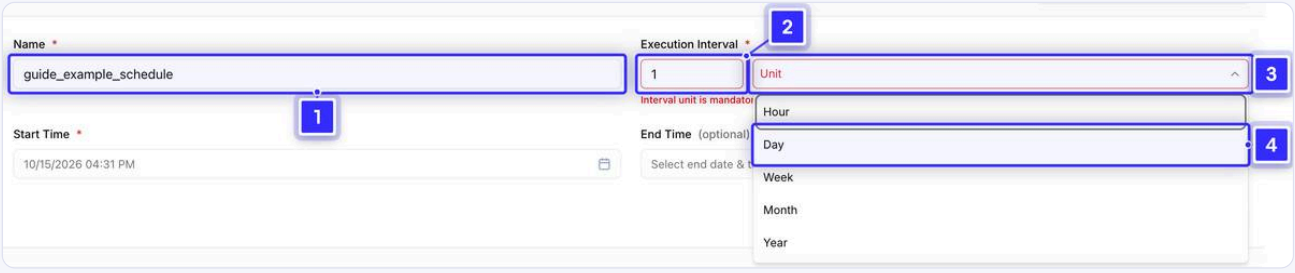


Figure 8.45 Name (1) and interval (2) entered; the Unit list (3): Hour, Day (4), Week, Month, Year

Step 5 **Open the start time picker**

Click **Start Time** (1). A calendar opens on the current month, with arrows for the previous and next month. Dates before today (2) are greyed out and cannot be chosen. Below the calendar are a **Time** box (3) and **Clear** (4).

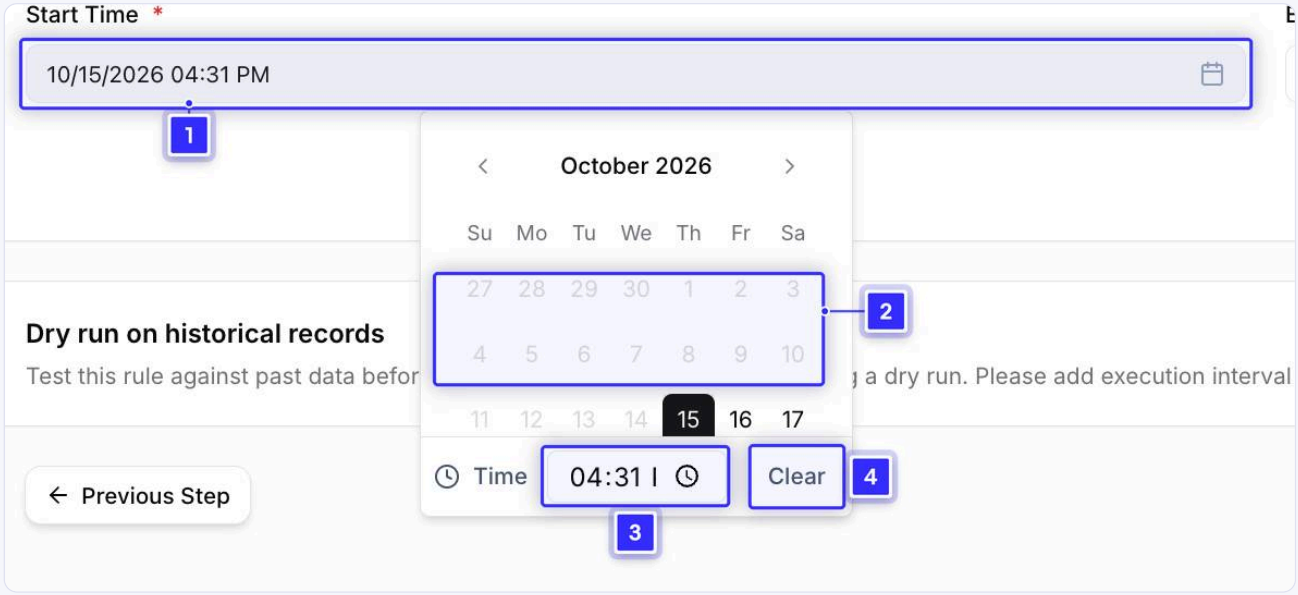


Figure 8.46 The Start Time field (1) and picker: past dates greyed out (2), Time (3) and Clear (4)

Step 6 **Choose the start date and time**

Click a future date (2) (here 16 October 2026) and type the time in **Time** (3) (09:00 AM). The field (1) reads **10/16/2026 09:00 AM** (month/day/year). The rule shown in Part 6 was saved on 7 October 2026 with a start of 08 Oct 2026, 09:00 AM.

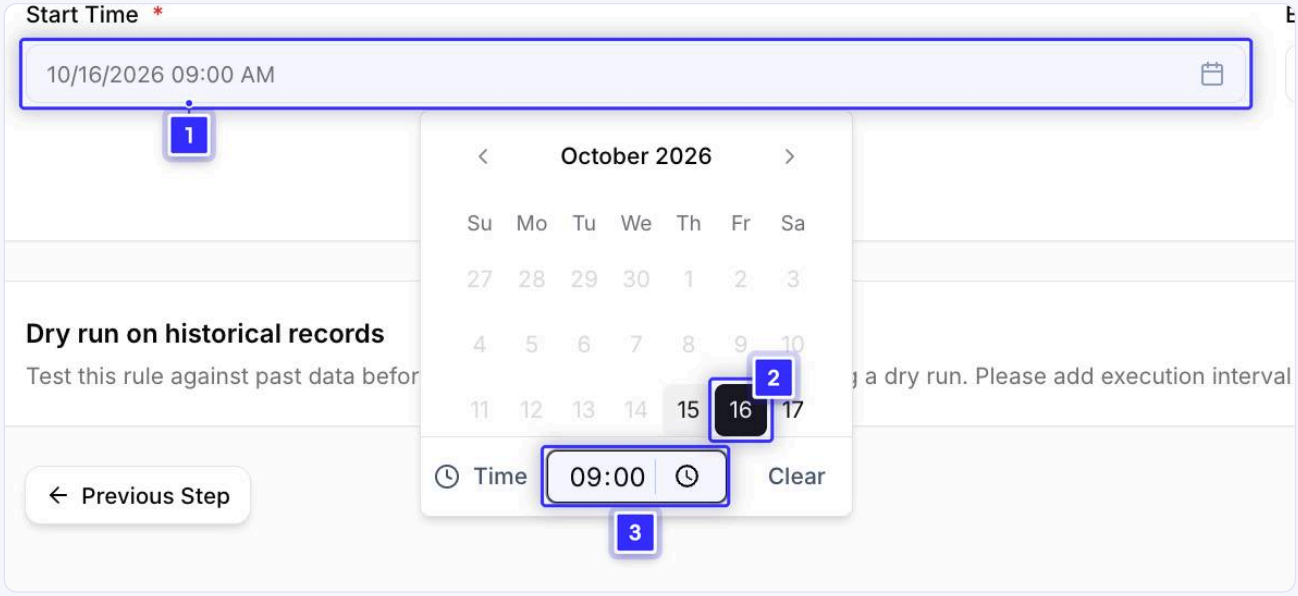


Figure 8.47 16 October chosen (2) and 09:00 AM typed in Time (3); the field reads 10/16/2026 09:00 AM (1)

Step 7 **Leave End Time blank**

Leave **End Time** (optional) (1) empty: the card states “End date is optional — leave blank to run indefinitely.” With **Name**, **Execution Interval**, **Unit** and a future **Start Time** set, **Save as Draft** (2) becomes available.

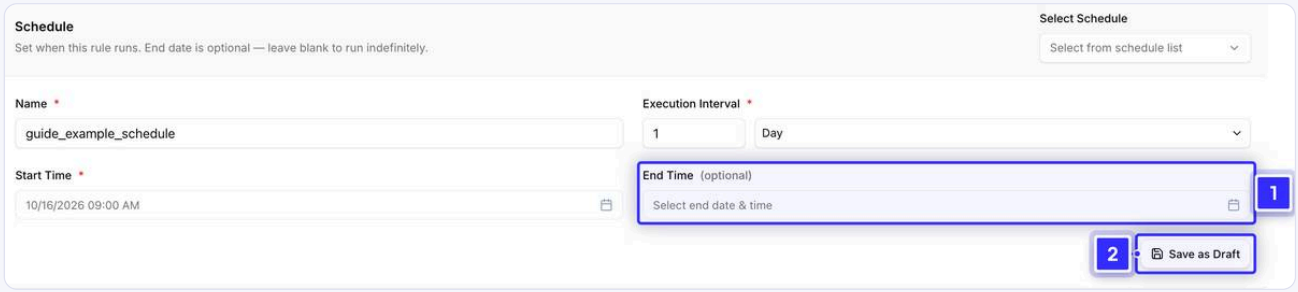


Figure 8.48 The new schedule complete: End Time blank (1) and Save as Draft available (2)

Schedule fields: reference

Field	Required	What to enter / options
Select Schedule	Yes (a schedule)	A searchable list of existing schedules (name and SCH-ID), and **+ New** to create one.
Name	Yes (*)	Free text; placeholder “Enter Name”.
Execution Interval	Yes (*)	A number (placeholder 0) and a **Unit**: **Hour**, **Day**, **Week**, **Month**, **Year**. Example: 1 Day.
Start Time	Yes (*)	Date and time, MM/DD/YYYY hh:mm AM/PM. Filled with the current date and time for a new schedule. Past dates are greyed out in the picker; a past start shows “Start time cannot be in the past”. Example: 10/08/2026 09:00 AM.
End Time	No (optional)	Placeholder “Select end date & time”. Leave blank to run indefinitely.

Part 6: Save as draft

Fyscal ARCX → Transaction Monitoring → Typology → + New → Next Step → Save as Draft

Step 1 **Save the draft**

Click **Save as Draft** in the schedule card. Wait a few seconds: the page title changes to **Update Typology** (1). **Select Schedule** (2) now shows the new schedule, and the card shows the sentence “This rule will run every 1 day starting 08 Oct 2026, 09:00:00 am” (3). **Save as Draft** is replaced by **Update** (4), greyed out. **Dry Run** (5) is now available, and **Activate** (6) appears at the bottom right. Opened again after its start time has passed, as in the screenshot, the page also shows “Start time cannot be in the past” under **Start Time**; the saved draft is not affected.

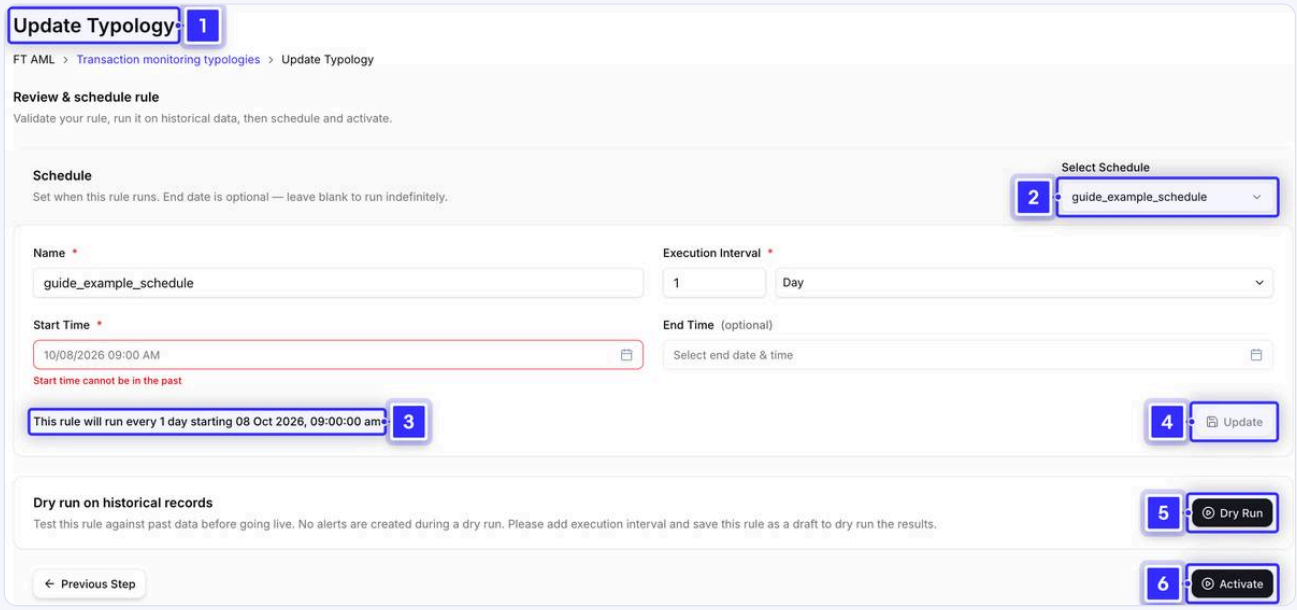


Figure 8.49 After Save as Draft: Update Typology (1), the schedule (2), the run summary (3), Update (4), Dry Run (5) and Activate (6)

Step 2 **Find the draft in the list**

Open **Transaction Monitoring → Typology**. The new rule is the first row; later, find it by typing its name in the search box (1). The row shows the name and rule ID (2) (TMR-07102026-001091 in the example), status **Draft** (3), typology **Velocity** (4) and its creation time (5).



Figure 8.50 The new rule found by name (1): rule ID (2), status Draft (3), Velocity (4) and creation time (5)

Step 3 **Check the rule page**

Click the row. The rule page shows the **Draft** chip and rule ID with the description (1), and the Draft actions **Delete**, **Update**, **Duplicate Typology**, **Activate** and **Timeline & Notes** (2). The summary strip (3) reads **EXECUTION PERIOD** 08 Oct 2026, 09:00:00 am → N/A, **INTERVAL** Every 1 day, **COMPLEXITY** Advanced, **SUPPRESSION** 7Day and **TYPOLOGY** Velocity. Group 1 (4) shows both conditions read-only, joined by **AND — all must match**. **VARIABLES** (5) has a card for each variable: the new one as Num_agg_sum and `sender_txn_count_7d` as Num_agg_count, both with **WINDOW** in last 7 day and **GROUP** `sender_entity_id`.

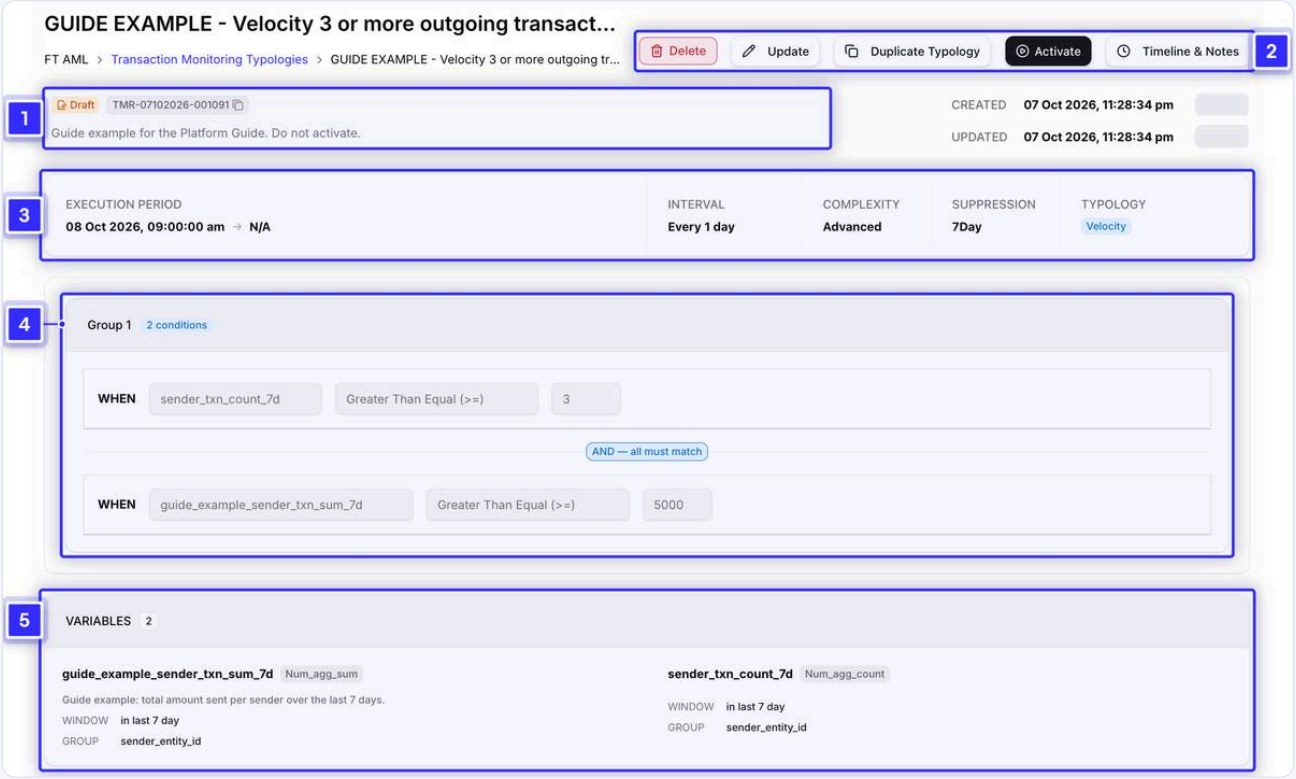


Figure 8.51 The draft rule page: Draft chip, ID and description (1), Draft actions (2), summary strip (3), Group 1 (4) and the two variables (5)

Step 4 **Check the new schedule**

Open **Transaction Monitoring → Schedules** and switch to **Schedule List**. The new schedule is the first row; later, find it by typing its name in the search box (1). The row shows its name and ID (2) (SCH-07102026-000397 in the example), **Last Executed** — (3), **Rules Linked** 1 (4) and status **Inactive** (5).



Figure 8.52 Schedule List searched by name (1): the new schedule (2), Last Executed — (3), Rules Linked 1 (4), Inactive (5)

Note

A Draft rule does not run. The next controls are **Dry Run** and **Activate** (Figure 8.49), described in Part 7.

Part 7: Next: test and activate

Fyscal ARCX → Transaction Monitoring → Typology → + New → Next Step → Save as Draft

These steps start from the **Update Typology** page in Figure 8.49.

Illustrated steps

The Typology Library shows these steps screen by screen: Test a typology with Dry Run and Request Shadow activation.

Step 1 **Run a dry run**

In **Dry run on historical records** (“Test this rule against past data before going live. No alerts are created during a dry run.”), click **Dry Run**. It is available once the execution interval is set and the rule is saved as a draft. The result shows **Time Windows**, **Records Scanned** and **Alert Created** in total and per window; **Re-run** repeats the test and **Hide Result** collapses it. The dry run offers no date choice: in the Typology Library tests, with a schedule that runs every 1 day, it covered the last four one-day windows. If Records Scanned is 0, there was no data in the tested dates. A result of 0 alerts does not prove the rule works; see Judge the result: 0 is not proof. If the alert count is more than your team can review, raise the thresholds and re-run.

Step 2 **Request activation**

Click **Activate**. In **Activation Mode** choose **Shadow Mode** (“Alert generated against live data will be shown in rule detail page.”) or **Published Mode** (“Alert from this rule will flow into Alert Manager.”). The **Submit Request** dialog asks for a **Reason** (required) and optional **Supporting Documents** (1 file, max 2 MB, .jpg, .jpeg, .jpe, .png, .pdf, .webp or .md) added with **Attach File**. Write a reason a reviewer can act on, for example “Velocity rule, 3 or more transactions totalling ₱5,000 in 7 days; dry run reviewed; start in Shadow”. Click **Confirm**.

Step 3 **Wait for approval**

Activation goes through Maker Checker Approval. The request appears as an **Activate Typology** ticket, with status Pending, in Maker Checker Approval → Tickets, where a checker reviews it. Until it is approved, the rule stays a **Draft** in the typology list.

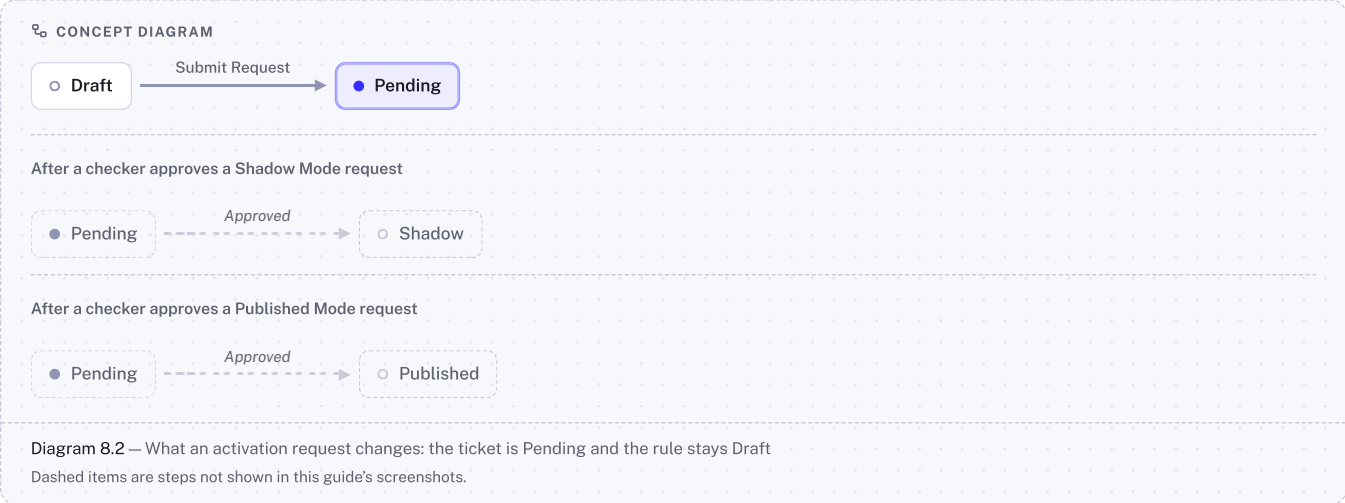


Diagram 8.2 — What an activation request changes: the ticket is Pending and the rule stays Draft

Dashed items are steps not shown in this guide’s screenshots.

The main track of Diagram 8.2 is what the screens show after **Confirm**. **Draft** is the rule's status; **Pending** is the status of the **Activate Typology** ticket in Maker Checker Approval. While the ticket is Pending, the rule's status is still **Draft**. The dashed branches use the statuses the typology list offers (**Shadow**, **Published**); an approval is not shown in this guide's screenshots.

Step 4 **Check the live rule**

Open the rule from the list. Its page shows the status (**Shadow** or **Published**), the execution period and interval from the schedule, and the conditions and variables. Use **Schedule Details** to see each run, and the **Shadow Alerts** and **Live Alerts** columns in Run History to see how many alerts each run raised. A paused rule shows **Paused** and a **Resume** button.

AML context

Running a new or changed rule in parallel with production, without sending its alerts to analysts, is a common way to check alert volume and quality before go-live.

How conditions are evaluated: an example

Each run calculates every variable once per **Group by** value (here, per sender) over its window, ending at the trigger time T. Then each group is checked.

Example: at a run on 10 Jul, sender A’s outgoing remittances in the last 14 days were as below, and the run calculated the variable values in the second table.

Date	Amount
09 Jul	₱2,000
09 Jul	₱3,500
09 Jul	₱1,500
09 Jul	₱2,500
09 Jul	₱3,000
01 Jul	₱8,000

Variable	Value for sender A
outgoing remittance 1 day sum	₱12,500
outgoing remittance 1 day vol	5
outgoing remittance 14 day sum	₱20,500
outgoing remittance 14 day vol	6

1. Group 1: 1 day vol 5 >= 5 is true, AND 1 day sum ₱12,500 >= 10000 is true. Group 1 is true.
2. Group 2: 14 day vol 6 >= 5 is true, AND 14 day sum ₱20,500 >= 20000 is true. Group 2 is true.
3. Groups are combined with OR, so one true group is enough: the rule raises an alert for sender A.

The rule also has a **Suppression Window** of 2 Day (see Create Typology form).

If sender A had made no transactions at all in a variable's window, that variable would have no value for A, not 0. A condition such as **Equal** 0 then never matches, and **Is Null** is not saved in a typology condition. To test for “no transactions”, compare with the variable through a large multiplier, as the Typology Library's Rule 4 shows.

A **variable** only calculates a value. A **condition** decides whether that value is suspicious. Keeping them separate is what lets one variable serve many rules.

RELATED IN DETECTION & MONITORING

Name Screening | Typology Library | Data Ingestion

DETECTION & MONITORING

9 Typology Library

Fyscal ARCX → Transaction Monitoring → Typology

Fifteen typologies for patterns that standard AML rule libraries cover: structuring, velocity, high value, dormant accounts, fan-out, fan-in, large single payments, smurfing, spikes against a customer's own history, many devices, IP addresses, instruments, currencies and destination countries, and cross-border volume. Every rule here was built in Fyscal ARCX, tested with a dry run and submitted for Shadow activation, and each step shows the screen it was done on. Follow a rule step by step, then adjust its numbers to your own risk policy.

FOR	IN THE MENU	READING TIME
Administrators	Fyscal ARCX → Transaction Monitoring → Variables and Typology	About 2 h

Building blocks: what the variable and typology forms can express, time windows, empty values, AND and OR, and how to read a dry run of 0 alerts.

Rule index: all fifteen rules compared on one page, with their dry-run results.

Before you build: the schedule, naming and activation rules that apply to every typology.

Rule 1 · Structuring: several transactions just below an amount you review.

Rule 2 · Velocity: an unusually high number of transactions in one day.

Rule 3 · High value: a large total sent within 30 days.

Rule 4 · Dormant account: no activity for 100 days, then a sudden payment.

Rule 5 · Fan-out: one sender paying many different receivers.

Rule 6 · Fan-in: many different senders paying one receiver.

Rule 7 · Large single transaction: one very large payment in a day.

Rule 8 · Smurfing: many very small payments in a day.

Rule 9 · Spike against own history: a week's total that is large against the customer's 90 days.

Rule 10 · Many devices: one sender using several devices.

Rule 11 · Many IP addresses: one sender using many IP addresses.

Rule 12 · Many instruments: one sender paying from many cards or accounts.

Rule 13 · Many currencies: one sender using several currencies.

Rule 14 · Many destination countries: payments to receivers in several countries.

Rule 15 · Cross-border volume: a large total sent abroad within 30 days.

Test a typology with Dry Run: run a draft on past records, judge the result and tune it.

Request Shadow activation: submit a draft for approval in Shadow Mode.

Tuning and false positives: what to adjust in each rule and the ordinary activity that sets it off.

Proposed typologies: further rules built from the same parts, not yet tested.

About the examples

The screenshots come from building these rules in Fyscal ARCX. There, each example is named with a **GUIDE EXAMPLE** (typology) or **guide_example_** (variable and schedule) prefix so it can be told apart from real rules. Each example name also carries the build number used on the test system (R01 to R06 and R09 to R17); the Rule index maps them to the rule numbers here. In the text the names are shown without the prefix: use your own names. All amounts are in pesos (₱) and are starting values, not recommendations; set them from your own risk assessment.

Building blocks

Every rule in this chapter is made from the same few parts. This table lists what the forms offer, as seen while building the rules. For a tour of each form, see Build a typology from scratch.

Part	Where	What you can set
Field	Create Variables → Aggregation	One of the transaction fields, for example `amount`, `id`, `sender_entity_id`, `receiver_entity_id`, `sender_amount`, `receiver_amount`, `receiver_provider_country`.
Function	Create Variables → Aggregation	Depends on the field. Numeric fields such as `amount` offer **Count**, **Count Distinct**, **Sum**, **Average**, **Minimum** and **Maximum**. Text and ID fields such as `id` or `receiver_entity_id` offer only **Count**, **Count Distinct**, **Minimum** and **Maximum**.
Group by	Create Variables → Aggregation	The field the result is calculated per, usually `sender_entity_id` (per sender) or `receiver_entity_id` (per receiver).
Time Window	Create Variables	A unit (**Hours**, **Days**, **Weeks**, **Months**, **Years**) and a range "Analyze Transaction from *X* to *Y* ... ago". The range can end before now: **100 to 1 Days** covers the 100 days up to yesterday.
Filters	Create Variables → Filters (optional)	Rows of *field · operator · value*, combined as "AND — all must match". Number fields: Equal, Not Equal, Greater Than, Greater Than Equal, Less Than, Less Than Equal, Between, Not Between, In, Not In. Text fields: Equal, Not Equal, In, Not In, Contains, Not Contains, Starts With, Ends With, Is Null, Is Not Null. **In** takes a list (type a value and press Enter for each). **Static** compares with a value you type; **Dynamic** compares with another field.
Condition	Create Typology → Group	**WHEN** a variable, an operator, and a comparison with a **Static Value** or another **Variable**. When you compare with a variable, a **THAN MULTIPLIER** box lets you compare with a fraction or multiple of it (for example 0.9 for 90%).
Groups	Create Typology	Rows in a group are combined with **Match** AND or OR; several groups are combined with **Combine groups with** AND or OR.
Typology type	Create Typology	A category from the list, for example Structuring (TP100), Velocity (V-01), High Value (HV01), Cardinality (C-01), Large Transaction (LT-01), Anomaly (TP103).
Suppression Window	Create Typology	A number and a unit (Hour, Day, Week, Month, Year).

> **Note**
> The rules in this chapter set the **Suppression Window** to the same length as their variable window.

Time windows

A variable's window is counted back from the trigger time T of each run. The first number is where the window starts and the second where it ends, both in days (or the chosen unit) before T. Diagram 9.1 places the three kinds of window used in this chapter on one line.

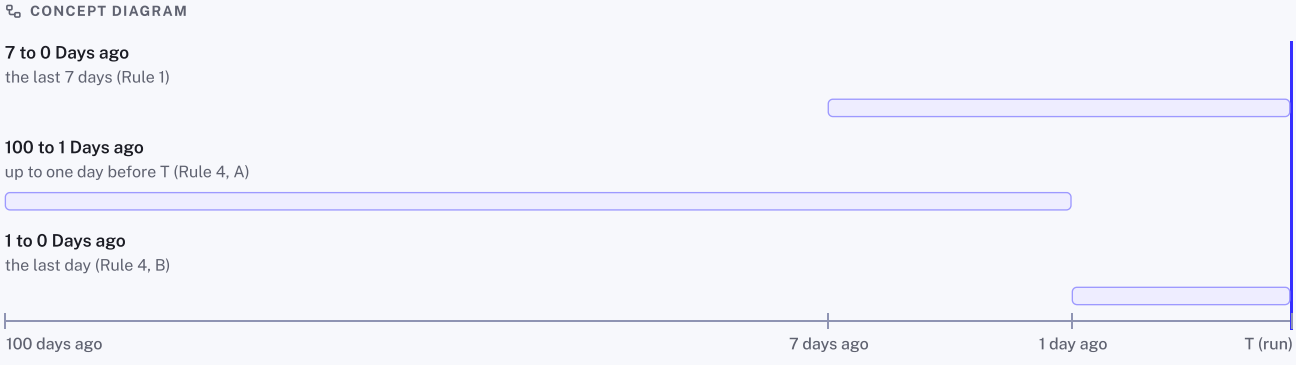


Diagram 9.1 — Variable windows counted back from the trigger time T (not to scale)

7 to 0 Days ago covers the last 7 days up to T. Most rules here use a window that ends at 0.

100 to 1 Days ago ends one day before T, so it leaves out the most recent day. The form's timeline then reads **1 day ago**. On a typology page the variable card shows only the start ("in last 100 day"); check the end on **View Variable**.

1 to 0 Days ago covers only the most recent day. Rule 4 pairs it with the 100-to-1 window: the two windows meet at "1 day ago" and do not overlap, so "no activity before, then a payment now" can be tested.

An empty value is not 0

When a customer has no transactions in a variable's window, the variable has no value for that customer: it is empty, not 0. A comparison with a fixed number, such as **Equal** 0 or **Less Than Equal** 0, therefore does not match that customer.

The operator list also offers **Is Null** and **Is Not Null**, but do not use them in a typology condition: the condition is not saved with the rule, and the rule runs without it. No message is shown, and the rule page then lists only the other conditions.

When one variable is compared with another, an empty value counts as 0. Rule 4 uses this to test for "no transactions": it compares the amount sent in the last day with the earlier transaction count multiplied by 1,000,000,000,000. One earlier transaction makes that product far larger than any amount, so the condition fails. No earlier transaction makes it 0, so the condition passes.

Condition on a Count variable	Sender with 4 transactions in the window	Sender with no transactions in the window
Value of the variable	4	Empty (no value)
Equal 0 matches	✕ No	✕ No Rule 4 first version: 0 alerts
Greater Than Equal 0 matches	✓ Yes	✕ No Test with no matching transactions: 0 alerts
Is Null in a typology condition	✕ Not saved	✕ Not saved Rule 4 second version ran as "≥ ₱5,000" only
Last-day sum **Greater Than Equal** the count × 1,000,000,000,000 (Rule 4)	✕ No	✓ Yes Rule 4: 279 alerts

How AND and OR combine conditions

Inside a group, **Match** decides how the rows combine; the form and the rule page print the choice between the rows as **AND — all must match** or **OR — any one matches**. For two conditions A and B on the same sender:

Condition A	Condition B	Match AND: alert	Match OR: alert
True	True	✓ Yes	✓ Yes
True	False	✕ No	✓ Yes
False	True	✕ No	✓ Yes
False	False	✕ No	✕ No

Groups combine the same way, following **Combine groups with**. The rule in Typology detail (Figure 8.6) has **AND — all must match** inside each group and **OR — any one matches** between its three groups: it alerts when any one group is fully true. Every rule in this chapter uses a single group; Rules 4 and 9 have two conditions joined by AND.

Reading a dry run of 0 alerts

A dry run that creates 0 alerts can mean that the test period has no such pattern, or that the rule cannot read the data. A positive control tells them apart: lower the threshold for one run so that any matching record would alert, then restore it. The method is shown step by step in Test a typology with Dry Run.

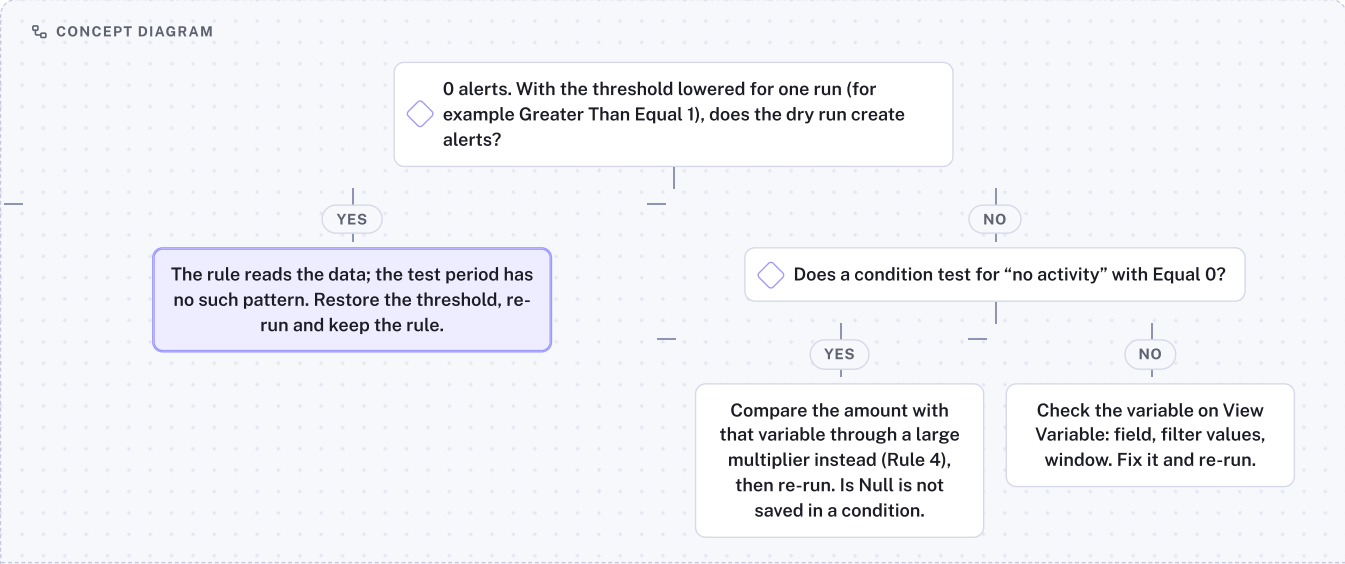


Diagram 9.2 — Does a rule with 0 alerts work? The positive-control check

Nine of the fifteen rules in this chapter created 0 alerts at their real threshold, and every one of them created alerts in its positive control (see the Rule index). A control only shows that the variable reads data: for Rule 13 it shows that `currency_code` is filled in, not that any sender uses several currencies.

Rule index

All fifteen rules at a glance. **Entity** is the field the variables are grouped by: `sender_entity_id` (per sender) for every rule except Rule 6, which uses `receiver_entity_id` (per receiver). **Dry run** gives the alerts created at the rule's real threshold; where that was 0, **Control** gives the result with the threshold lowered for one run (see Test a typology with Dry Run).

> **Screenshot labels**
> On the test system the rules were built under build numbers R01 to R17, and every screenshot carries that number in the example name. Rules 1 to 6 here are R01 to R06; Rules 7 to 15 are R09 to R17. R07 and R08 are not part of this chapter. The first column gives each rule's build number.

Rule (screens)	Red flag	Entity	Variable type	Window	Threshold	Dry run	Control	Verdict
1 · Structuring (R01)	Several payments just under an amount you review	Sender	STR_AGG_COUNT, two amount filters	7 to 0 Days	≥ 3 between ₱450,000 and ₱499,999	0	≥ 1: 4	Works; pa not in test data
2 · Velocity (R02)	A burst of transactions in a day	Sender	STR_AGG_COUNT	1 to 0 Days	≥ 10	0	≥ 1: 764	Works; pa not in test data
3 · High value (R03)	A large total sent in 30 days	Sender	NUM_AGG_SUM	30 to 0 Days	≥ ₱5,000,000	0	≥ 1: 6,512	Works; pa not in test data
4 · Dormant account (R04)	Activity after a long quiet period	Sender	STR_AGG_COUNT and NUM_AGG_SUM	100 to 1 Days and 1 to 0 Days	Sum ≥ ₱5,000 AND sum ≥ 1,000,000,000,000 × count	279	Not needed	Fires
5 · Fan-out (R05)	One sender paying many receivers	Sender	STR_AGG_COUNT_DISTINCT	7 to 0 Days	≥ 10 receivers	240	Not needed	Fires

Rule (screens)	Red flag	Entity	Variable type	Window	Threshold	Dry run	Control	Verdict
6 · Fan-in (R06)	Many senders paying one receiver	Receiver	STR_AGG_COUNT_DISTINCT	7 to 0 Days	≥ 10 senders	240	Not needed	Fires
7 · Large single transaction (R09)	One very large payment	Sender	NUM_AGG_MAX	1 to 0 Days	≥ ₱1,000,000	0	≥ 1: 764	Works; pa not in test data
8 · Smurfing (R10)	Many very small payments in a day	Sender	STR_AGG_COUNT, amount filter	1 to 0 Days	≥ 20 under ₱1,000	0	≥ 1: 339	Works; pa not in test data
9 · Spike against own history (R11)	A week that is large against the sender's 90 days	Sender	NUM_AGG_SUM (two variables)	7 to 0 Days and 90 to 0 Days	7-day ≥ ₱100,000 AND ≥ 0.5 × 90-day	42	Not needed	Fires
10 · Many devices (R12)	One account used from many devices	Sender	STR_AGG_COUNT_DISTINCT	7 to 0 Days	≥ 3 devices	0	≥ 1: 4,043	Works; pa not in test data
11 · Many IP addresses (R13)	One account used from many network locations	Sender	STR_AGG_COUNT_DISTINCT	7 to 0 Days	≥ 15 IP addresses	120 (758 at ≥ 5)	Not needed	Fires; threshold tuned
12 · Many instruments (R14)	Payments funded from many cards or accounts	Sender	STR_AGG_COUNT_DISTINCT	7 to 0 Days	≥ 5 instruments	0	≥ 1: 4,615	Works; pa not in test data
13 · Many currencies (R15)	Switching between currencies	Sender	STR_AGG_COUNT_DISTINCT	30 to 0 Days	≥ 3 currencies	0	≥ 1: 6,512	Works; the control on shows tha currency_ is filled in
14 · Many destination countries (R16)	Payments spread across countries	Sender	STR_AGG_COUNT_DISTINCT	30 to 0 Days	≥ 3 countries	94	Not needed	Fires
15 · Cross-border volume (R17)	A large total sent abroad	Sender	NUM_AGG_SUM, Dynamic country filter	30 to 0 Days	≥ ₱1,000,000	0	≥ 1: 991	Works; pa not in test data

About the test data

Every dry run covered the same four one-day windows, 04 Oct 2026, 09:00 am to 08 Oct 2026, 09:00 am, and scanned 1,560 records. Only two of the four windows held records (1,140 and 420); the two newest windows scanned 0. A rule with a 7- or 30-day variable can still alert in a window that scanned 0 records, because its variable looks further back than the window (Rule 5 created 60 alerts in each window). The counts show that a rule works on this data; they are not the alert volume to expect on your own data.

The variables and conditions of each rule:

Rule	Variables	Condition	Type · suppression
1 · Structuring (R01)	`struct_count_7d` : Count of transactions, last 7 days, amount ≥ 450,000 and < 500,000	≥ 3	Structuring (TP100) · 7 Day
2 · Velocity (R02)	`txn_count_1d` : Count of transactions, last 1 day	≥ 10	Velocity (V-01) · 1 Day
3 · High value (R03)	`sent_sum_30d` : Sum of amount, last 30 days	≥ 5,000,000	High Value (HV01) · 30 Day
4 · Dormant account (R04)	`count_100d_to_1d` : Count, 100 to 1 days ago · `sent_sum_1d` : Sum of amount, last 1 day	second ≥ 5,000 AND second ≥ 1,000,000,000,000 × first	Anomaly (TP103) · 1 Day
5 · Fan-out (R05)	`distinct_receivers_7d` : Count Distinct of receivers, last 7 days	≥ 10	Cardinality (C-01) · 7 Day
6 · Fan-in (R06)	`distinct_senders_7d` : Count Distinct of senders per receiver, last 7 days	≥ 10	Cardinality (C-01) · 7 Day
7 · Large single transaction (R09)	`max_amount_1d` : Maximum of amount, last 1 day	≥ 1,000,000	Large Transaction (LT-01) · 1 Day
8 · Smurfing (R10)	`small_txn_count_1d` : Count of transactions, last 1 day, amount < 1,000	≥ 20	Structuring (TP100) · 1 Day
9 · Spike against own history (R11)	`sent_sum_7d_spike` : Sum, last 7 days · `sent_sum_90d` : Sum, last 90 days	7-day ≥ 100,000 AND 7-day ≥ 90-day × 0.5	Anomaly (TP103) · 7 Day
10 · Many devices (R12)	`distinct_devices_7d` : Count Distinct of sender_device_id, last 7 days	≥ 3	Anomaly (TP103) · 7 Day
11 · Many IP addresses (R13)	`distinct_ips_7d` : Count Distinct of sender_ip, last 7 days	≥ 15	Anomaly (TP103) · 7 Day
12 · Many instruments (R14)	`distinct_instruments_7d` : Count Distinct of sender_instrument_id, last 7 days	≥ 5	Cardinality (C-01) · 7 Day
13 · Many currencies (R15)	`distinct_currencies_30d` : Count Distinct of currency_code, last 30 days	≥ 3	Anomaly (TP103) · 30 Day
14 · Many destination countries (R16)	`distinct_dest_countries_30d` : Count Distinct of receiver_provider_country, last 30 days	≥ 3	Anomaly (TP103) · 30 Day
15 · Cross-border volume (R17)	`crossborder_sum_30d` : Sum of amount, last 30 days, receiver country ≠ sender country	≥ 1,000,000	High Value (HV01) · 30 Day

Before you build

These points apply to every rule in this chapter.

- **Create variables first.** A typology's conditions can only pick variables that already exist.
- **Names.** Typology names can contain only letters, digits, spaces, hyphens, underscores and parentheses, so write amounts as "PHP 5000" rather than "₱5,000". A name must be 3 to 100 characters (see Rule 9).
- **A schedule with a future start.** Save as Draft stays disabled until you choose a schedule whose start time is in the future. Rule 1 creates a daily schedule; the other rules reuse it. Its start was later moved from 01 Jan 2027 to 09 Oct 2026, 09:00 AM (Rule 1, step 31); screenshots taken before the change still show 01/01/2027. Choosing an existing schedule shows its fields in the form; those fields belong to that schedule, which other rules may also use.
- **Saving.** After **Save as Draft**, wait a few seconds: the page becomes **Update Typology** and the rule is listed as **Draft**.
- **Before it goes live.** Test each rule with **Dry Run** (see Test a typology with Dry Run) and request activation, which goes through Maker Checker Approval (see Request Shadow activation).

Rule 1 · Structuring

RED FLAG **Several payments just under an amount you review**

LOGIC

Counts the sender's transactions of ₱450,000 up to ₱499,999 in the last 7 days.

WINDOW	THRESHOLD
7 to 0 Days	≥ 3 between ₱450,000 and ₱499,999

✓ Verified by positive control

What it detects and why. This rule flags a sender who makes three or more transactions within 7 days, each from ₱450,000 up to just under ₱500,000. Several payments that each stay just below an amount you want reviewed can be one larger sum split up to avoid that review, so the pattern is worth a look even when no single payment stands out.

This is the most detailed of the rules: it shows every screen once, including the schedule that the other rules reuse. In the screenshots every example object carries the **GUIDE EXAMPLE** or `guide_example_` prefix; the text gives the names without it (see Before you build). For a tour of each form, see Build a typology from scratch.

Item	Setting
Variable `struct_count_7d`	**Count** of `id` (the number of transactions), grouped by `sender_entity_id`, **Days** from 7 to 0, filters `amount` **Greater Than Equal** 450000 AND `amount` **Less Than** 500000
Typology type	Structuring (TP100)
Suppression Window	7 Day
Condition	Group 1, Match AND: `struct_count_7d` **Greater Than Equal (>=)** Static Value 3
Schedule	New schedule `schedule_2027` : every 1 Day, no end time; created with the start 01 Jan 2027, 09:00 AM and later moved to 09 Oct 2026, 09:00 AM (step 31)

Part A: Create the variable

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 1 **Open the form and name the variable**

Go to **Transaction Monitoring → Variables** and click **+ New**. In **Create Variables**, leave **Transaction** selected. In **Variable name** (1) type `struct_count_7d`. In **Description** (2) write what the number means, for example “Number of transactions per sender between PHP 450000 and 500000 in the last 7 days.” The name says what is counted and over which window, so it is easy to pick later in a condition.



Figure 9.1 Create Variables: Variable name and Description filled in

Step 2 **Choose the Field: id**

Open **Field**. The list has a **Search Fields** box and the 51 transaction fields. Choose `id`. Every transaction has one `id`, so counting `id` values counts transactions.

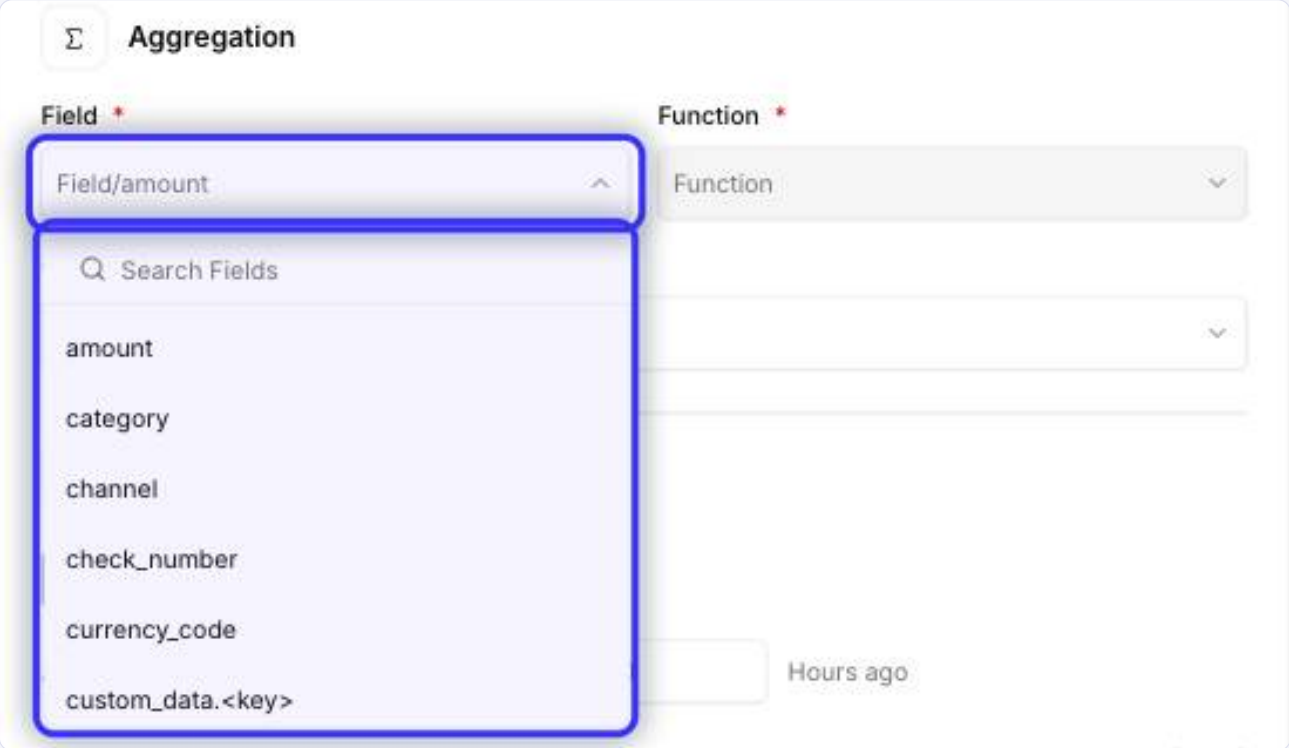


Figure 9.2 The Field list, before id is chosen

Step 3 **Choose the Function: Count**

Open **Function**. Because `id` is an ID field, the list offers only **Count**, **Count Distinct**, **Minimum** and **Maximum**; **Sum** and **Average** appear only for numeric fields such as `amount`. Choose **Count**: the rule needs the number of qualifying transactions.

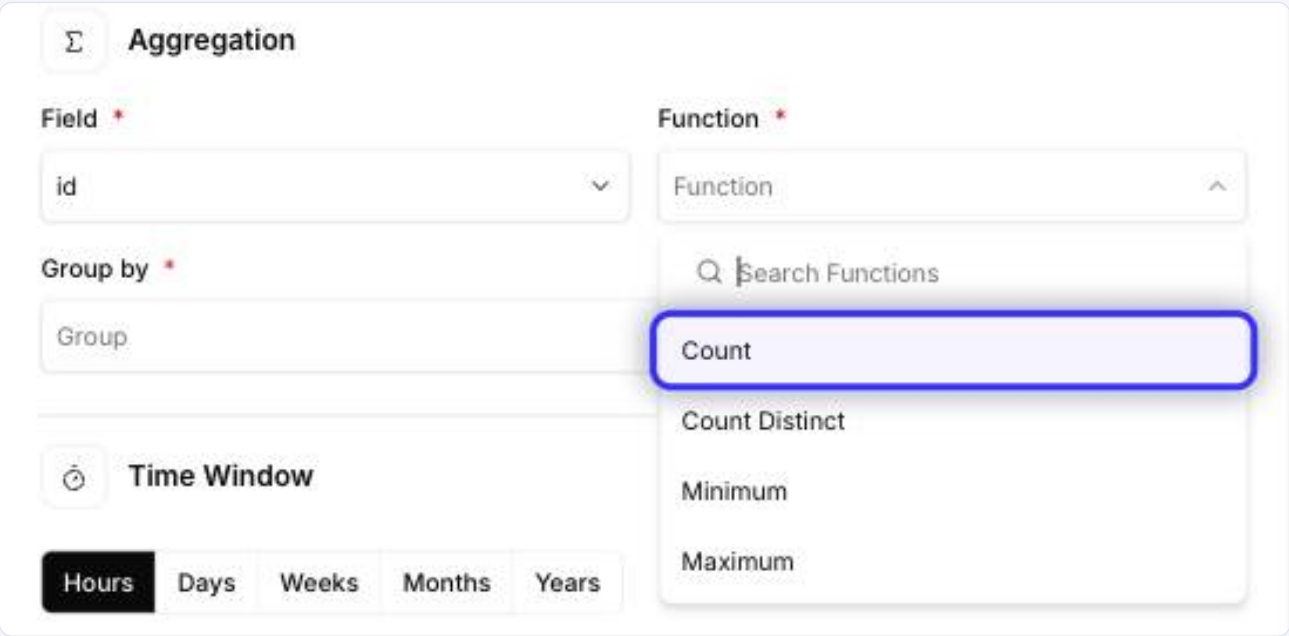


Figure 9.3 Function for the id field: Count, Count Distinct, Minimum, Maximum

Step 4 **Choose Group by: sender_entity_id**

Open **Group by**, type `sender_entity` in **Search Fields** and choose `sender_entity_id`. The count is then calculated separately for each sender, which is what makes it a per-customer measure.

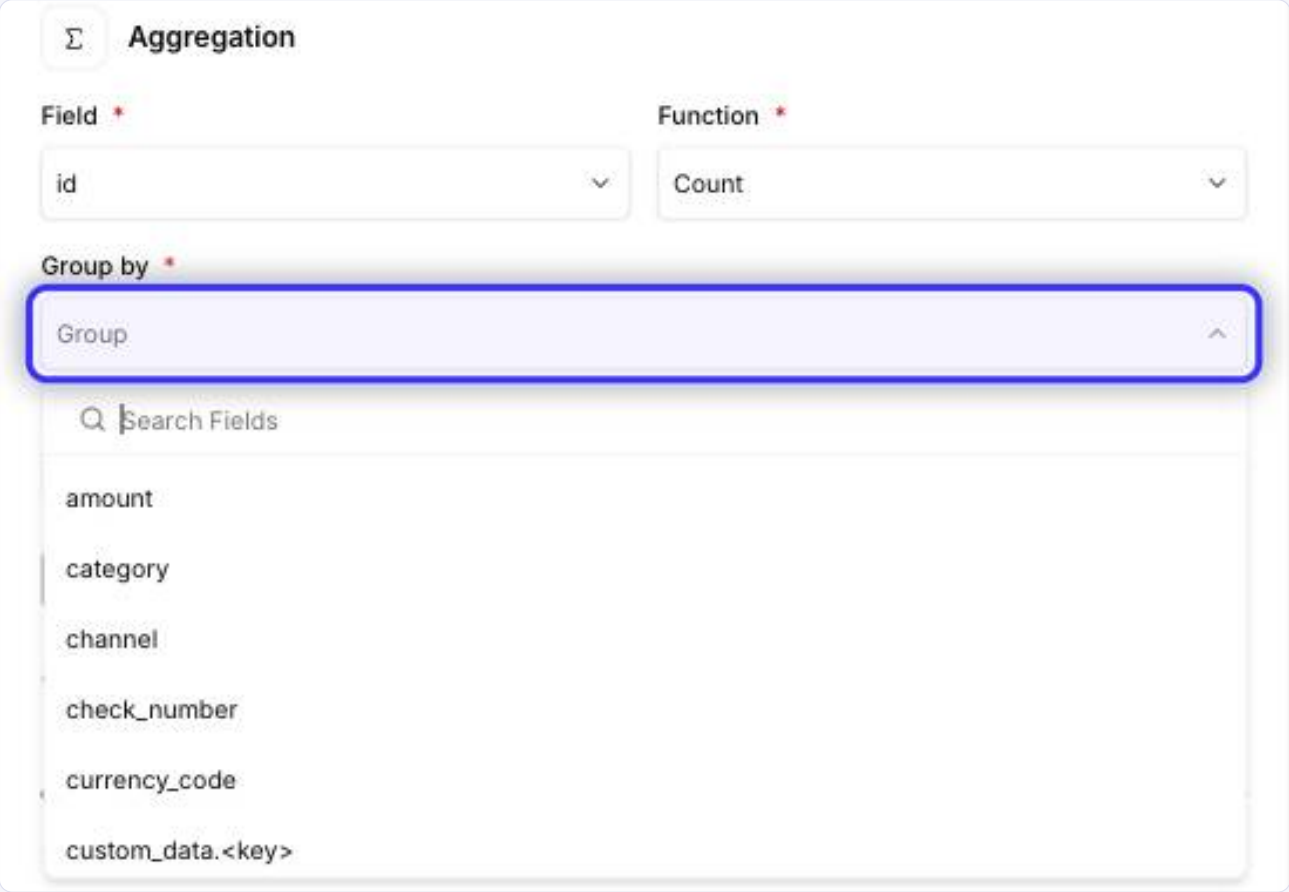


Figure 9.4 The Group by list

Step 5 **Set the time window: Days, 7 to 0**

Scroll down. **Group by** now reads `sender_entity_id` (1). Under **Time Window**, click **Days** (2); the default is **Hours**. In **Analyze Transaction from** enter 7 and in **to** enter 0 (3). The line reads “from 7 to 0 Days ago”: the 7 days up to the trigger time, shown as “Triggered at T (00:00)”.

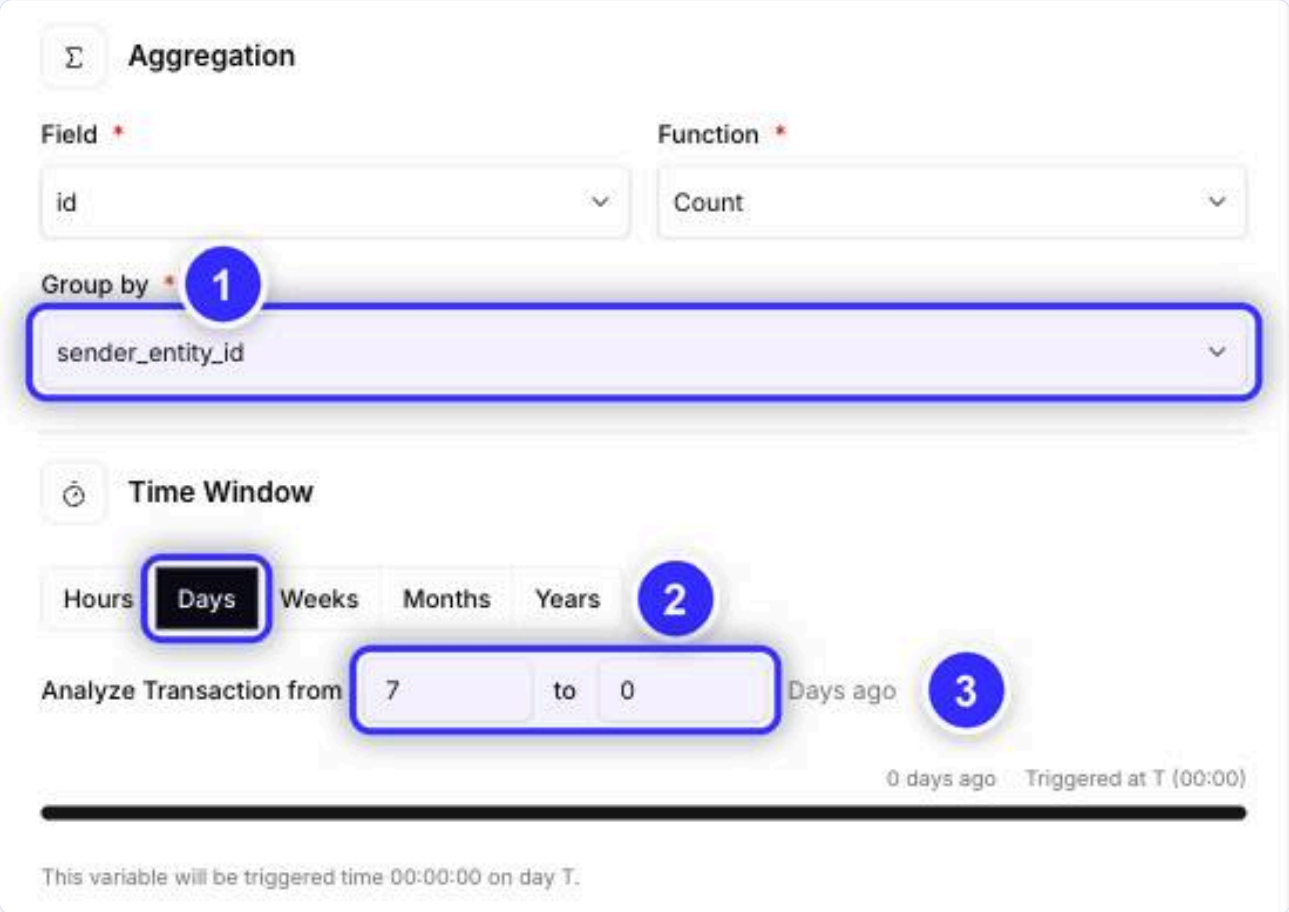


Figure 9.5 Group by set, and the time window set to 7 to 0 Days ago

Step 6 **Add filter 1: choose the amount field**

Under **Filters (1)** *(optional)*, open **Field** in the blank row and type `amount`. Four fields match: `amount`, `orig_currency_amount`, `receiver_amount` and `sender_amount`. Choose `amount`. The filters decide which transactions are counted; without them every transaction would count.

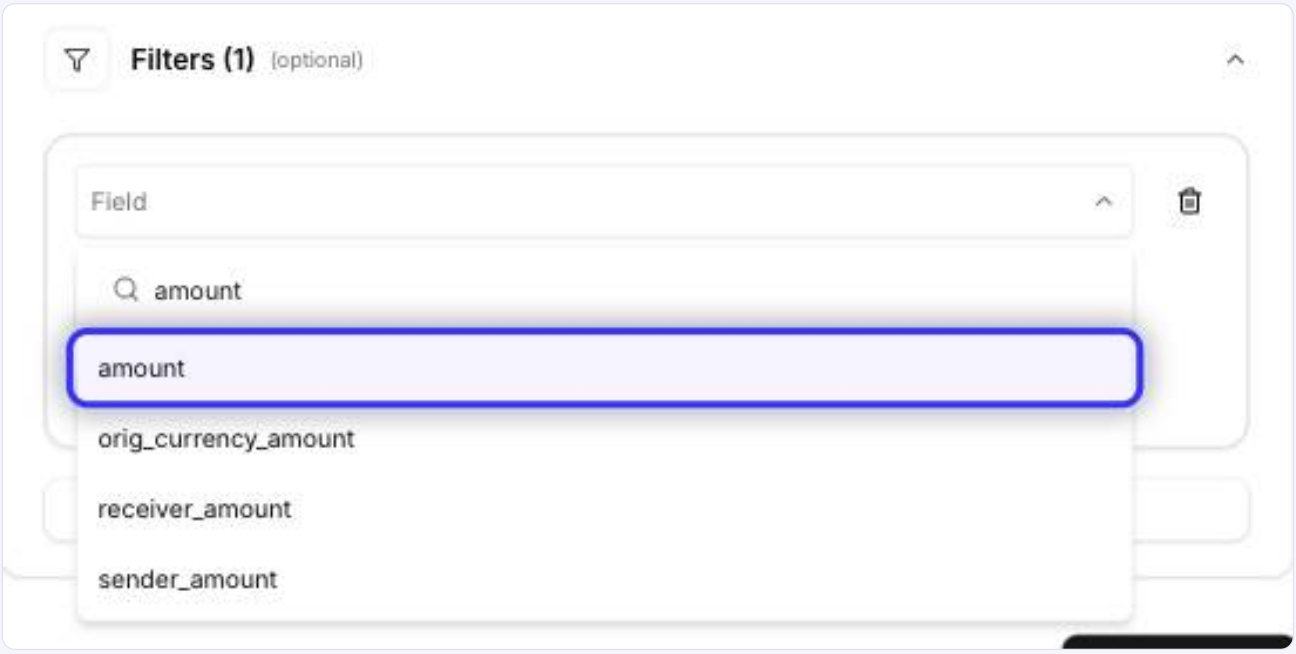


Figure 9.6 Filter row 1: the field search for amount

Step 7 **Filter 1: choose Greater Than Equal and type 450000**

Open **Operator...**. For a number field the list is **Equal**, **Not Equal**, **Greater Than**, **Greater Than Equal**, **Less Than**, **Less Than Equal**, **Between**, **Not Between**, **In** and **Not In** (scroll for the last four). Choose **Greater Than Equal**, then type 450000 in **Enter value**. This sets the lower edge of the band: ₱450,000 itself is counted.

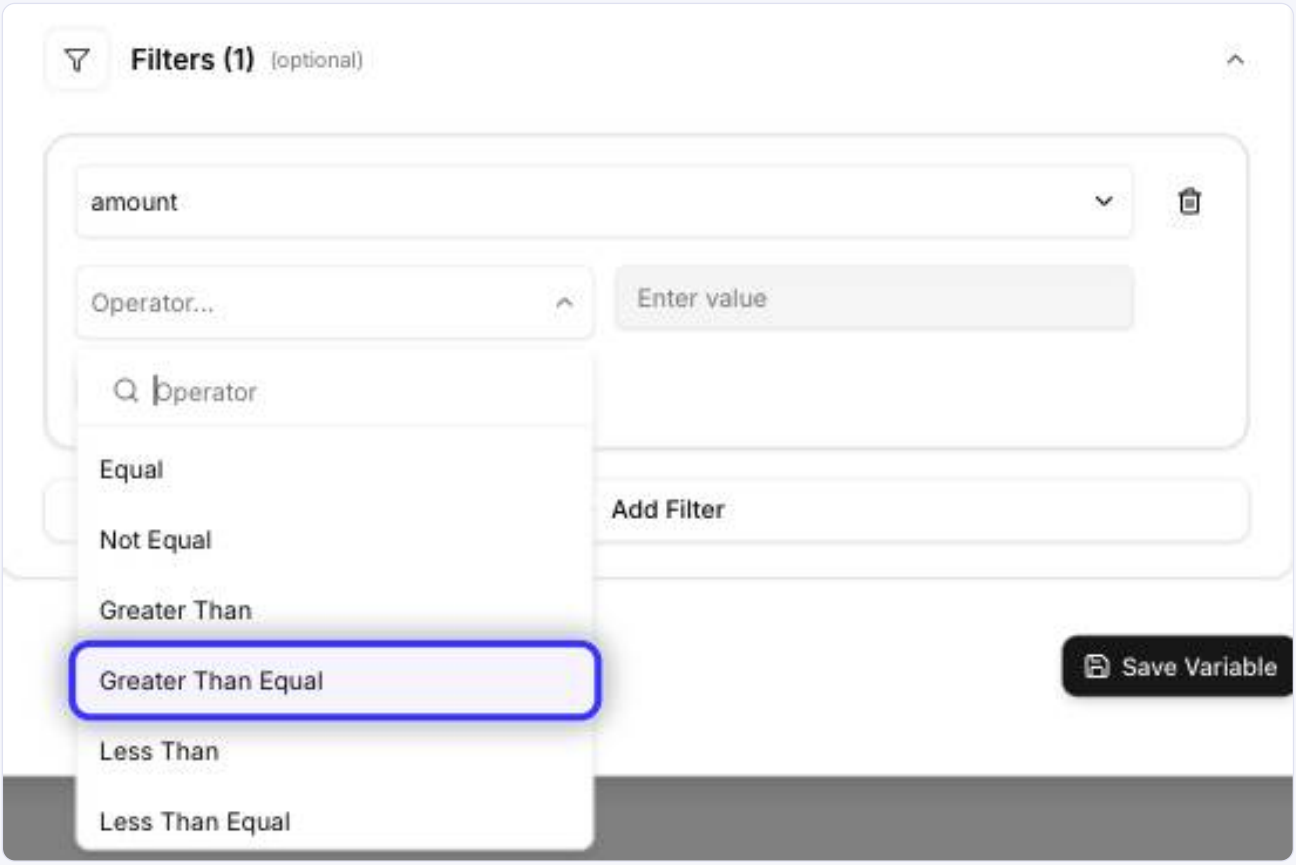


Figure 9.7 Filter operators for a number field

Step 8 **Why not Between**

Choosing **Between** (1) replaces the value box with **From** and **To** (2). The screen does not say whether Between includes its end values, so this rule uses two rows with explicit operators instead. Under every row is a **Static** / **Dynamic** toggle (3): **Static** compares with a value you type.

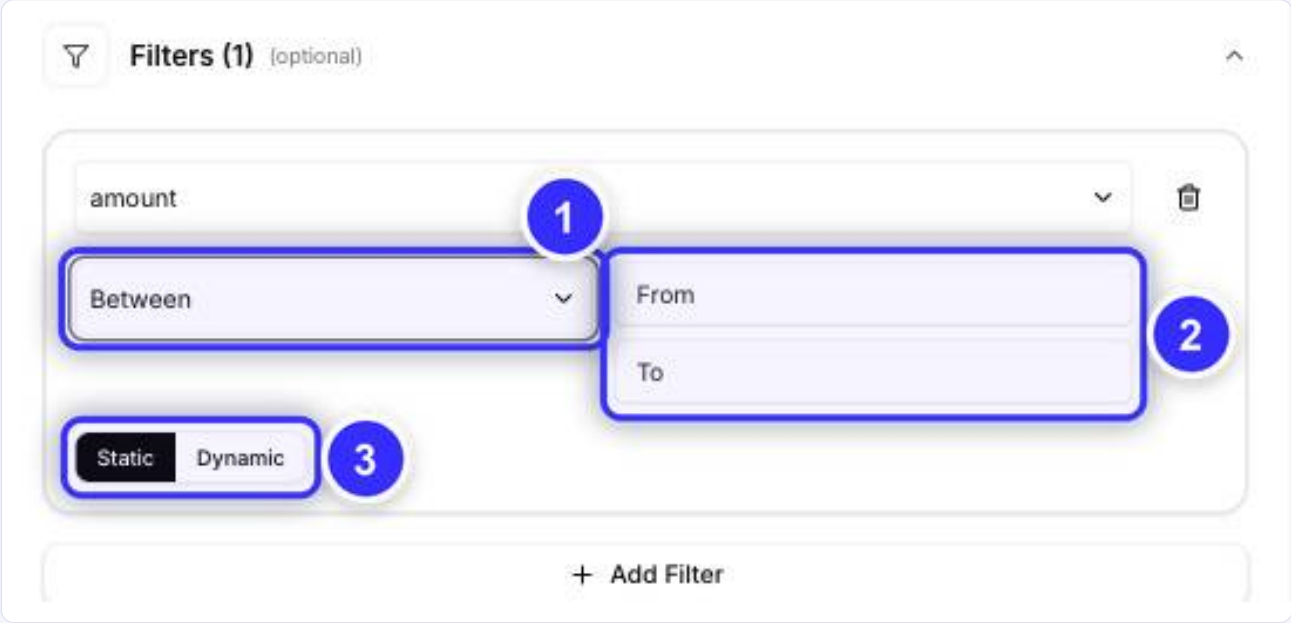


Figure 9.8 Between shows From and To boxes; the Static and Dynamic toggle

Step 9 **Add filter 2: amount Less Than 500000**

With row 1 reading `amount` **Greater Than Equal** 450000 (1), click **Add Filter**. A second row appears, joined to the first by **AND — all must match** (2): a transaction is counted only if it passes both rows. Choose `amount`, open the operator list, type `Less Than` and choose **Less Than** (3). Type 500000. ₱500,000 itself is not counted, so the band is ₱450,000 up to, but not including, ₱500,000.

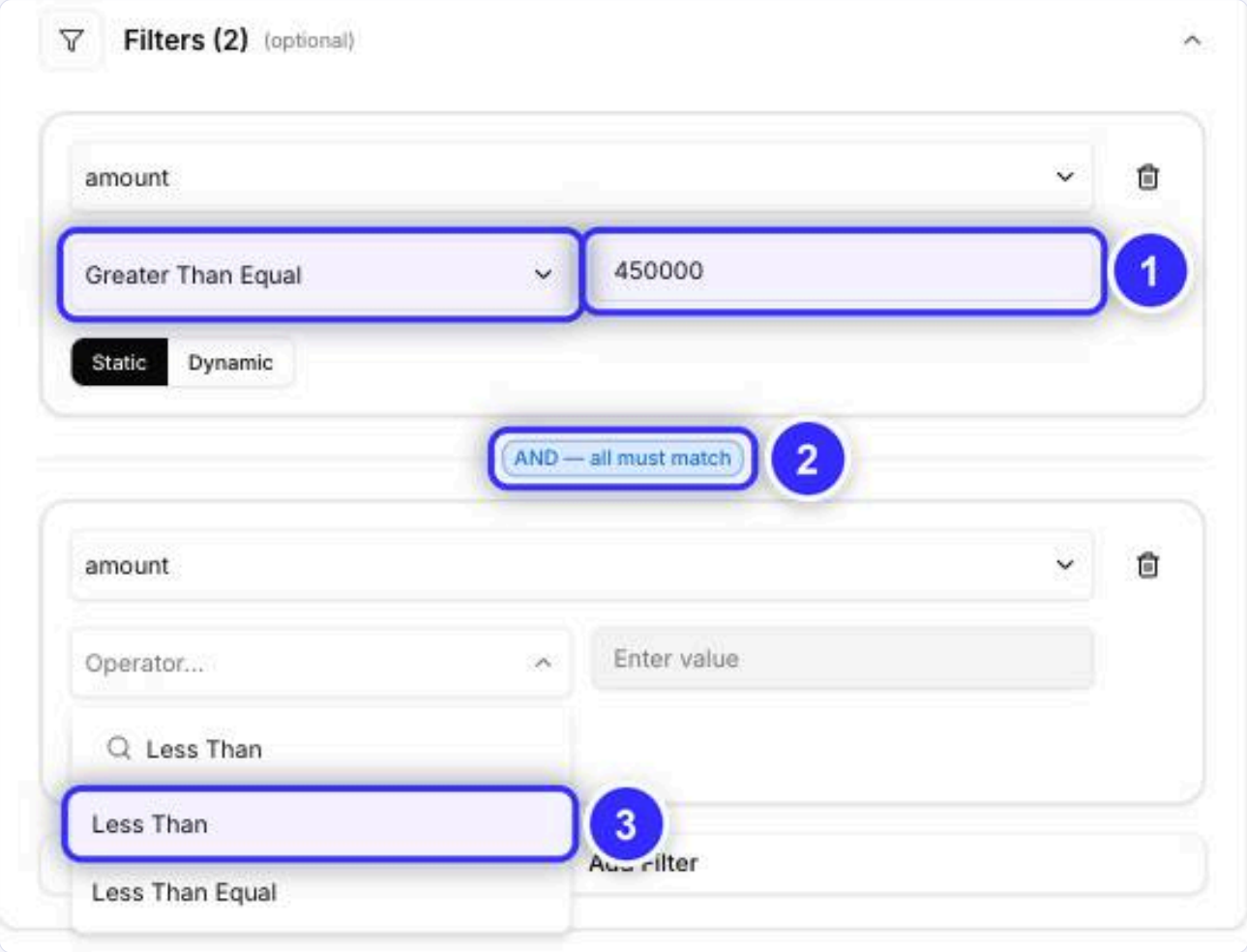


Figure 9.9 Filter row 2 added, joined by AND — all must match

Step 10 **Keep Static**

Clicking **Dynamic** (1) changes the value box to **Field...**, a list of other numeric fields to compare with: `mode_of_transaction`, `orig_currency_amount`, `receiver_amount` and `sender_amount` (2). This rule compares with fixed amounts, so switch the row back to **Static** and keep 500000.

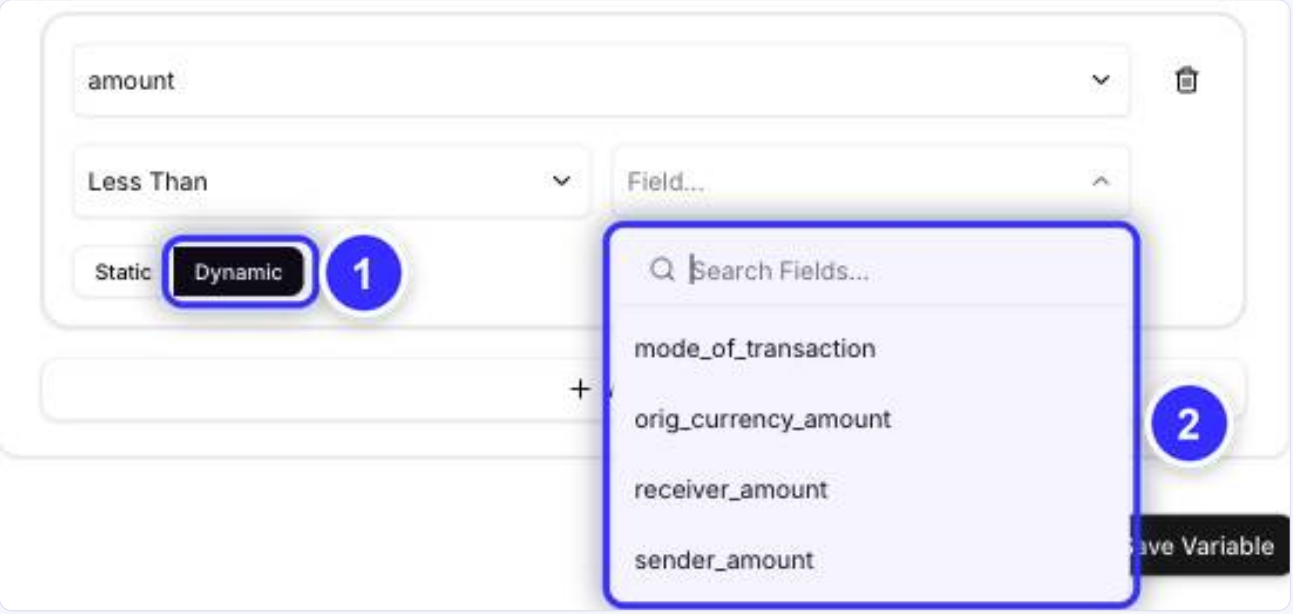


Figure 9.10 Dynamic compares with another numeric field

Step 11 **Check the form and save**

Check the whole form: `id` / **Count** / `sender_entity_id` (1), **Days** 7 to 0 (2), and **Filters (2)** with both rows set to **Static** (3). Click **Save Variable** (4).

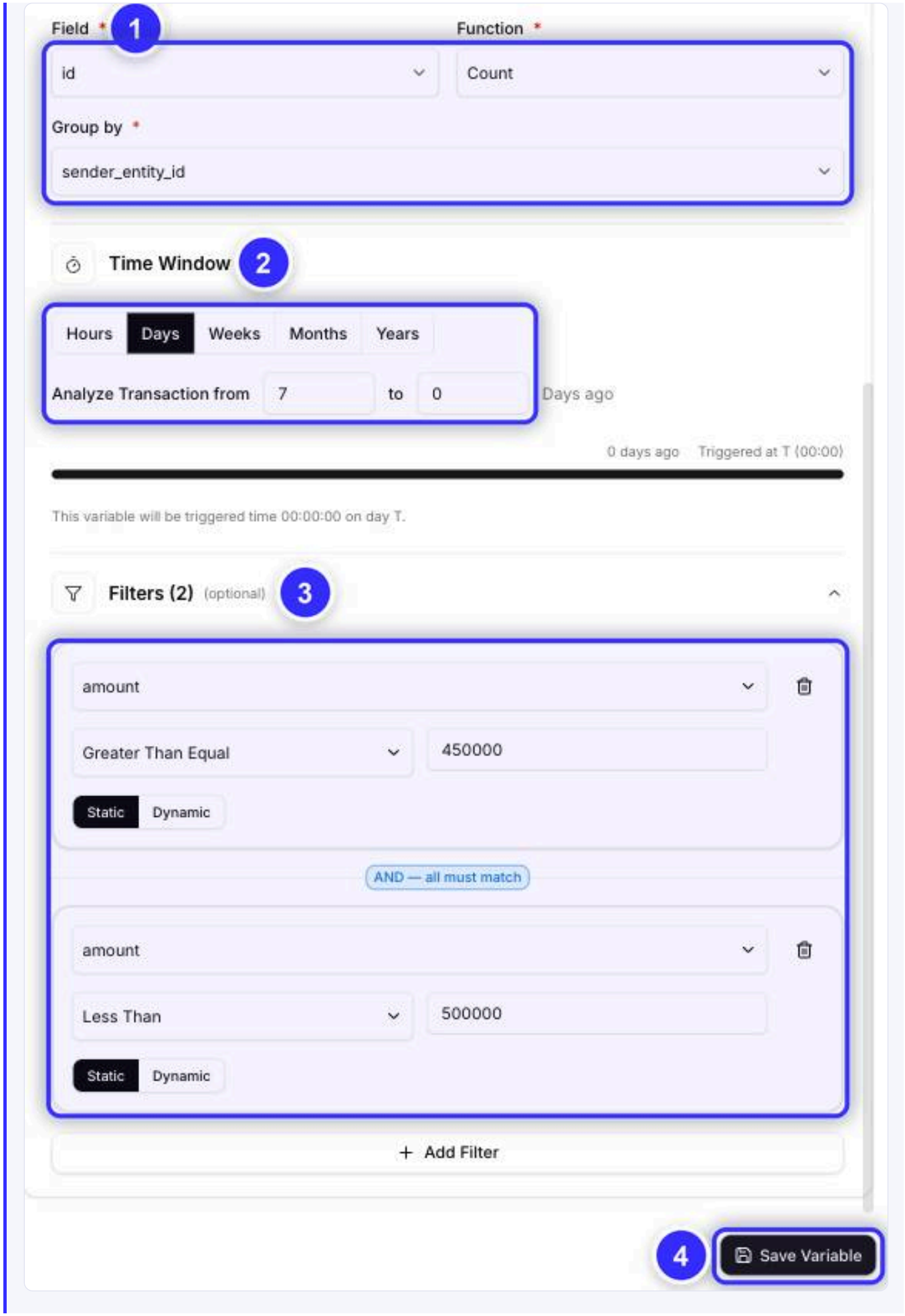

Field *
1
Function *
id
Count
Group by *
sender_entity_id
Time Window
2
Hours
Days
Weeks
Months
Years
Analyze Transaction from
7
to
0
Days ago
0 days ago
Triggered at T (00:00)
This variable will be triggered time 00:00:00 on day T.
Filters (2)
(optional)
3
amount
Greater Than Equal
450000
Static
Dynamic
AND — all must match
amount
Less Than
500000
Static
Dynamic
+ Add Filter
4
Save Variable

Figure 9.11 The completed variable form before saving

Step 12 **Find the variable in the list**

The dialog closes and the variable is the first row of the **Variables** list, with its ID (VAR-08102026-000769 in the example) and the **Created** time.

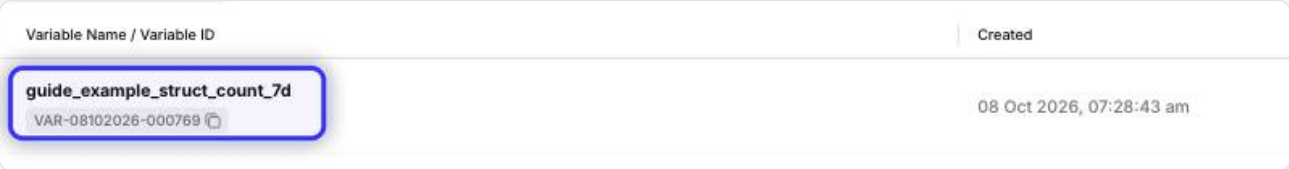


Figure 9.12 The new variable at the top of the Variables list

Step 13 **Check the saved variable**

Click the row. **View Variable** opens with the type tag **STR_AGG_COUNT** (1), the **CREATED** and **UPDATED** times and user (2), and **Edit**, **Delete** and **Duplicate** (3). The fields are read-only.

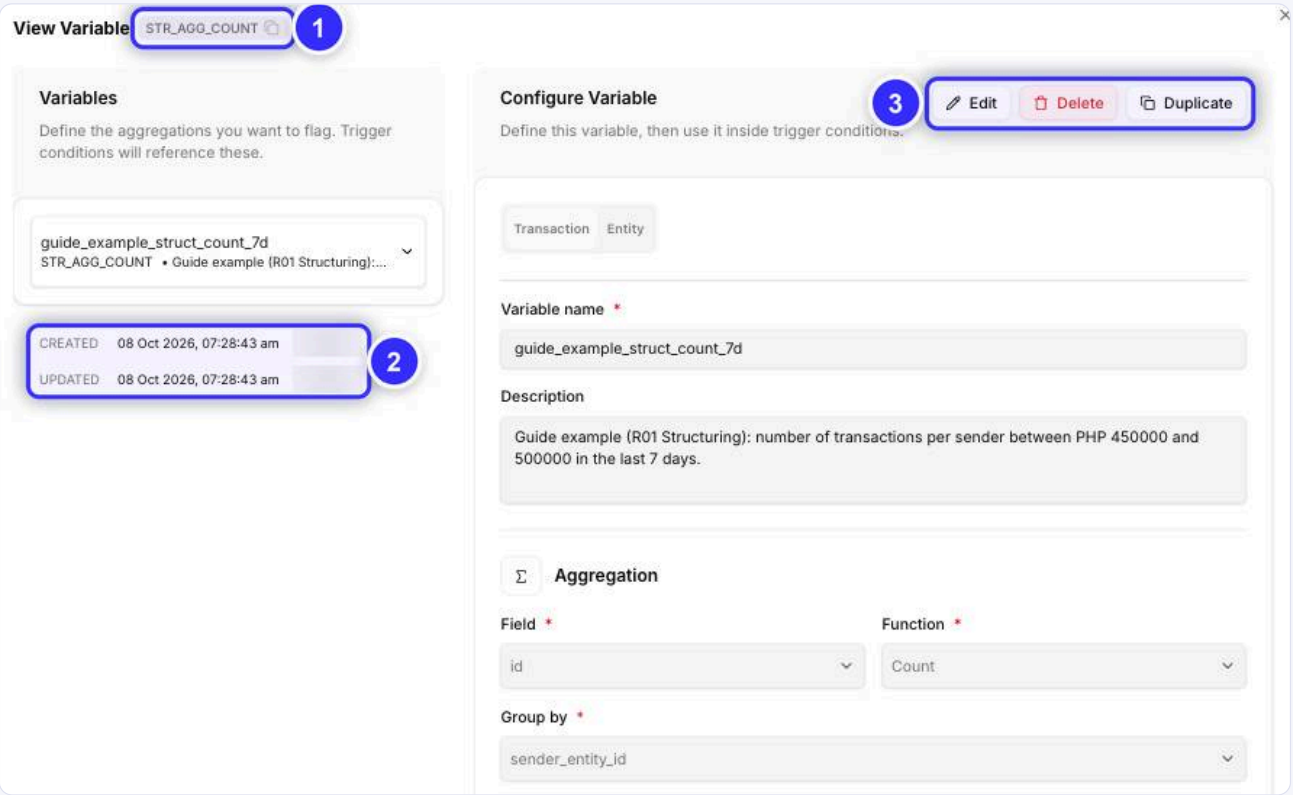


Figure 9.13 View Variable: type tag, created and updated, Edit, Delete and Duplicate

Step 14 **Check that both filters were saved**

Scroll down. **Filters (2)** (1) shows both rows joined by **AND — all must match**. **Update Variable** (2) is greyed out until you click **Edit**. Close the dialog with ×.

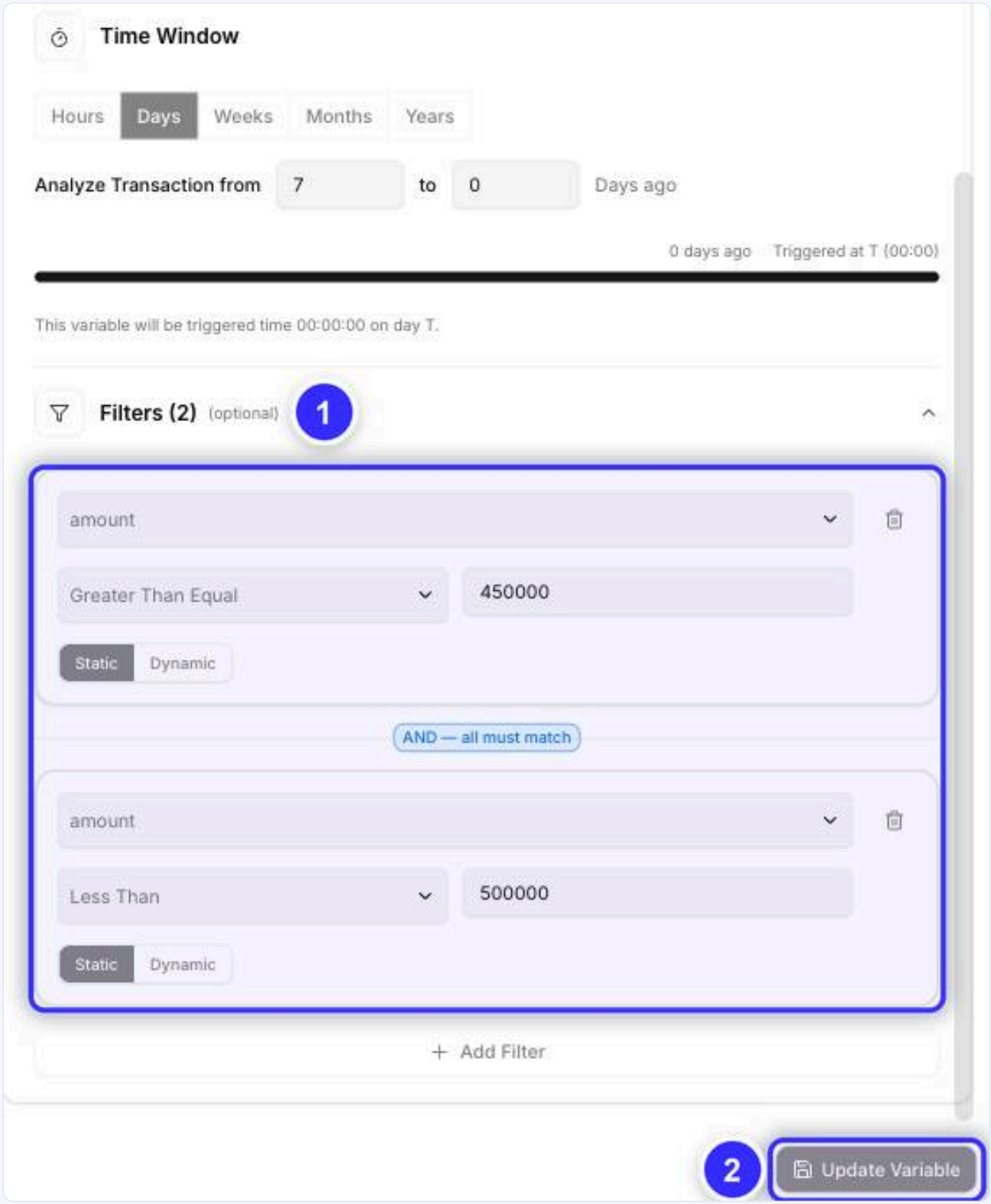


Figure 9.14 View Variable: both filters saved

Part B: Create the typology

Fyscal ARCX → Transaction Monitoring → Typology → + New

Step 15 **Name the rule and set the suppression window**

Go to **Transaction Monitoring → Typology** and click **+ New**. In **Typology Name** (1) type `R01 Structuring - 3 or more transactions between PHP 450000 and 500000 in 7 days`; names allow only letters, digits, spaces, hyphens, underscores and parentheses, so the amount is written as PHP. In **Suppression Window** type 7 (2), open the unit list (**Hour**, **Day**, **Week**, **Month**, **Year**) and choose **Day** (3). The example matches the 7-day variable window (see Building blocks).

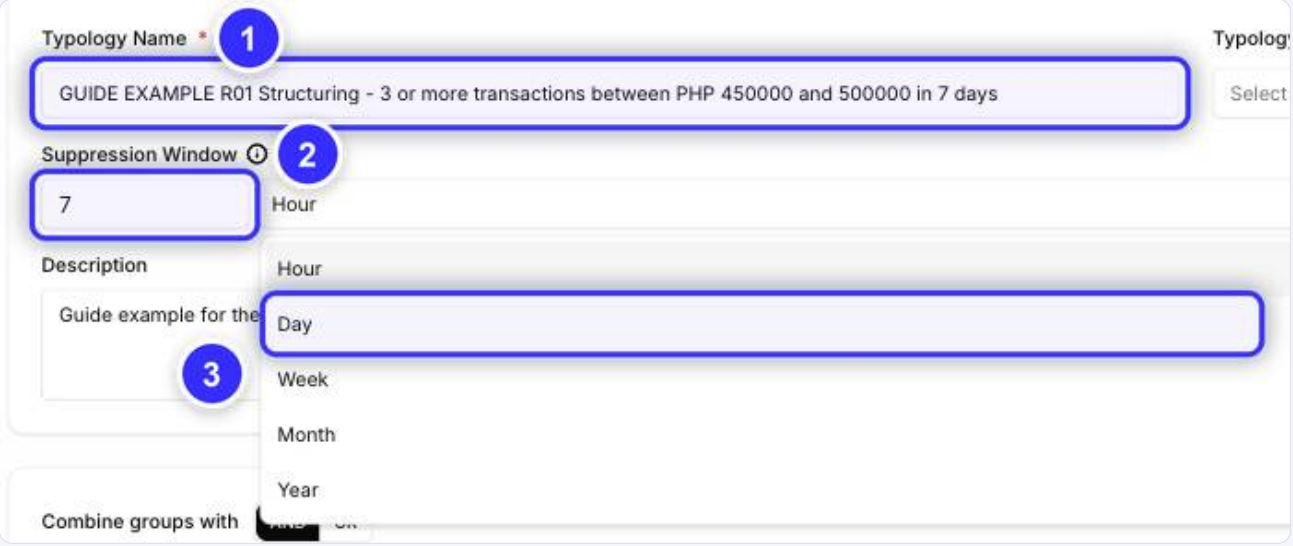


Figure 9.15 Typology Name, Suppression Window 7 and the unit list

Step 16 **Choose the typology type**

Open **Typology type** *(optional)* and type `Struct`. One type matches: **Structuring** TP100. Click it. Do not click **+ New**, which creates a new type.

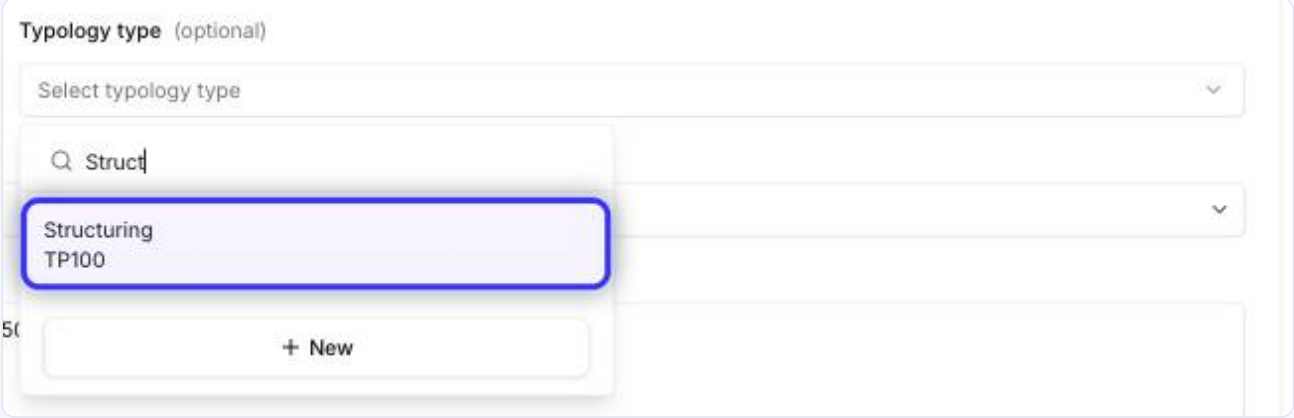


Figure 9.16 Typology type search: Structuring TP100

Step 17 **Write the description and check the card**

In **Description** state the rule in words, for example “Flags a sender with 3 or more transactions of PHP 450000 to under 500000 in 7 days.” The card now shows the name (1), the chip **Structuring (TP100)** (2), **7 Day** (3) and the description (4).

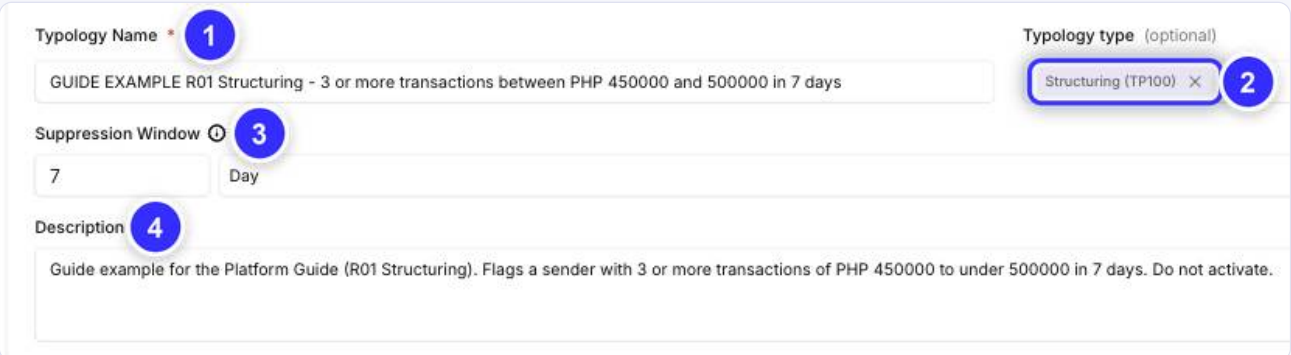


Figure 9.17 The completed details card

Step 18 **Choose the variable in row 1**

Below the card, leave **Combine groups with** and **Match** on **AND**. In **Group 1**, click **Select field** next to **WHEN**, type `struct` and click `struct_count_7d` under **VARIABLES**.

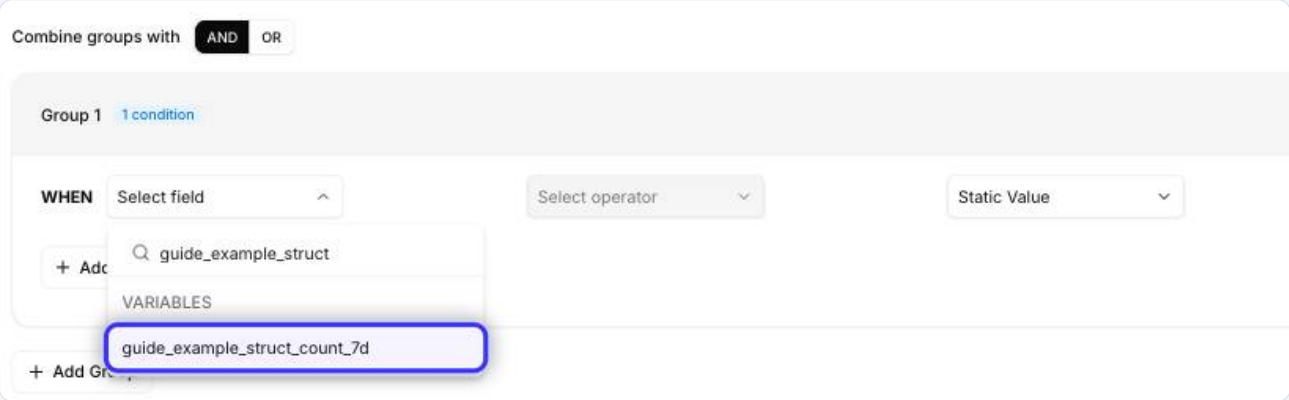


Figure 9.18 Row 1: the variable search

Step 19 **Choose the operator: Greater Than Equal**

Open **Select operator**. The list is **Equal**, **Not Equal**, **Greater Than**, **Greater Than Equal**, **Less Than**, **Less Than Equal**, then (scroll) **Between**, **Not Between**, **In**, **Not In**, **Is Null** and **Is Not Null**. Choose **Greater Than Equal**; the field shows **Greater Than Equal (>=)**.

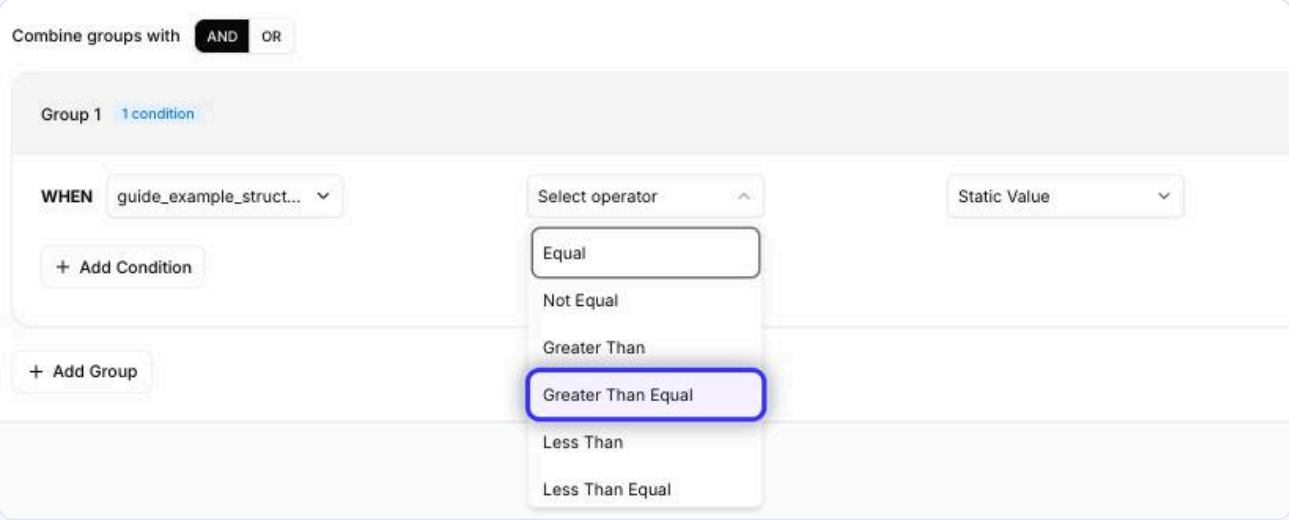


Figure 9.19 Row 1: the operator list

Step 20 **Keep Static Value**

The compare-to list offers **Static Value** (selected) and **Variable**; **Ingested Data** is greyed out. Keep **Static Value**: the threshold is a fixed number.



Figure 9.20 Row 1: compare with Static Value

Step 21 **Enter 3 and go to the next step**

Type 3 in **Enter value**. Check the page: name (1), type (2), **7 Day** (3), description (4), **Match** AND (5) and the row `struct_count_7d` **Greater Than Equal (>=)** **Static Value** 3 (6). **Next Step** (7) is now available. Click it.



Figure 9.21 The completed Create Typology page

Part C: Create the schedule and save

Step 22 **Read the Review & schedule rule page**

Review & schedule rule opens. **Select Schedule** (1) is empty. **Dry Run** (2) and **Save as Draft** (3) are greyed out. **Previous Step** (4) returns to the conditions.



Figure 9.22 Review & schedule rule before a schedule is chosen

Step 23 **Start a new schedule**

Open **Select Schedule**. The search finds only an older schedule from another walkthrough. This rule creates its own, so click **+ New**. A schedule can serve many rules, which is why the other rules reuse this one.

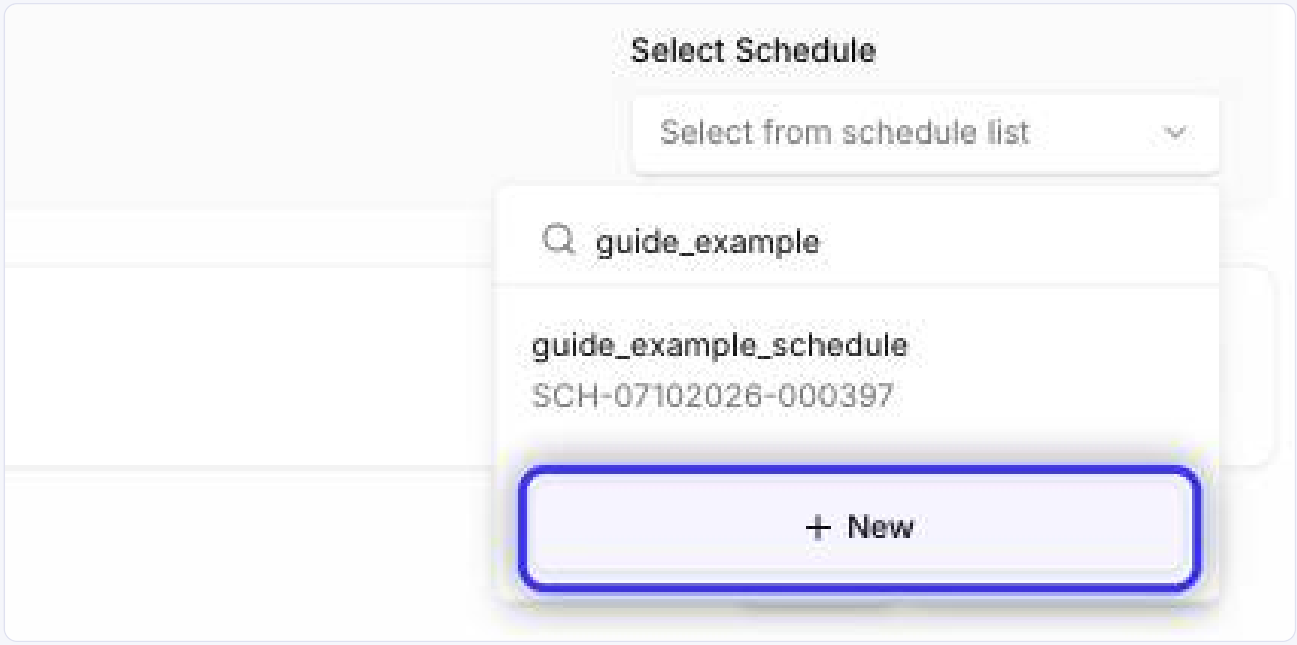


Figure 9.23 Select Schedule with + New

Step 24 **Read the empty schedule fields**

The card shows **Name** (1), **Execution Interval** (2) with a **Unit** list (3), **Start Time** (4), filled with the current date and time, and **End Time** *(optional)* (5). A **Save as Draft** button (6) appears inside the card, greyed out.

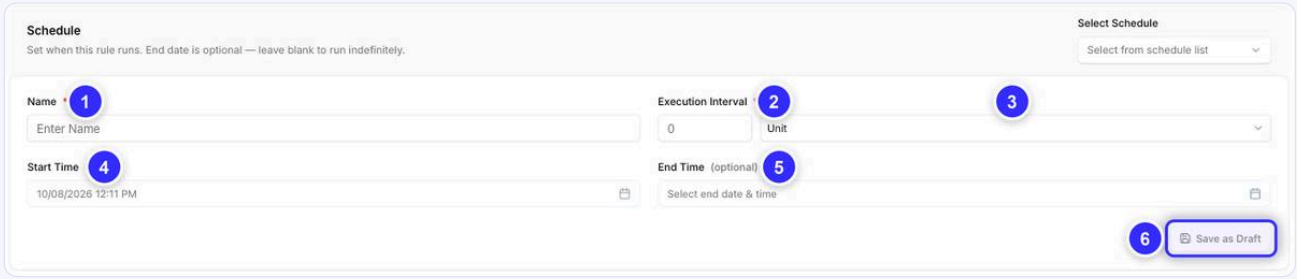


Figure 9.24 Empty fields for a new schedule

Step 25 **Name the schedule and set every 1 Day**

Type `schedule_2027` in **Name** and 1 in **Execution Interval** (1). Until you choose a unit, the message “Interval unit is mandatory” shows under the field. Open **Unit** and choose **Day** (2). The rule then runs once a day.



Figure 9.25 Execution Interval 1 and the Unit list

Step 26 **Open the start time picker**

Click **Start Time**. The calendar opens on the current month; dates before today are greyed out. Below it are **Time** and **Clear**.

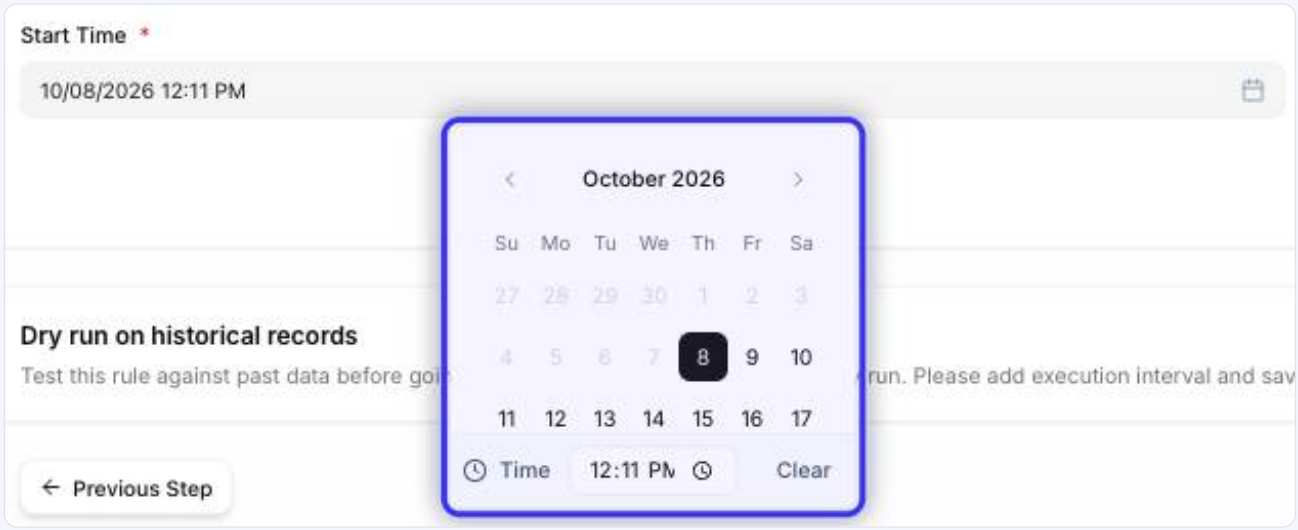


Figure 9.26 The Start Time calendar

Step 27 **Set 01 Jan 2027, 09:00 AM**

Click the next-month arrow until January 2027, click 1 (2) and type 09:00 AM in **Time** (3). The field reads 01/01/2027 09:00 AM (1). The start time must be in the future for **Save as Draft** to become available (see Before you build).

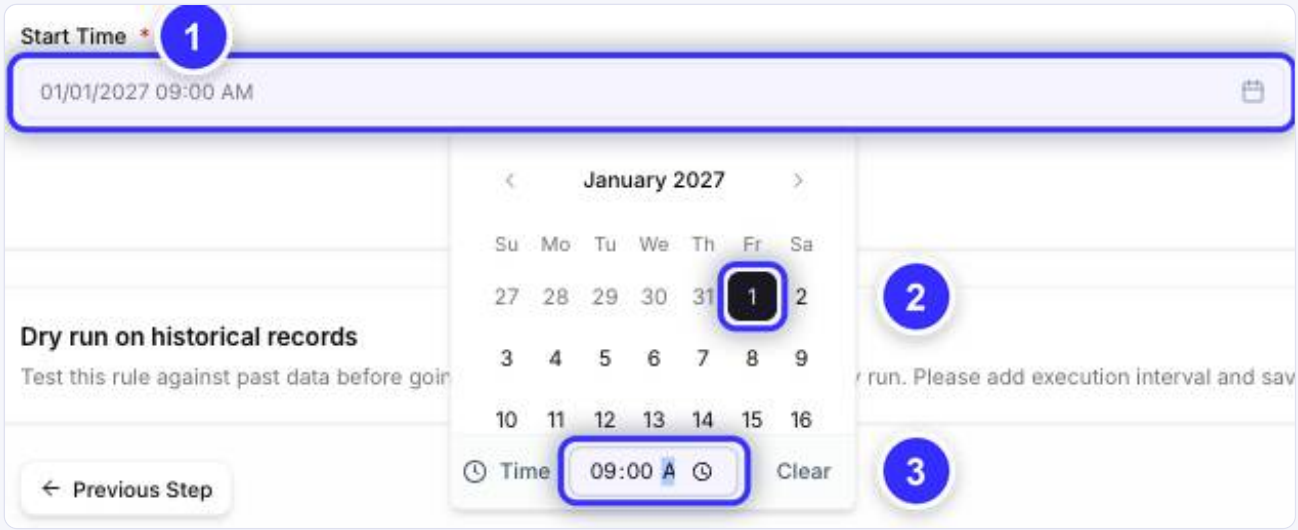


Figure 9.27 Start Time set to 01/01/2027 09:00 AM

Step 28 **Leave End Time blank and save the draft**

Leave **End Time** empty (1): “End date is optional — leave blank to run indefinitely.” Click **Save as Draft** in the card (2).

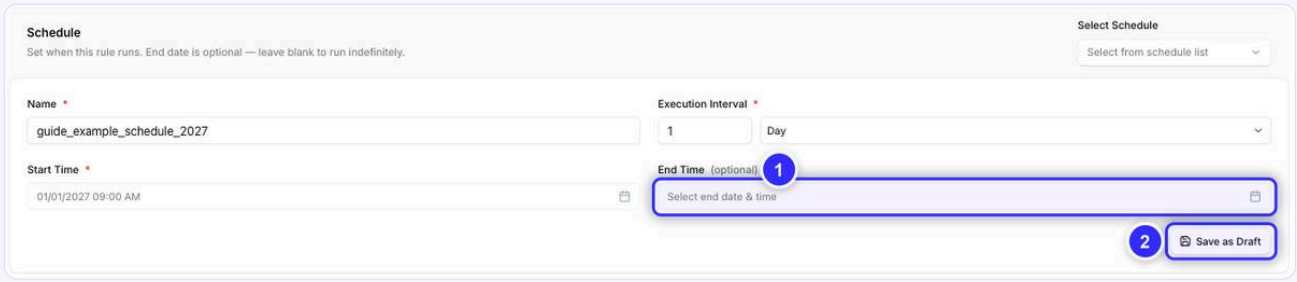


Figure 9.28 The completed schedule and Save as Draft

Step 29 **Check the saved draft**

Wait a few seconds: the title changes to **Update Typology** (1). **Select Schedule** shows `schedule_2027` (2) and the card reads “This rule will run every 1 day starting 01 Jan 2027, 09:00:00 am” (3). **Save as Draft** is replaced by **Update** (4); **Dry Run** (5) and **Activate** (6) are now available. To test and activate, see Test a typology with Dry Run and Request Shadow activation.

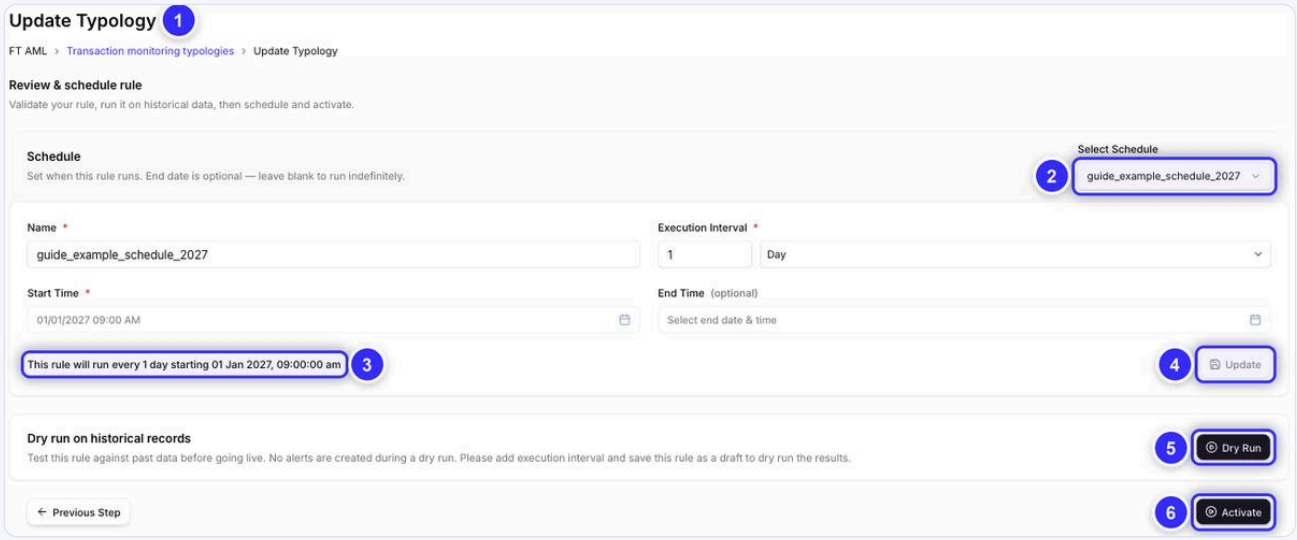


Figure 9.29 After Save as Draft: the Update Typology page

Step 30 **Check the rule page**

Open the rule from **Transaction Monitoring → Typology**. It shows **Draft** and the rule ID, here TMR-08102026-001123 (1); the summary **EXECUTION PERIOD** 01 Jan 2027, 09:00:00 am → N/A, **INTERVAL** Every 1 day, **SUPPRESSION** 7Day and **TYPOLOGY** Structuring (2); the condition (3); and the variable card, **Str_agg_count**, **WINDOW** in last 7 day, **GROUP** `sender_entity_id` (4).

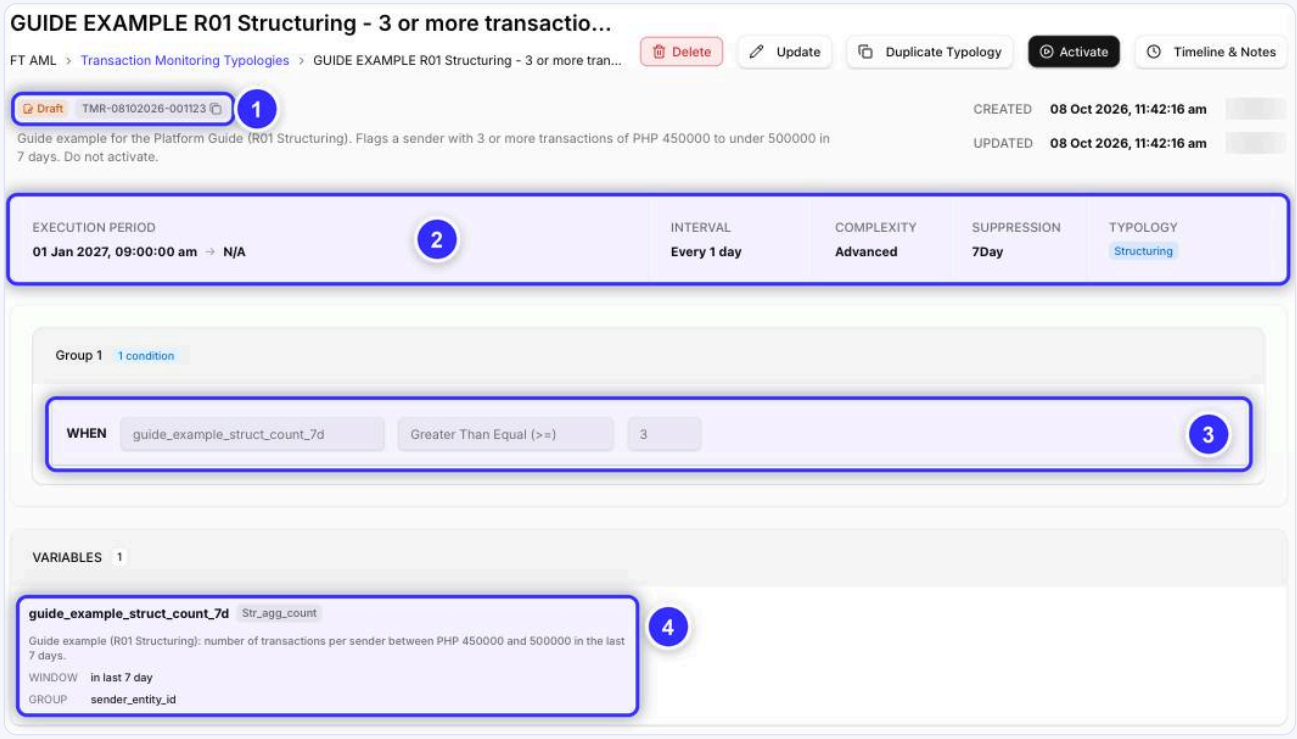


Figure 9.30 The saved Rule 1 as a Draft

Step 31 **Move the schedule's start (later change)**

The example schedule was later moved to start on 09 Oct 2026, so the rules could be activated sooner. On any rule that uses it, open **Review & schedule rule**, click **Start Time**, pick the date and keep 09:00 AM: the field reads 10/09/2026 09:00 AM (1) and the card "This rule will run every 1 day starting 09 Oct 2026, 09:00:00 am" (2). Click **Update** (3) and confirm the dialog (see Test a typology with Dry Run, step 5). The change is on the shared schedule: Rule 1's page showed the new start after a reload.

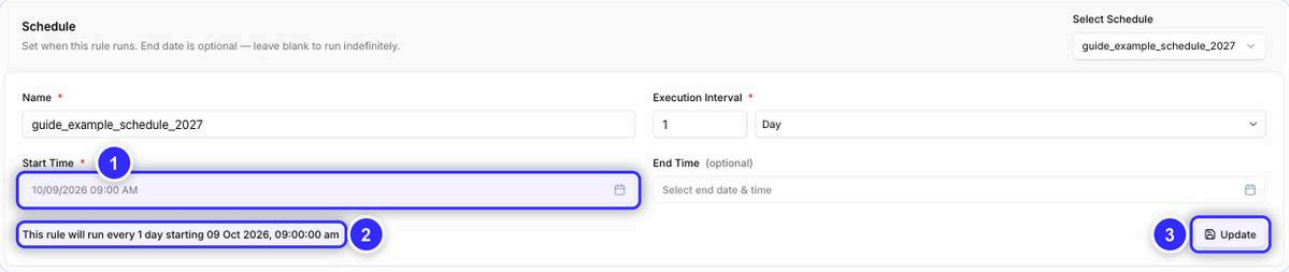


Figure 9.31 Start Time moved to 10/09/2026 09:00 AM; Update

How it evaluates. At each daily run the variable counts, for each sender, the transactions in the last 7 days whose amount is at least ₱450,000 and below ₱500,000. Sender A sent ₱480,000, ₱495,000 and ₱460,000 during those 7 days: the count is 3, 3 >= 3 is true, and the rule raises an alert. Sender B sent ₱480,000, ₱490,000 and ₱500,000: the ₱500,000 payment fails **Less Than** 500000, so the count is 2 and there is no alert. Sender C sent ₱300,000 four times: none is in the band, the count is 0, no alert.

Tuning. The numbers you can change are: the band (the two filter values, 450000 and 500000), set from the amount you want reviewed; the count threshold (3) in the condition; the window (**Analyze Transaction from** 7); and the **Suppression Window** (7 Day). A wider band, a lower count or a longer window raises more alerts. The example sets the **Suppression Window** to the same length as the variable window (see Building blocks). Run a **Dry Run** after each change to see the alert volume.

Dry-run result. In testing, the rule created 0 alerts at 3 or more transactions: few transactions fall in the ₱450,000 to ₱499,999 band. With the threshold temporarily at 1 it created 4 alerts, so the variable and its two filters work. The full dry run, control and restore for this rule are shown in Test a typology with Dry Run.

Rule 2 · Velocity

RED FLAG **A burst of transactions in a day**

LOGIC

Counts the sender's transactions in the last day.

WINDOW

1 to 0 Days

THRESHOLD

≥ 10

✓ Verified by positive control

What it detects and why. This rule flags a sender who makes 10 or more transactions in one day. A sudden burst of activity can mean an account is being used to move money quickly, so a count well above what your customers normally do is worth reviewing.

The screens are the same as in Rule 1; this section shows each step with this rule's values.

Item	Setting
Variable `txn_count_1d`	**Count** of `id` (the number of transactions), grouped by `sender_entity_id`, **Days** from 1 to 0, no filters
Typology type	Velocity (V-01)
Suppression Window	1 Day
Condition	Group 1, Match AND: `txn_count_1d` **Greater Than Equal (>=)** Static Value 10
Schedule	Existing `schedule_2027` (created in Rule 1): every 1 Day, starting 09 Oct 2026, 09:00 AM, no end time

Part A: Create the variable

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 1 **Open the form and name the variable**

Click **+ New** on **Variables**. Leave **Transaction** selected, type `txn_count_1d` in **Variable name** (1) and a description such as “Number of transactions per sender in the last 1 day.” (2).

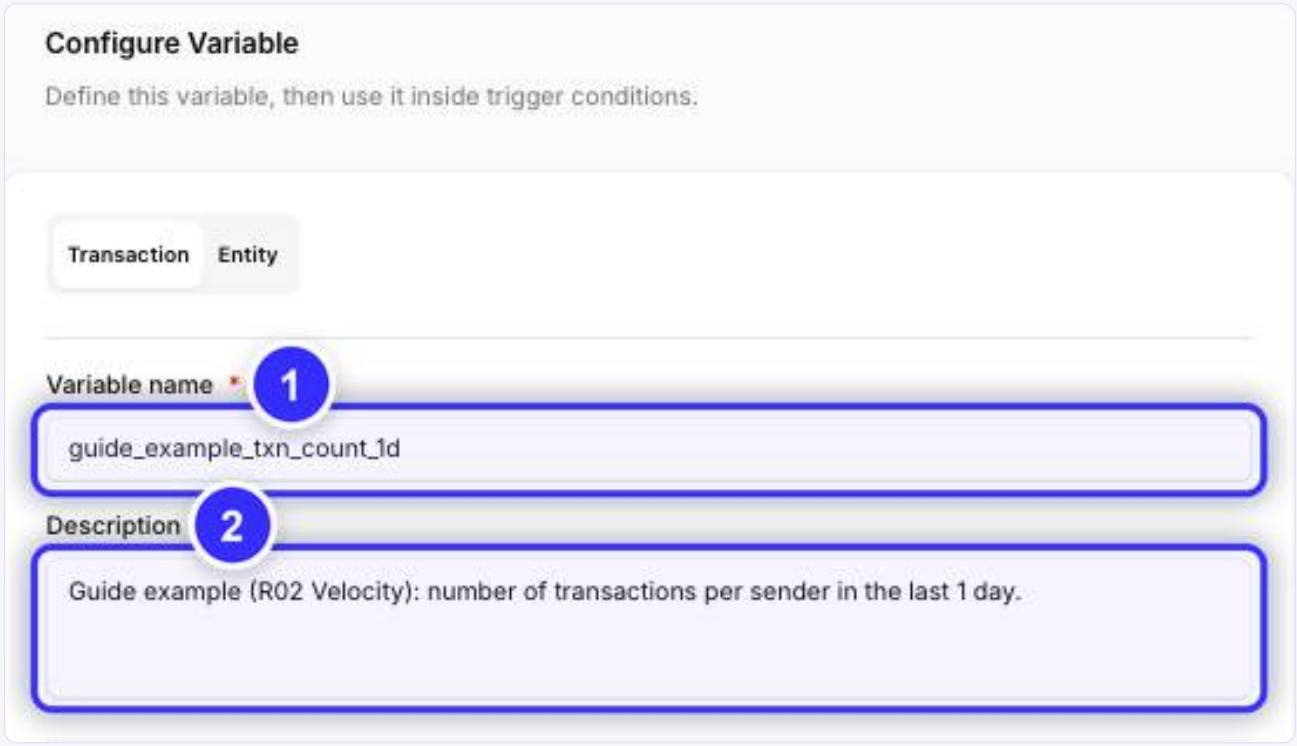


Figure 9.32 Rule 2 variable: name and description

Step 2 **Choose the Field: id**

Open **Field**, type `id` in **Search Fields** and choose `id`, the first match. Counting `id` counts transactions.

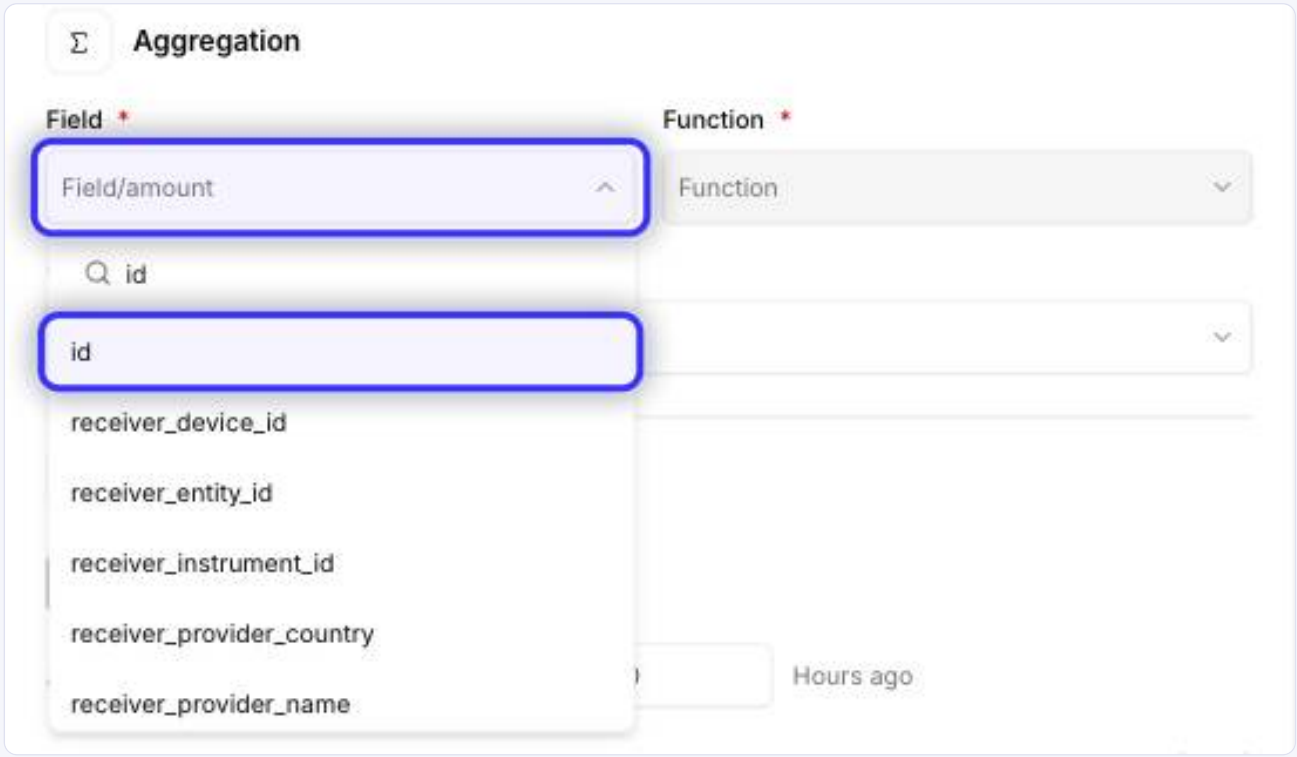


Figure 9.33 Field search for id

Step 3 **Choose the Function: Count**

Open **Function** (**Count**, **Count Distinct**, **Minimum**, **Maximum**) and choose **Count**.

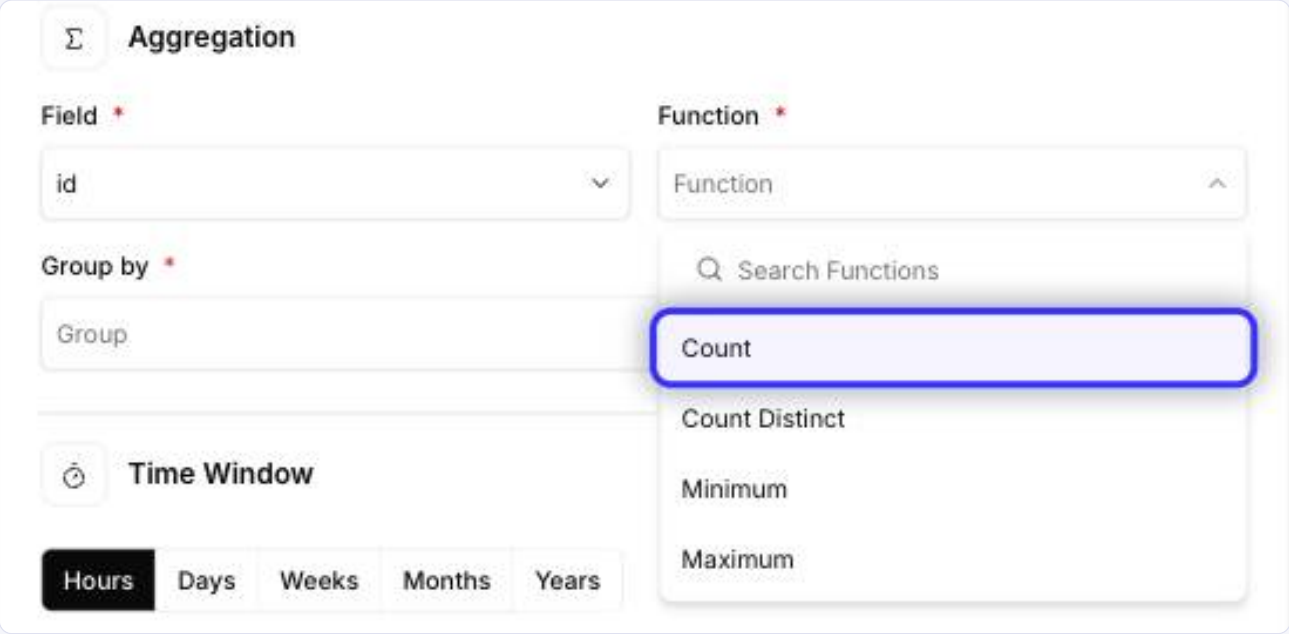


Figure 9.34 Function: Count

Step 4 **Choose Group by: sender_entity_id**

Open **Group by**, type `sender_entity` and choose `sender_entity_id`, so each sender gets their own count.



Figure 9.35 Group by search: sender_entity_id

Step 5 **Set the time window: Days, 1 to 0**

Click **Days** (1) and set **Analyze Transaction from** 1 **to** 0 (2): the last day up to the trigger time T.



Figure 9.36 Time window 1 to 0 Days ago

Step 6 **Leave the filter row empty and save**

Leave the blank row under **Filters (1)** (1) empty: every transaction counts. A blank row is dropped when you save. Click **Save Variable** (2).

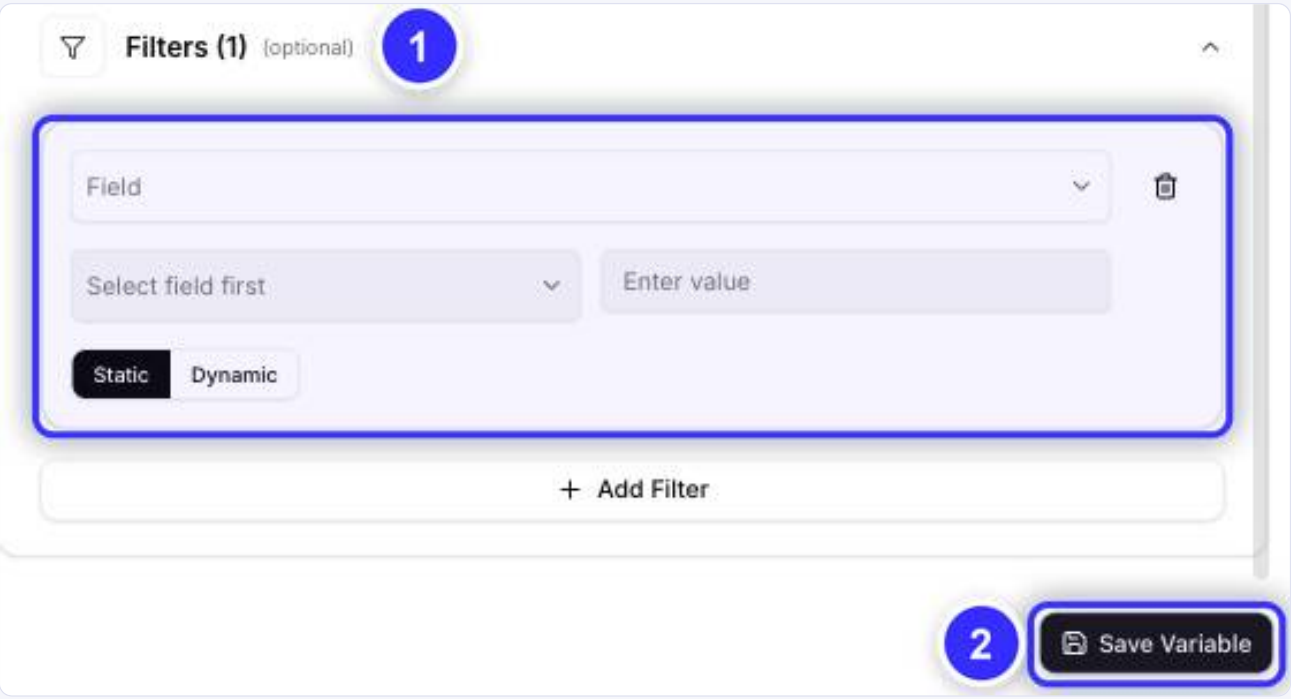


Figure 9.37 Blank filter row and Save Variable

Step 7 **Find the variable in the list**

The new variable is the first row, here VAR-08102026-000770.

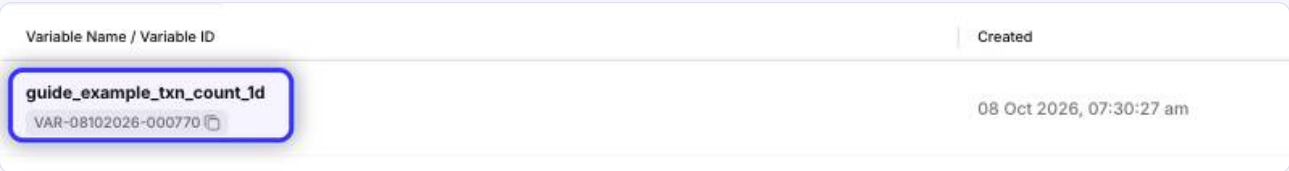


Figure 9.38 Rule 2 variable in the Variables list

Step 8 **Check the saved variable**

Click the row. **View Variable** shows **STR_AGG_COUNT** (1), the created and updated details (2), the window 1 to 0 **Days ago** (3) and **Filters (0)** (4), confirming that the blank row was not saved.

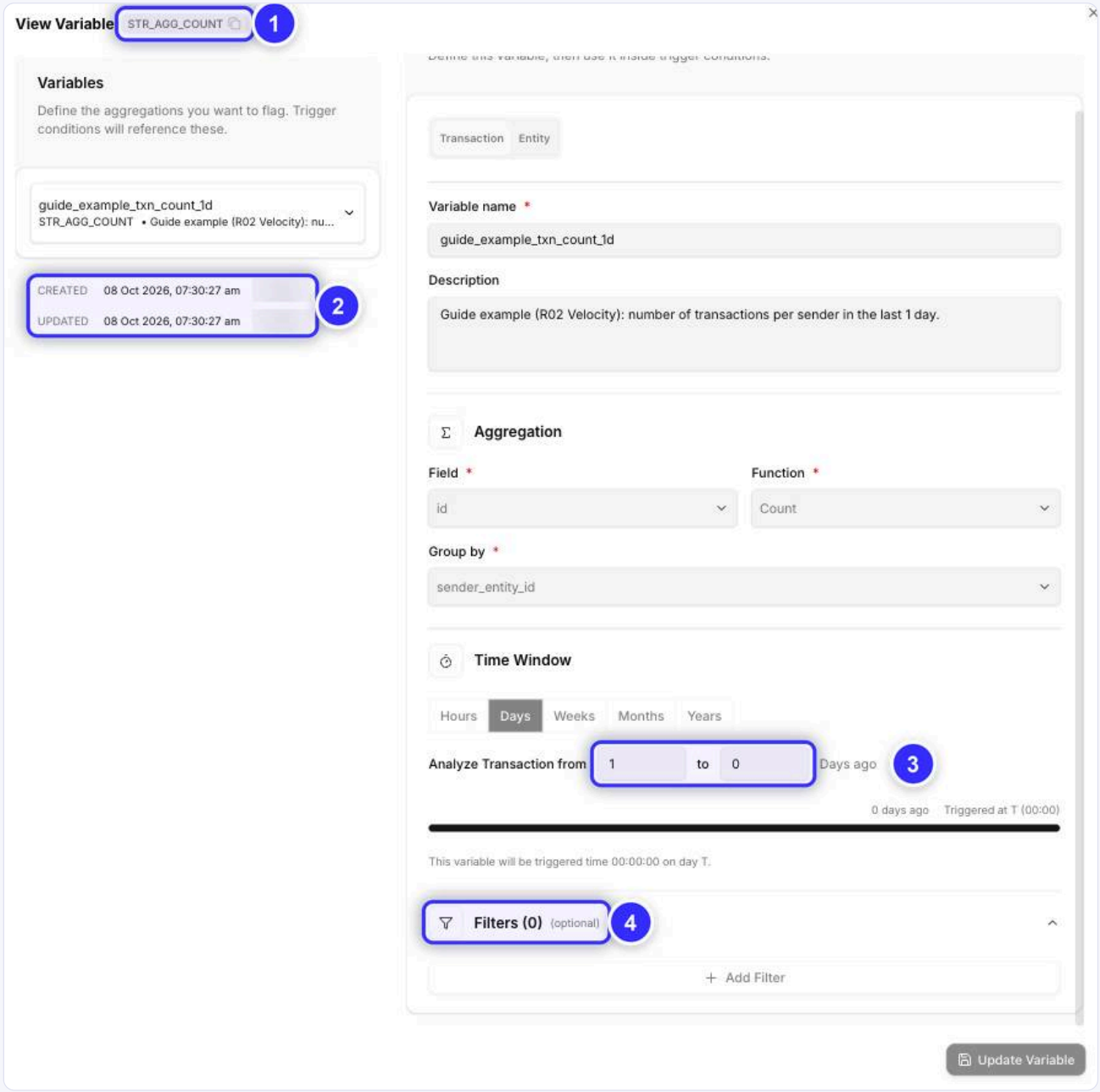


Figure 9.39 View Variable for the Rule 2 variable

Part B: Create the typology

Fyscal ARCX → Transaction Monitoring → Typology → + New

Step 9 **Fill in the details and choose Velocity**

Click **+ New** on **Typology**. Type the name `R02 Velocity - 10 or more transactions in 1 day` (1). Set **Suppression Window** to 1 and choose **Day** from the unit list (2), matching the 1-day window. Write a description (3). Open **Typology type** (4), type `Velo` and click **Velocity** V-01.

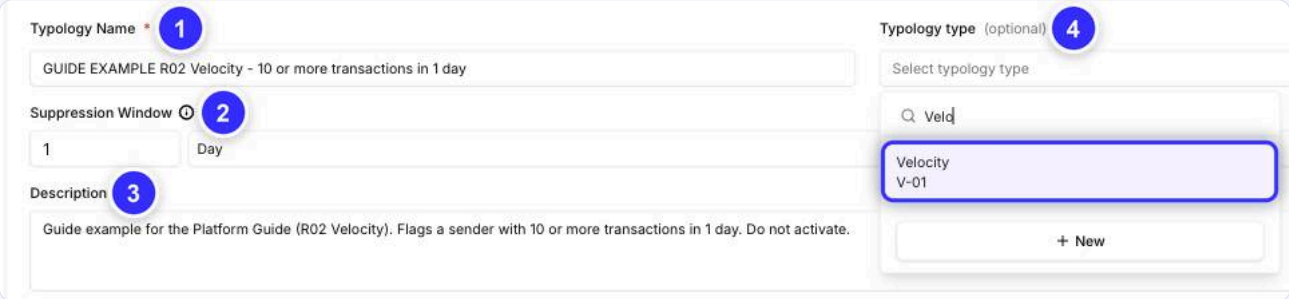


Figure 9.40 Rule 2 details and the Typology type search for Velocity

Step 10 **Choose the variable in row 1**

In **Group 1**, click **Select field**, type `txn` and click `txn_count_1d` .

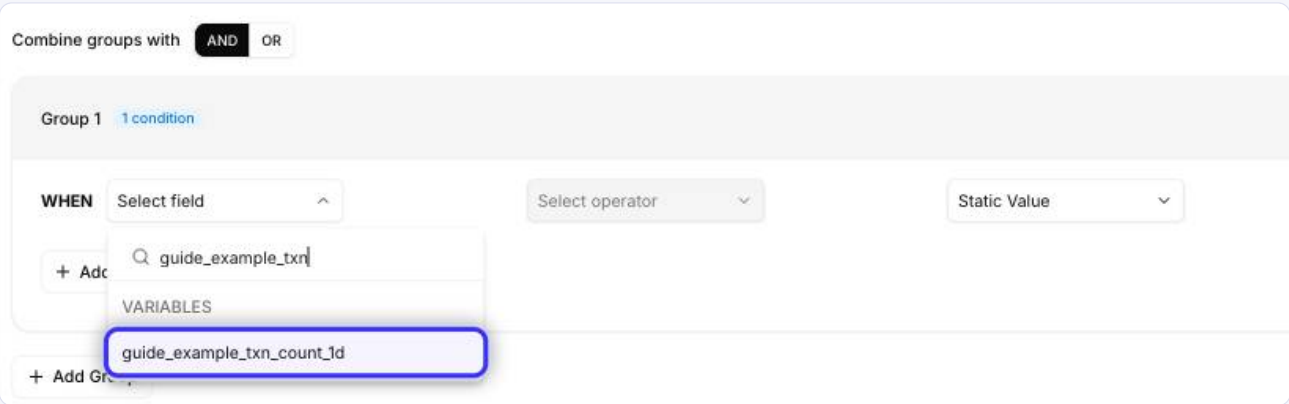


Figure 9.41 Rule 2 row 1: variable search

Step 11 **Choose Greater Than Equal**

Open **Select operator** and choose **Greater Than Equal**.

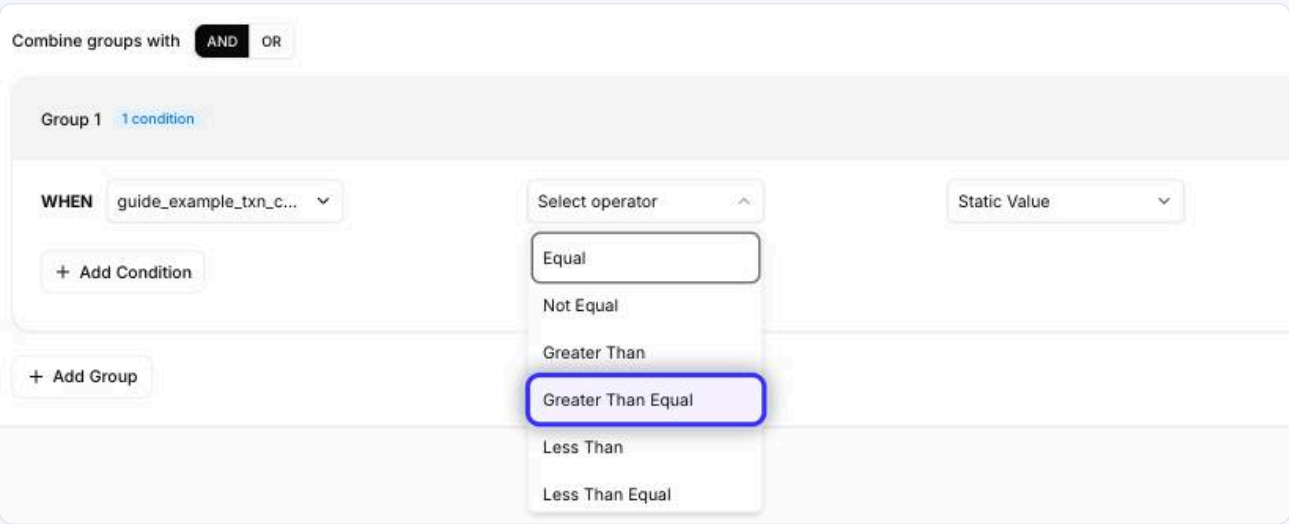


Figure 9.42 Rule 2 row 1: operator list

Step 12 **Keep Static Value**

Keep **Static Value** in the compare-to list.



Figure 9.43 Rule 2 row 1: Static Value

Step 13 **Enter 10 and go to the next step**

Type 10 in **Enter value**. The page shows the name (1), **Velocity (V-01)** (2), **1 Day** (3), the description (4), **Match** AND (5) and the row (6). Click **Next Step** (7).

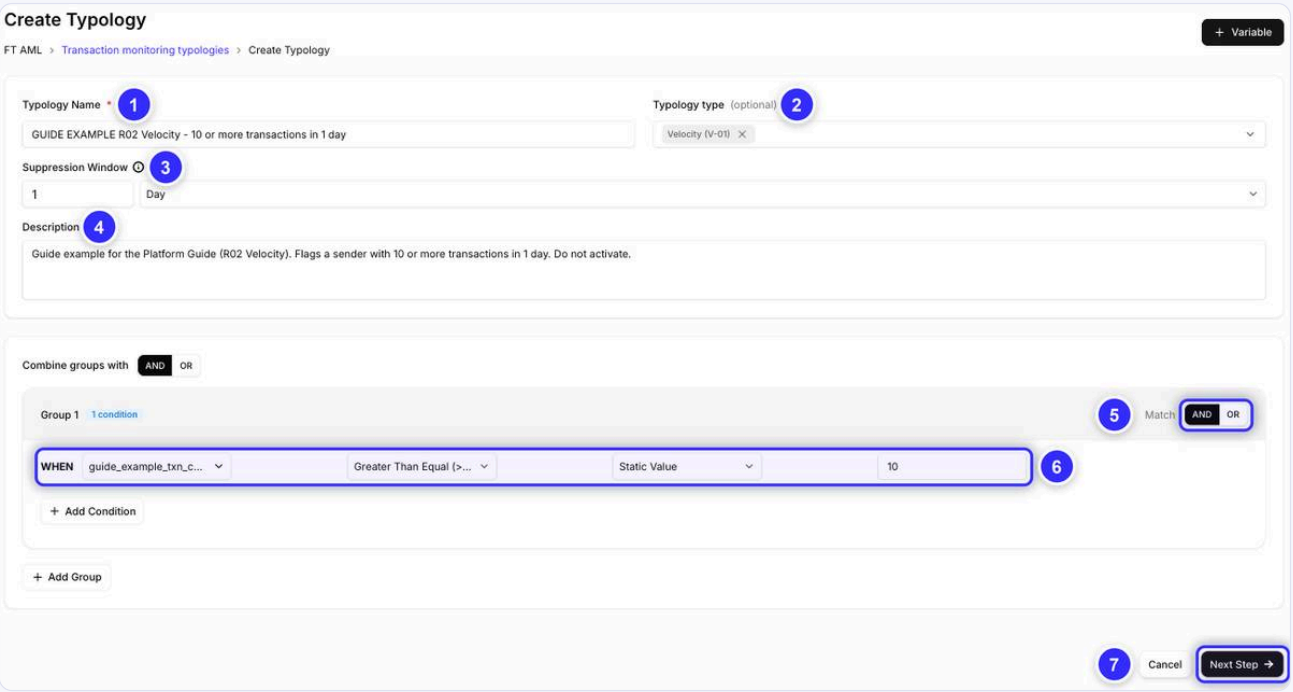


Figure 9.44 The completed Rule 2 page

Part C: Choose the schedule and save

Step 14 **Select the existing schedule**

On **Review & schedule rule**, open **Select Schedule**, type `schedule_2027` and click `schedule_2027` (SCH-08102026-000463), created in Rule 1. Do not click **+ New**.

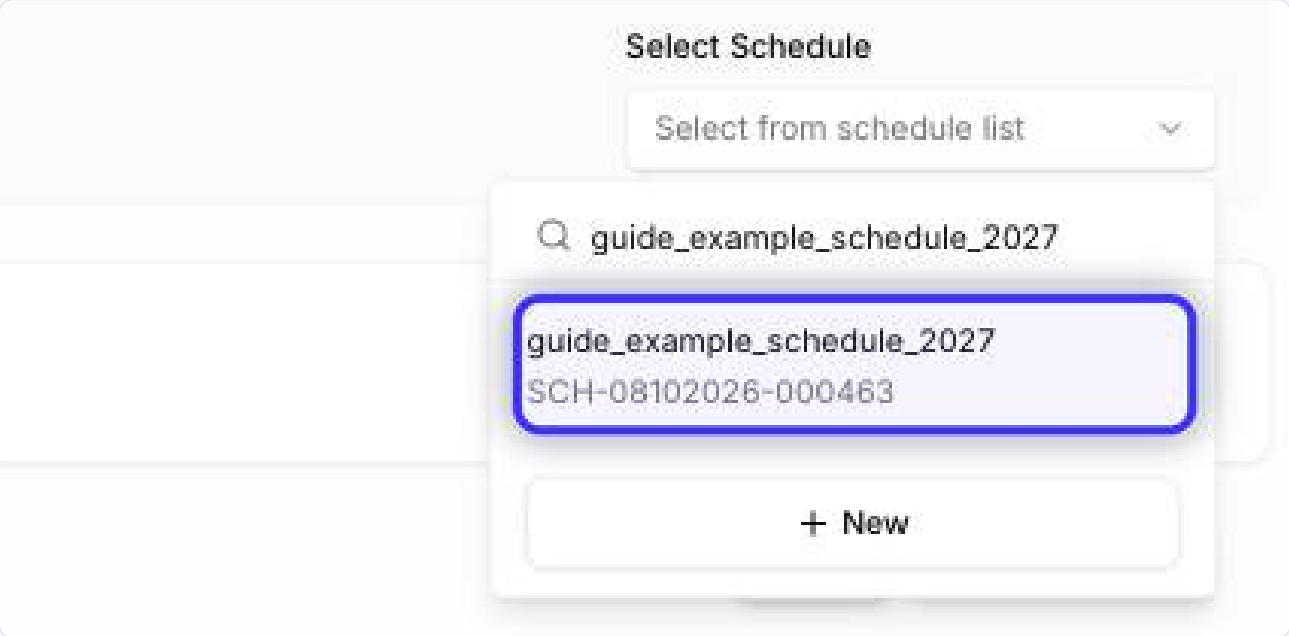


Figure 9.45 Select Schedule: the schedule from Rule 1

Step 15 **Check the schedule and save the draft**

The schedule's fields fill in (2): 1 **Day**, start 01/01/2027 09:00 AM, no end time. They belong to the shared schedule, so leave them unchanged; editing them would affect every rule that uses it. The screenshots show the start in force when they were taken. Click **Save as Draft** (3).

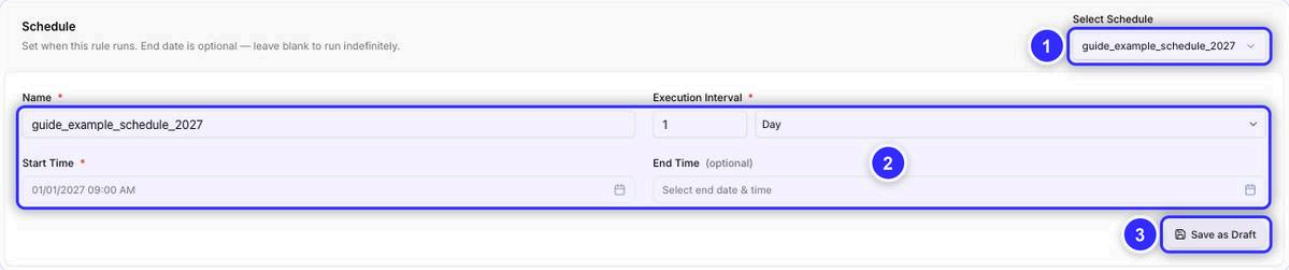


Figure 9.46 The selected schedule and Save as Draft

Step 16 **Check the saved draft**

Wait a few seconds: the page becomes **Update Typology** (1), with the schedule (2), the run sentence (3), **Update** (4), **Dry Run** (5) and **Activate** (6).

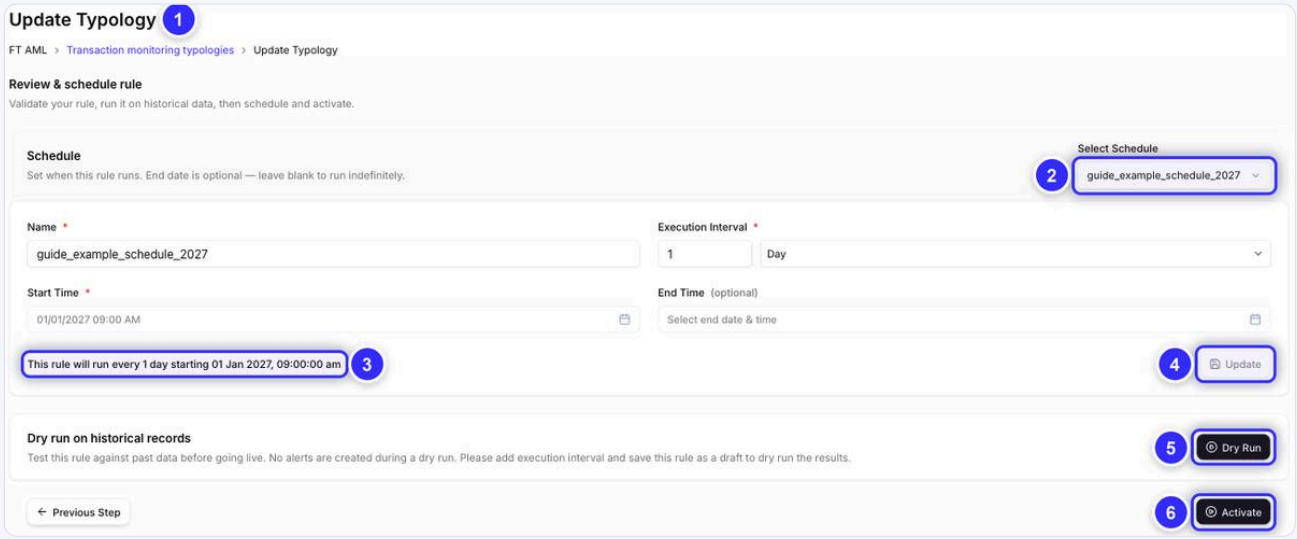


Figure 9.47 Rule 2 after Save as Draft

Step 17 **Check the rule page**

The rule page shows **Draft** TMR-08102026-001124 (1), **SUPPRESSION** 1Day and **TYPOLOGY** Velocity (2), the condition `txn_count_1d` **Greater Than Equal (>=)** 10 (3) and the variable card with **WINDOW** in last 1 day (4).

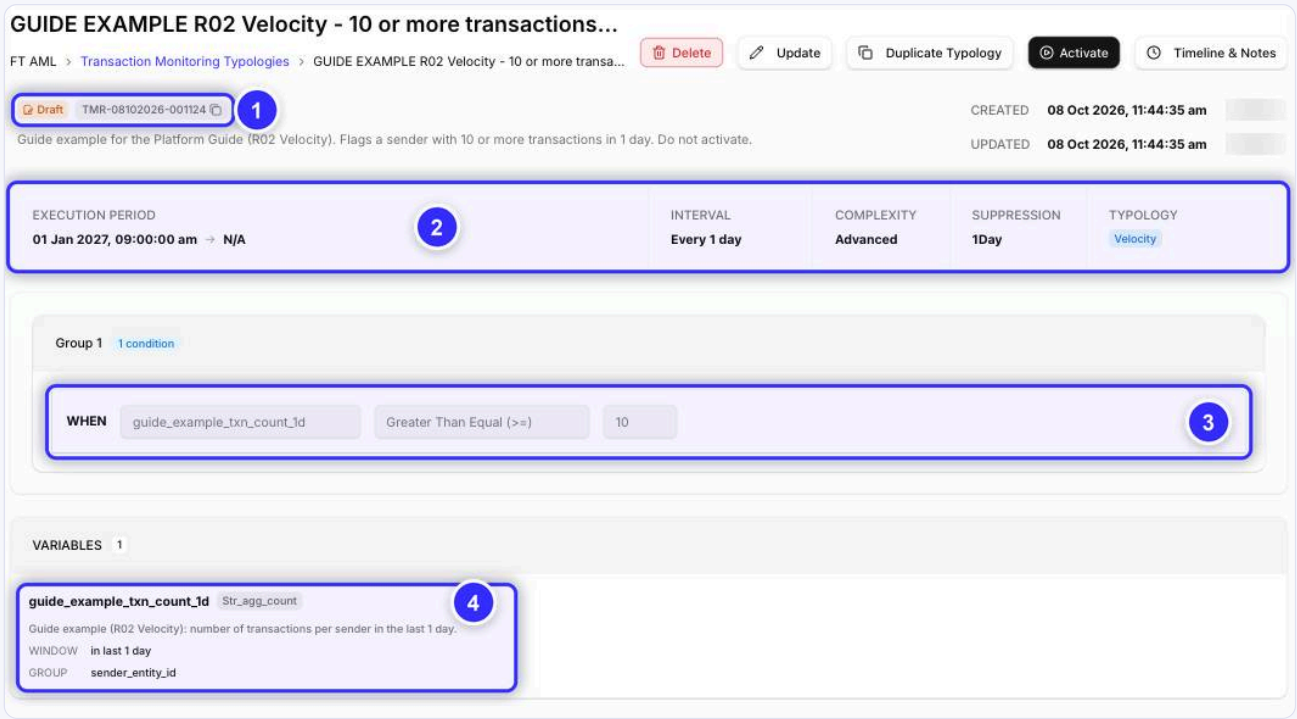


Figure 9.48 The saved Rule 2 as a Draft

How it evaluates. At each daily run the variable counts each sender's transactions in the last day, whatever their amount. Sender A made 12 transfers of about ₱1,000 each: 12 >= 10, so the rule raises an alert. Sender B made 9 transfers totalling ₱900,000: 9 is below 10, so there is no alert from this rule (Rule 3 looks at value instead).

Dry-run result. In testing, the rule created 0 alerts at 10 or more transactions in a day. With the threshold temporarily at 1 it created 764 alerts (0 / 0 / 500 / 264 by window, newest first): the 1-day window only finds transactions in the days that contain records. The threshold was then restored to 10.

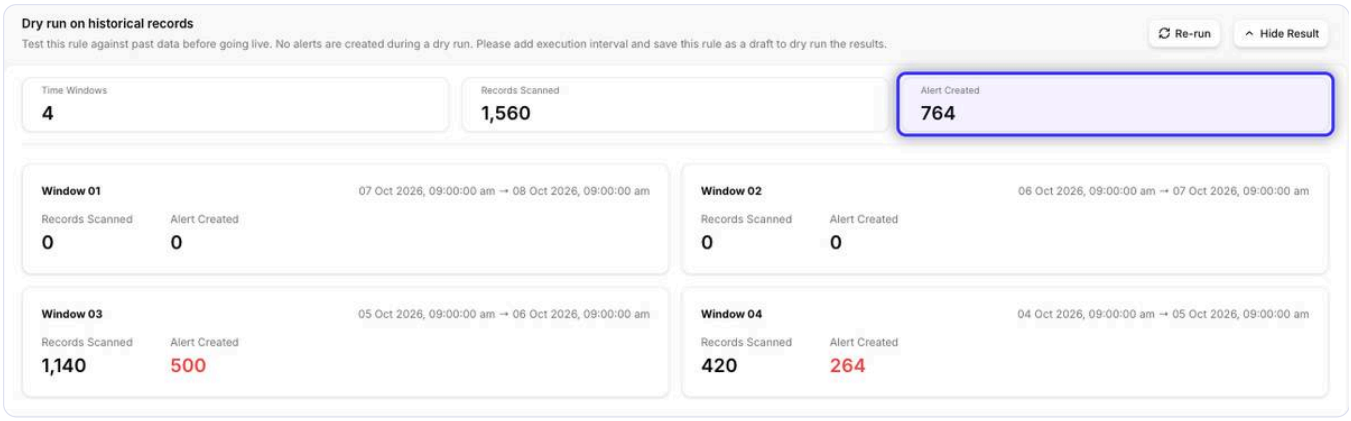


Figure 9.49 Rule 2 positive control (threshold temporarily >= 1): 764 alerts

Tuning. You can change the count threshold (10), the window (**Analyze Transaction from** 1, or a different unit such as **Hours** for a shorter burst) and the **Suppression Window** (1 Day). To count only one kind of transaction, add a filter row to the variable, as in Rule 1. Set the threshold from what your customers normally do, and check the volume with a **Dry Run**.

Rule 3 · High value

RED FLAG **A large total sent in 30 days**

LOGIC

Adds up the amount the sender sent in the last 30 days.

WINDOW

30 to 0 Days

THRESHOLD

≥ ₱5,000,000

✓ Verified by positive control

What it detects and why. This rule flags a sender whose payments add up to ₱5,000,000 or more within 30 days. Looking at the 30-day total, rather than single payments, catches a large amount moved in several pieces as well as in one.

The screens are the same as in Rule 1. The difference is the variable: it sums `amount` instead of counting transactions.

Item	Setting
Variable `sent_sum_30d`	**Sum** of `amount`, grouped by `sender_entity_id`, **Days** from 30 to 0, no filters
Typology type	High Value (HV01)
Suppression Window	30 Day
Condition	Group 1, Match AND: `sent_sum_30d` **Greater Than Equal (>=)** Static Value 5000000
Schedule	Existing `schedule_2027` (created in Rule 1): every 1 Day, starting 09 Oct 2026, 09:00 AM, no end time

Part A: Create the variable

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 1 **Open the form and name the variable**

Click **+ New** on **Variables**. Type `sent_sum_30d` in **Variable name** (1) and a description such as “Total amount sent per sender in the last 30 days.” (2).

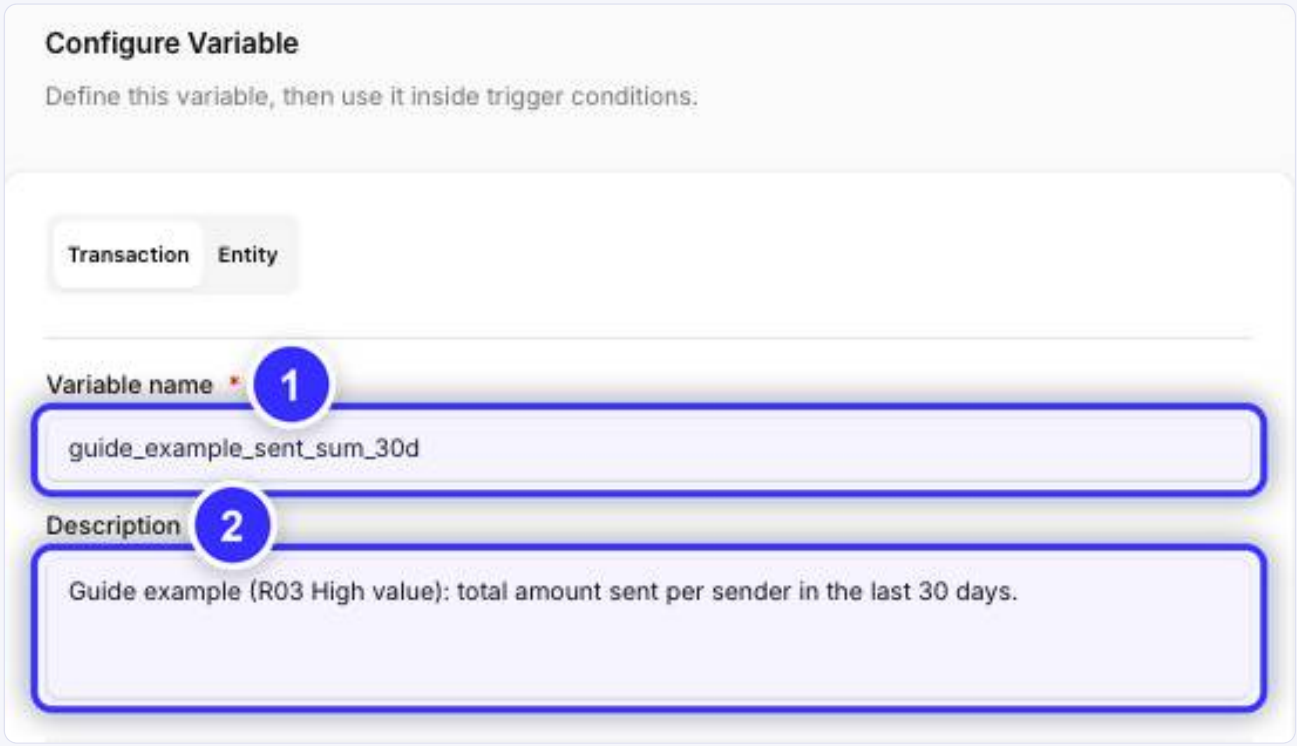


Figure 9.50 Rule 3 variable: name and description

Step 2 **Choose the Field: amount**

Open **Field** and choose `amount`, the transaction amount.

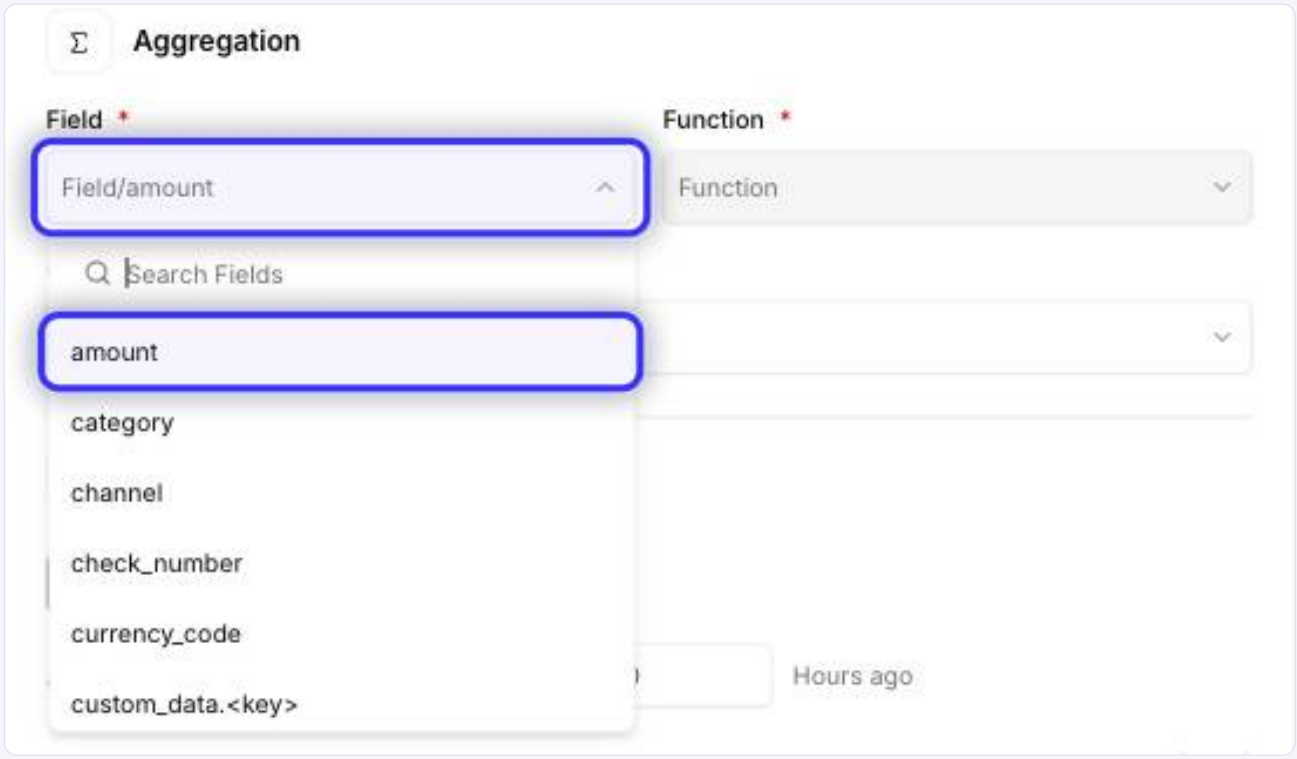


Figure 9.51 Field: amount

Step 3 **Choose the Function: Sum**

Open **Function**. Because `amount` is numeric, all six functions are offered: **Count**, **Count Distinct**, **Sum**, **Average**, **Minimum** and **Maximum**. Choose **Sum** to add the amounts together.

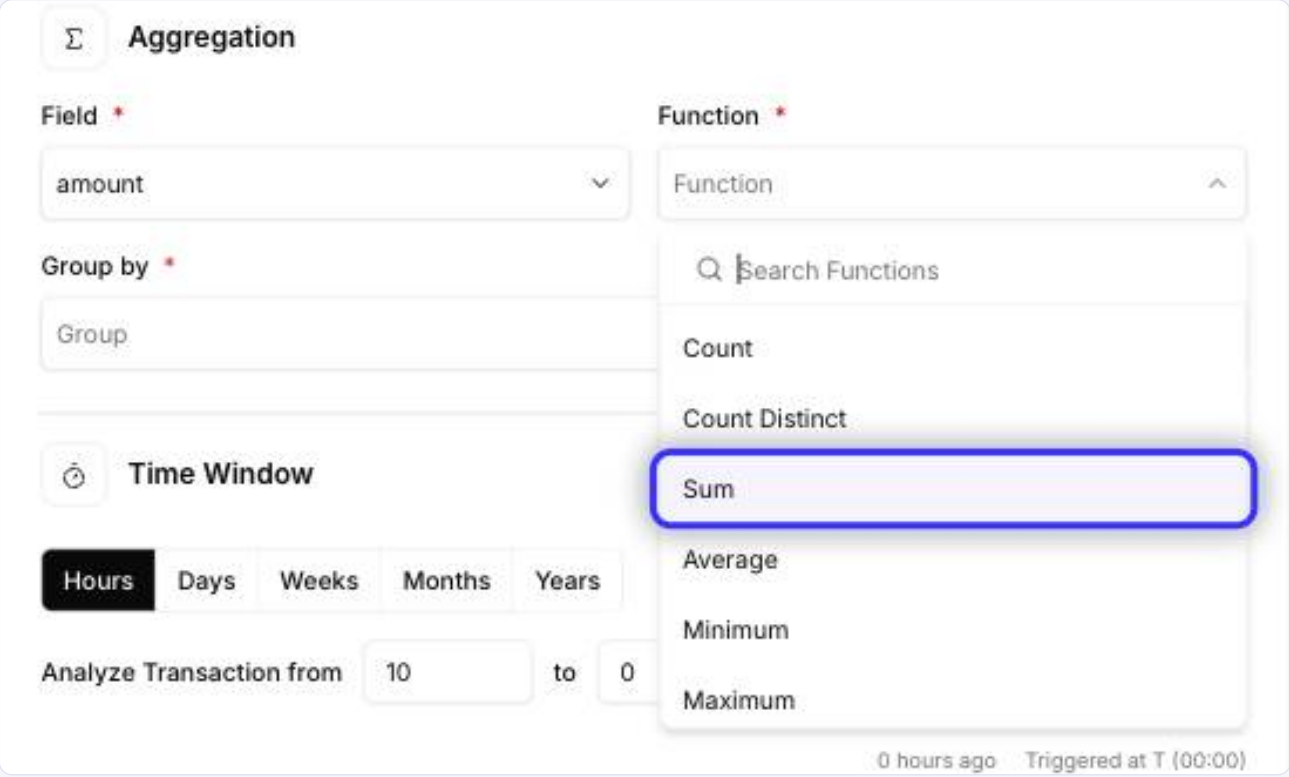


Figure 9.52 Function for amount: all six functions

Step 4 **Choose Group by: sender_entity_id**

Open **Group by**, type `sender_entity` and choose `sender_entity_id`, so each sender gets their own total.



Figure 9.53 Group by: sender_entity_id

Step 5 **Set the time window: Days, 30 to 0**

Click **Days** (1) and set **Analyze Transaction from** 30 **to** 0 (2).



Figure 9.54 Time window 30 to 0 Days ago

Step 6 **Leave the filter row empty and save**

Leave the blank filter row (1) empty, so every payment counts towards the total, and click **Save Variable** (2).

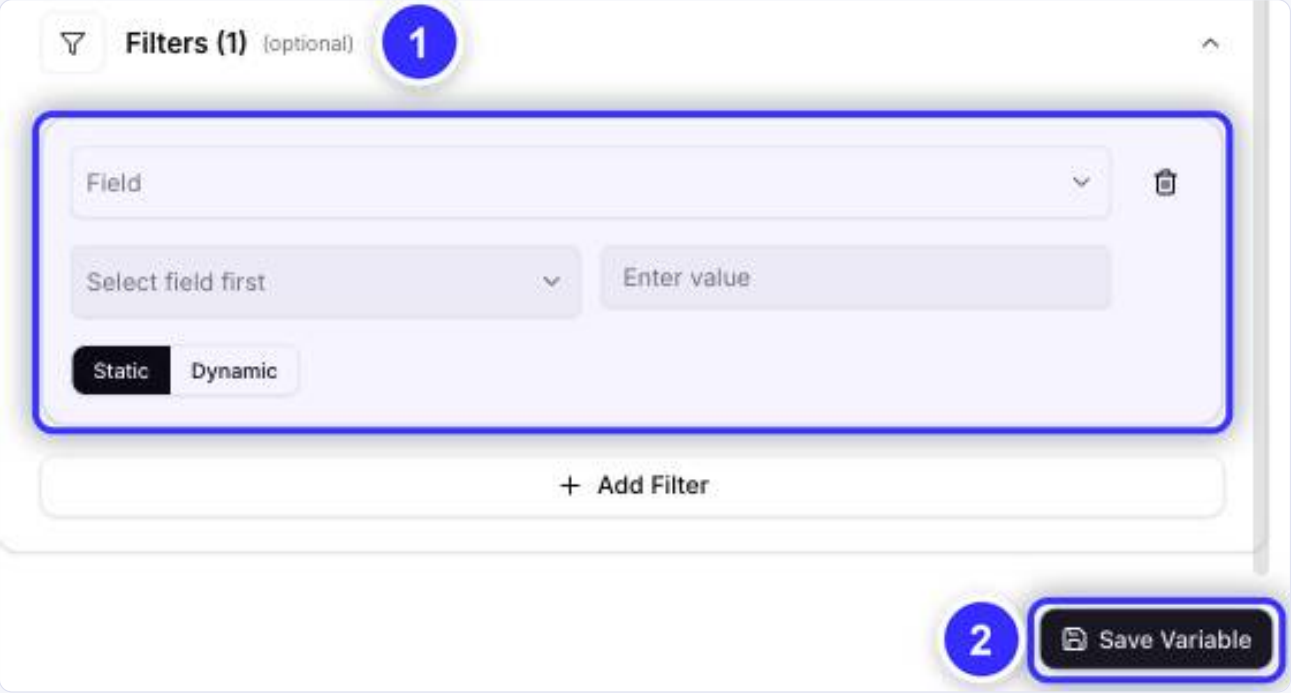


Figure 9.55 Blank filter row and Save Variable

Step 7 **Find the variable in the list**

The new variable is the first row, here VAR-08102026-000771.

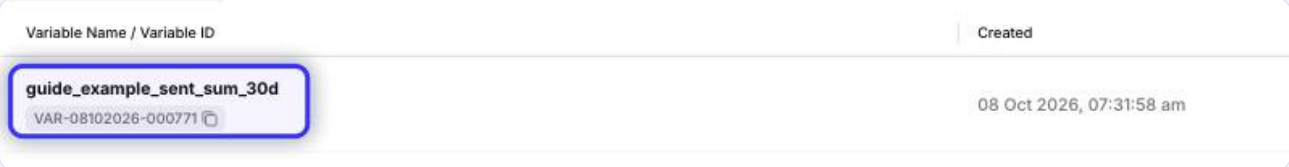


Figure 9.56 Rule 3 variable in the Variables list

Step 8 **Check the saved variable**

View Variable shows the type tag **NUM_AGG_SUM** (1), the created and updated details (2), 30 to 0 **Days ago** (3) and **Filters (0)** (4).

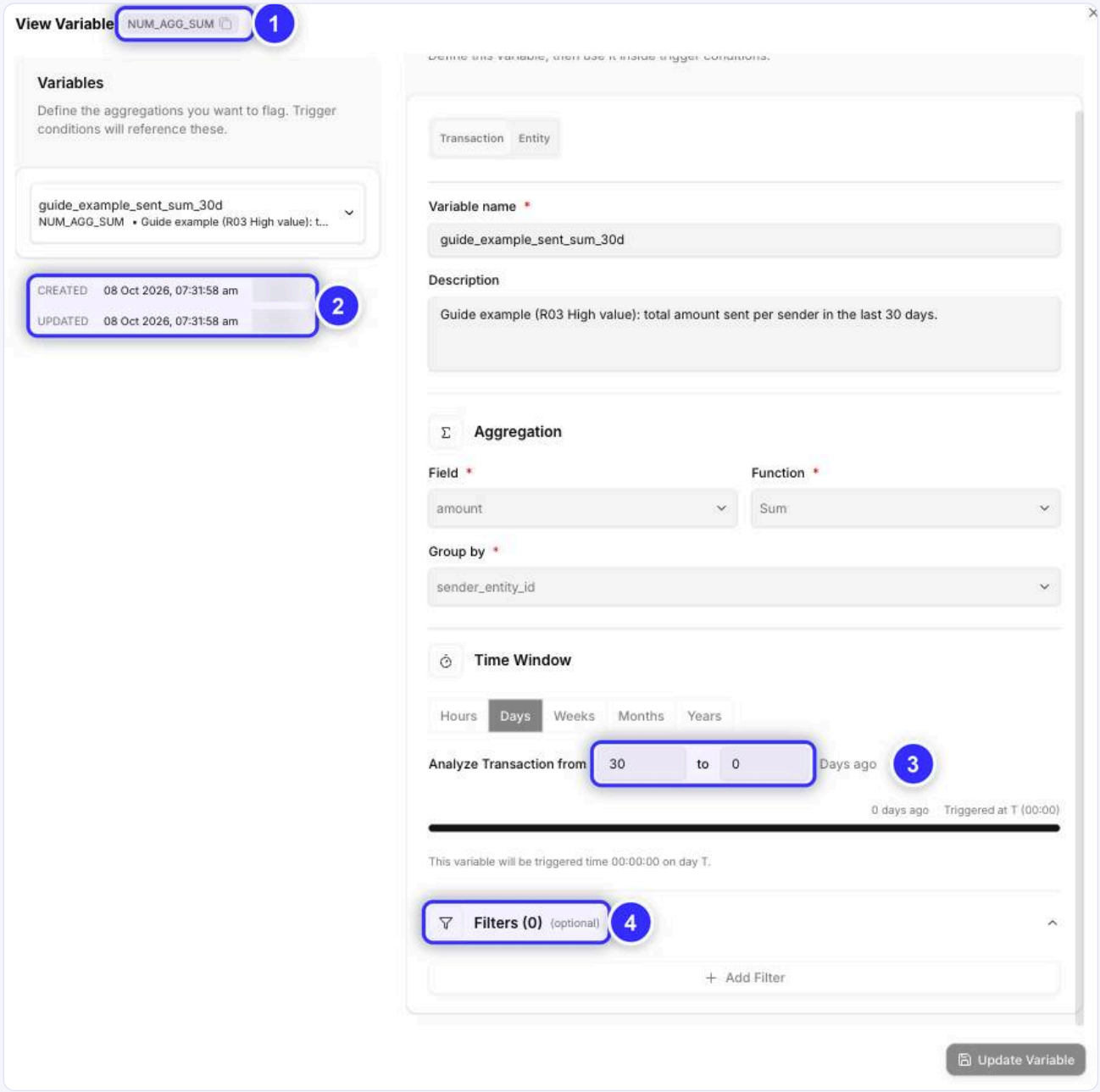


Figure 9.57 View Variable for the Rule 3 variable

Part B: Create the typology

Fyscal ARCX → Transaction Monitoring → Typology → + New

Step 9 **Fill in the details and choose High Value**

Click **+ New** on **Typology**. Type the name `R03 High value - PHP 5000000 or more sent in 30 days` (1), set **Suppression Window** 30 **Day** (2), matching the 30-day window, and write a description (3). Open **Typology type** (4) and type `High`: three types match, **High Value** HV01, **High Value Transfer** HV02 and **High Value** HV03. Click **High Value** HV01.



Figure 9.58 Rule 3 details and the Typology type search for High

Step 10 **Choose the variable in row 1**

Click **Select field** and type `sent_sum`. The list can show similar variables from other rules; click `sent_sum_30d`.

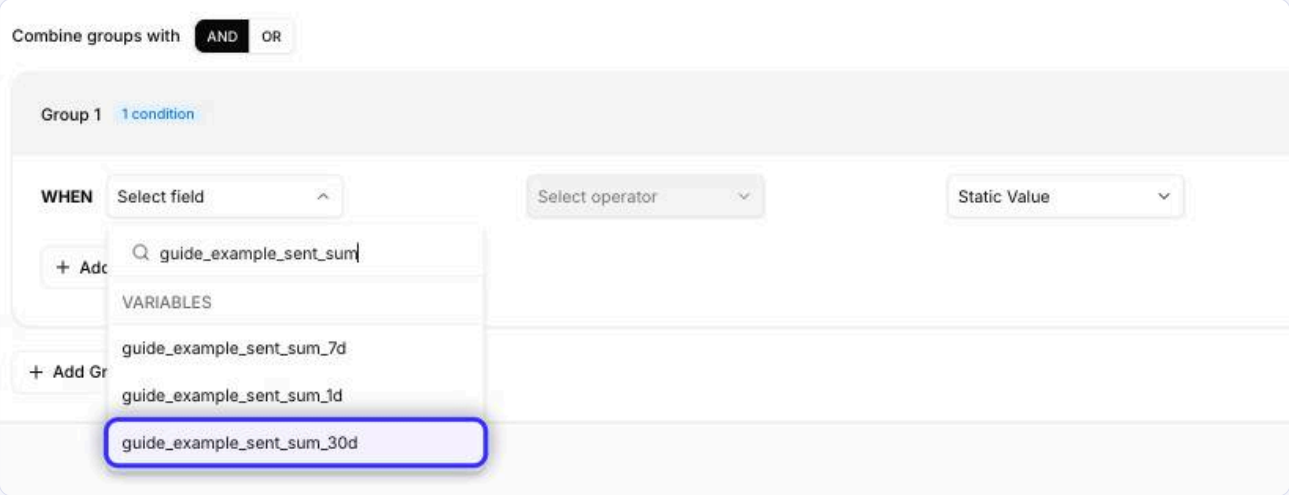


Figure 9.59 Rule 3 row 1: choose sent_sum_30d

Step 11 **Choose Greater Than Equal**

Open **Select operator** and choose **Greater Than Equal**.

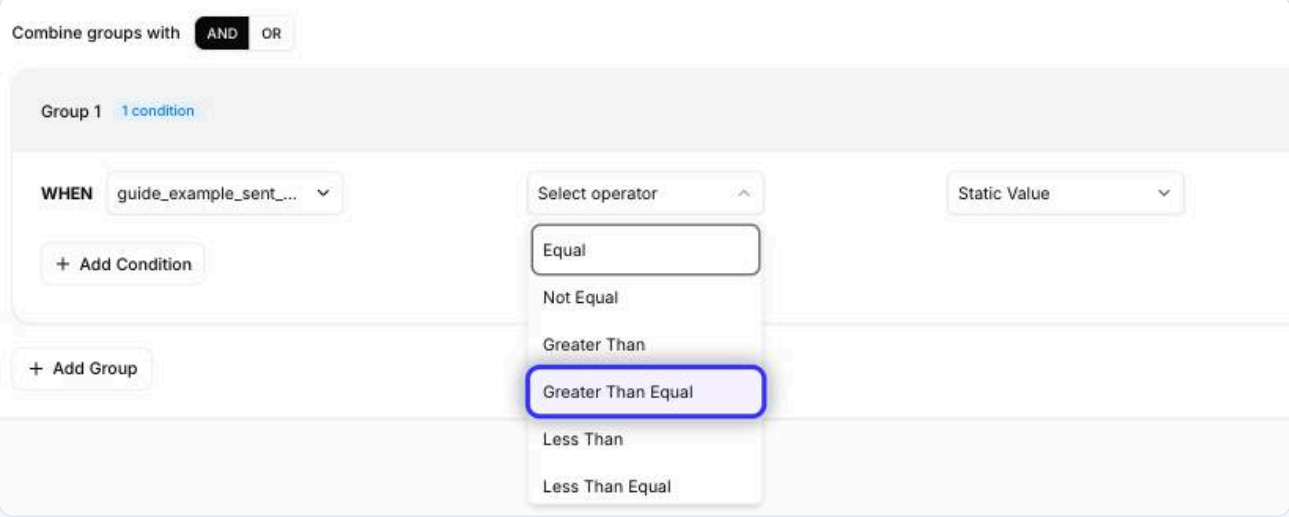


Figure 9.60 Rule 3 row 1: operator list

Step 12 **Keep Static Value**

Keep **Static Value**.



Figure 9.61 Rule 3 row 1: Static Value

Step 13 **Enter 5000000 and go to the next step**

Type 5000000 (no separators) in **Enter value**. Check the name (1), **High Value (HV01)** (2), **30 Day** (3), description (4), **Match** AND (5) and the row (6), then click **Next Step** (7).

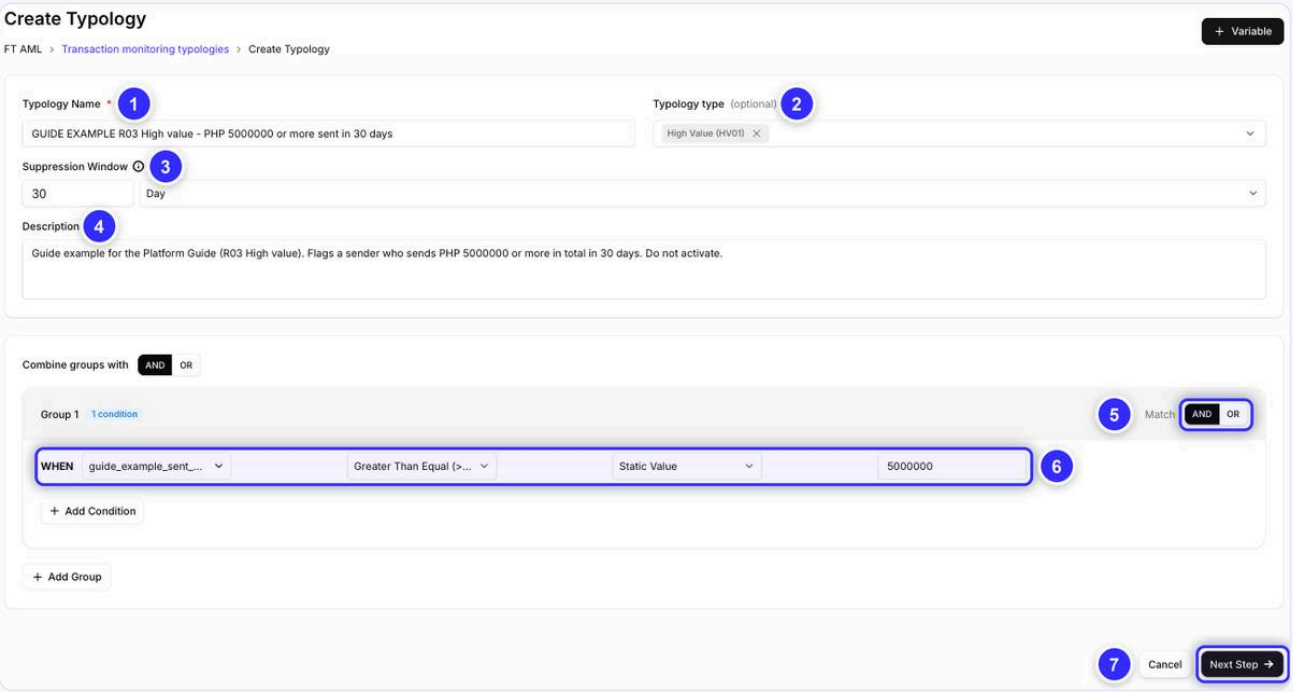


Figure 9.62 The completed Rule 3 page

Part C: Choose the schedule and save

Step 14 **Select the existing schedule**

Open **Select Schedule**, search for `schedule_2027` and click it.

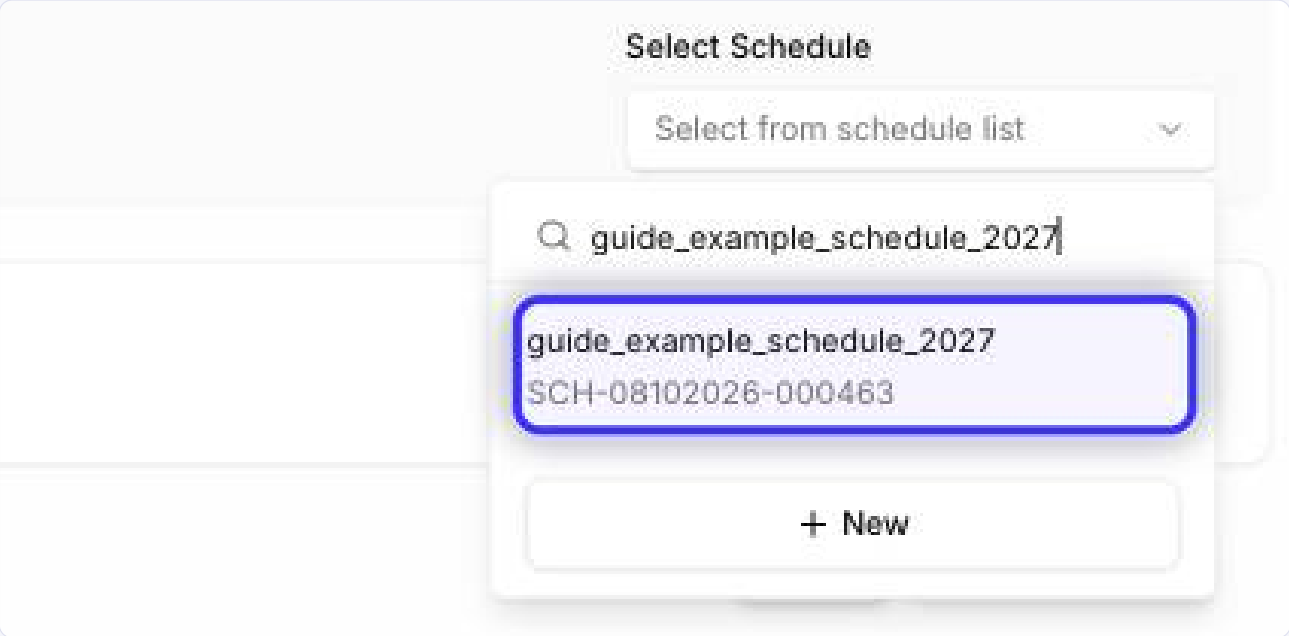


Figure 9.63 Select Schedule: the schedule from Rule 1

Step 15 **Save the draft**

Leave the shared schedule's fields (2) unchanged and click **Save as Draft** (3).

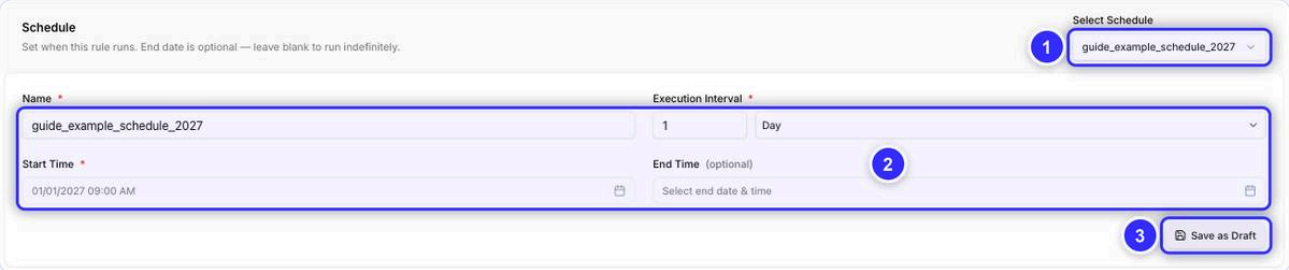


Figure 9.64 The selected schedule and Save as Draft

Step 16 **Check the saved draft**

The page becomes **Update Typology** (1) with the run sentence (3), **Dry Run** (5) and **Activate** (6).

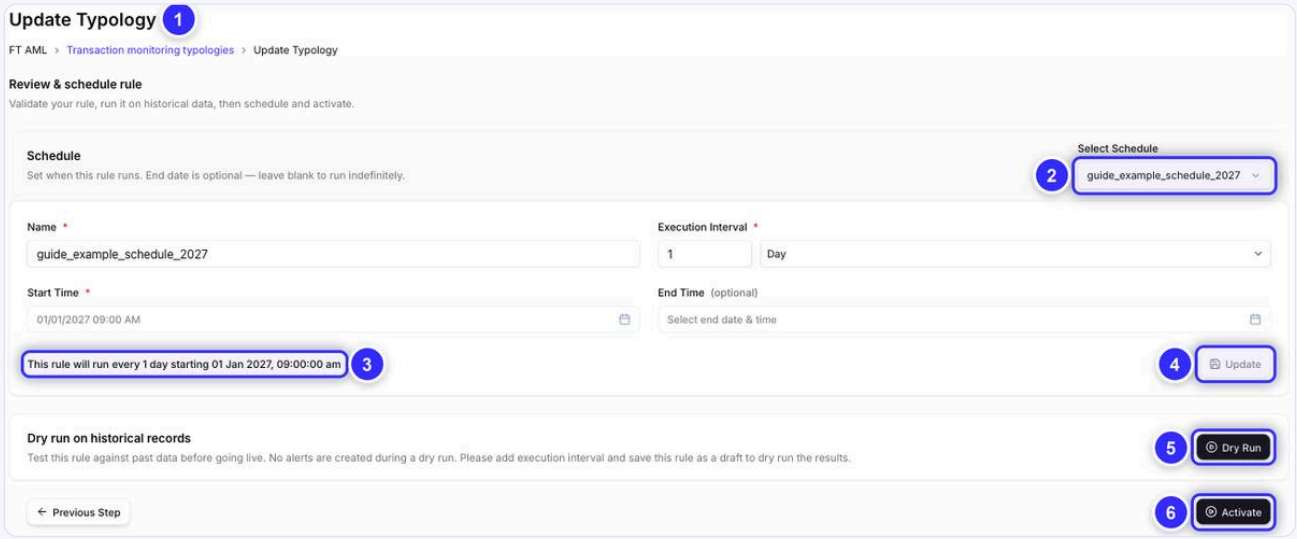


Figure 9.65 Rule 3 after Save as Draft

Step 17 **Check the rule page**

The rule page shows **Draft** TMR-08102026-001125 (1), **SUPPRESSION** 30Day and **TYPOLOGY** High Value (2), the condition with 5000000 (3) and the variable card, **Num_agg_sum**, in last 30 day (4).

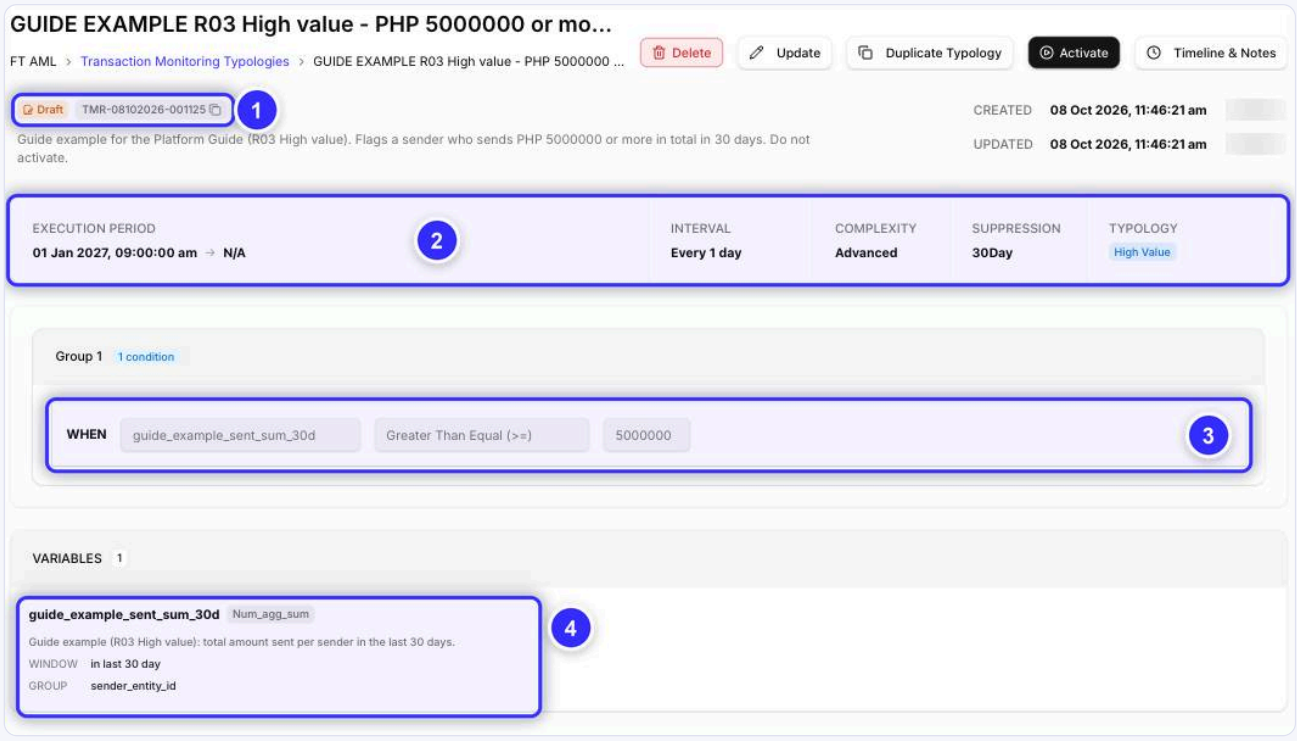


Figure 9.66 The saved Rule 3 as a Draft

How it evaluates. At each daily run the variable adds up each sender's payments over the last 30 days. Sender A sent ₱2,000,000, ₱1,800,000 and ₱1,500,000: the total is ₱5,300,000, which is >= 5000000, so the rule raises an alert. Sender B sent one payment of ₱4,900,000: the total is below ₱5,000,000 and there is no alert.

Dry-run result. In testing, no sender reached ₱5,000,000 in 30 days, so the rule created 0 alerts. With the threshold temporarily at 1 it created 6,512 alerts, then the threshold was restored.

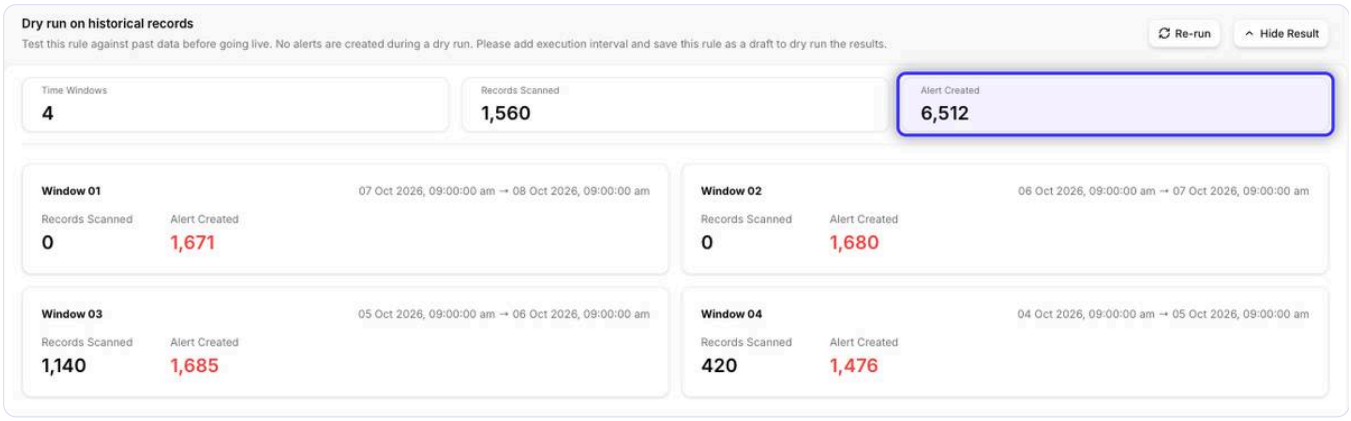


Figure 9.67 Rule 3 positive control (threshold temporarily >= 1): 6,512 alerts

Tuning. You can change the amount (5000000), the window (30 Days), and the **Suppression Window** (30 Day). Variant, not tested with Dry Run: for incoming value, build a second variable that sums `amount` grouped by `receiver_entity_id`. To total only one kind of transaction, add a filter row. Choose the amount from your own risk assessment and check the alert volume with a **Dry Run**.

Rule 4 · Dormant account

RED FLAG **Activity after a long quiet period**

LOGIC

Checks that the sender had no transactions from 100 to 1 days ago, then adds up what they sent in the last day.

WINDOW

100 to 1 Days and 1 to 0 Days

THRESHOLD

Sum ≥ ₱5,000 AND sum ≥ 1,000,000,000,000 × count

✓ Verified · 279 alerts

What it detects and why. This rule flags a sender who made no transactions from 100 days ago up to yesterday, and then sends ₱5,000 or more in the last day. An account that wakes up after a long quiet period and moves money straight away is a change in behaviour worth reviewing.

It needs two variables, one for the quiet period and one for the new activity, and two conditions that must both be true. The screens are the same as in Rule 1.

Item	Setting
Variable A `count_100d_to_1d`	**Count** of `id`, grouped by `sender_entity_id`, **Days** from 100 to 1: the transactions from 100 days ago up to 1 day ago, leaving out the last day
Variable B `sent_sum_1d`	**Sum** of `amount`, grouped by `sender_entity_id`, **Days** from 1 to 0: the amount sent in the last day
Typology type	Anomaly (TP103)
Suppression Window	1 Day
Conditions	Group 1, Match AND: `sent_sum_1d` **Greater Than Equal (>=)** 5000 AND `sent_sum_1d` **Greater Than Equal (>=)** variable `count_100d_to_1d`, multiplier 1000000000000
Schedule	Existing `schedule_2027` (created in Rule 1): every 1 Day, start moved to 16 Oct 2026, 10:00 AM, no end time

Part A: Create variable A, the quiet period

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 1 **Open the form and name variable A**

Click **+ New** on **Variables**. Type `count_100d_to_1d` (1) and a description such as “Number of transactions per sender from 100 days ago up to 1 day ago (excludes the last day).” (2).

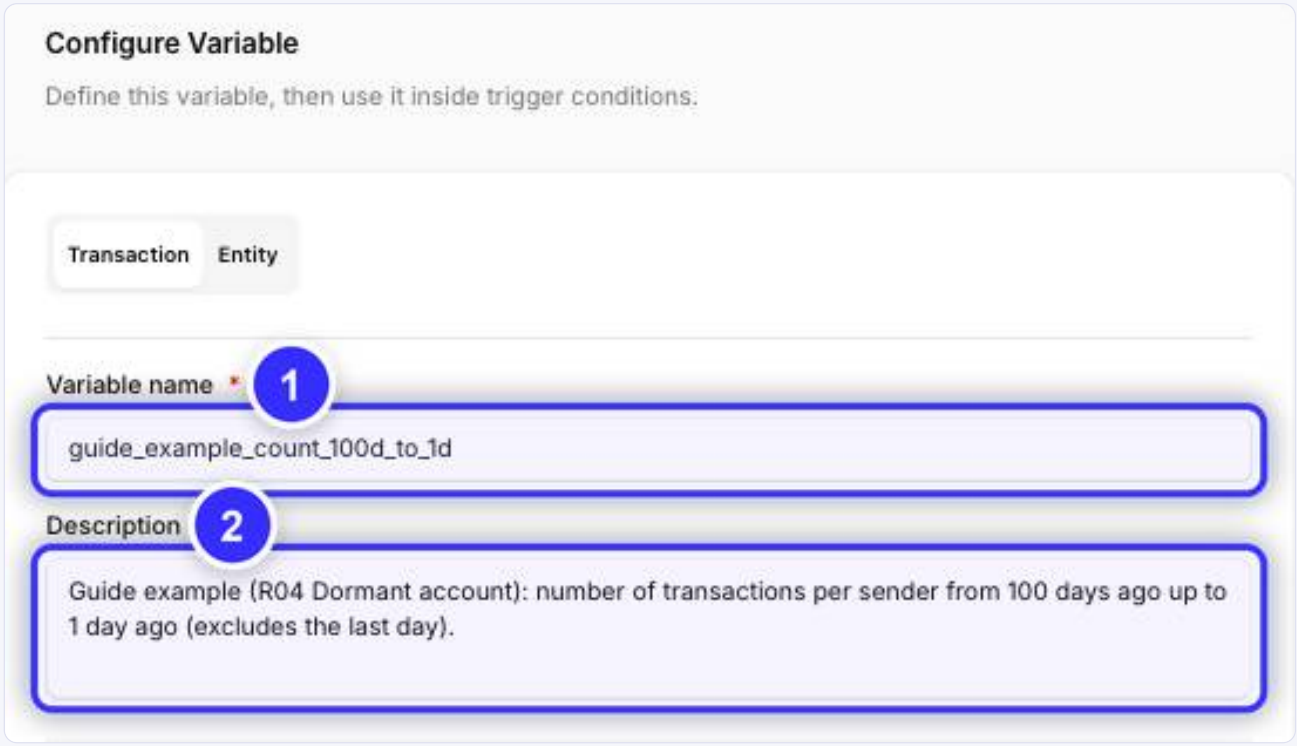


Figure 9.68 Variable A: name and description

Step 2 **Choose the Field: id**

Open **Field**, search `id` and choose `id`.

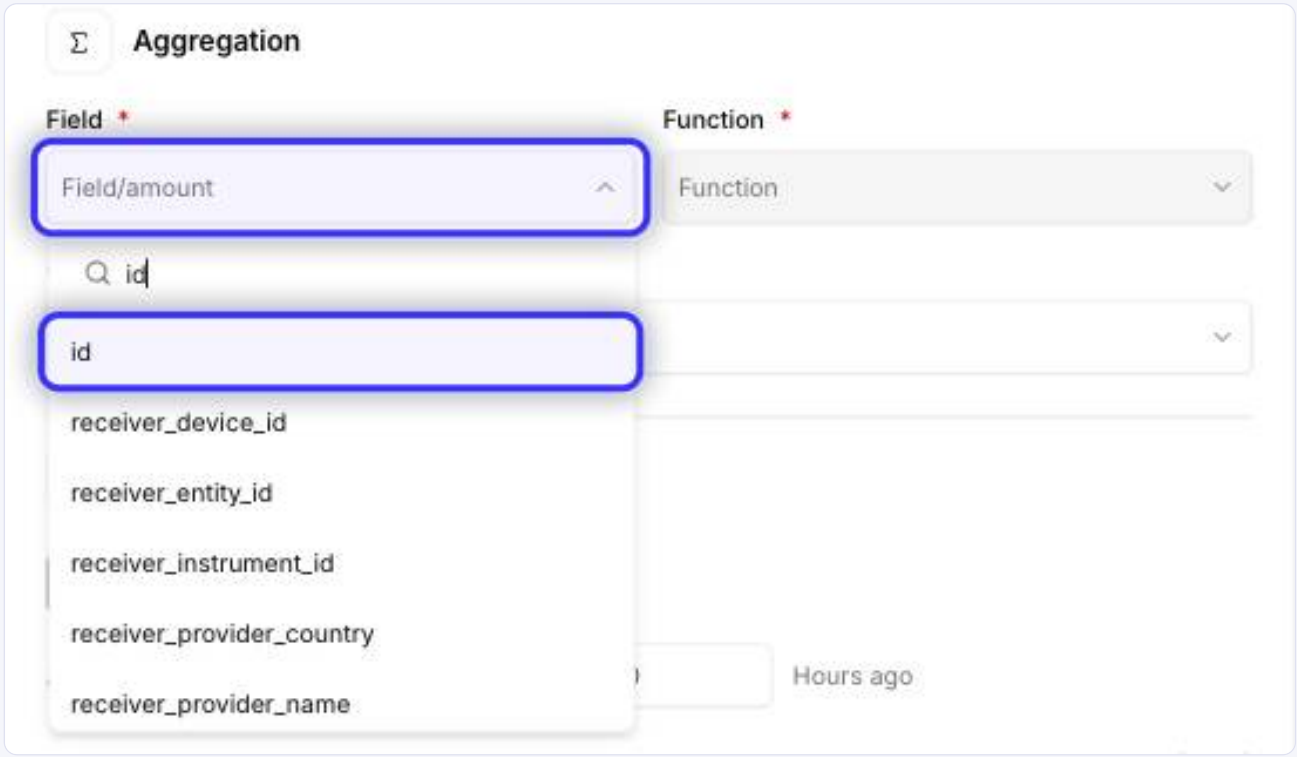


Figure 9.69 Variable A: Field id

Step 3 **Choose the Function: Count**

Choose **Count**: the rule needs to know whether there were any transactions at all.

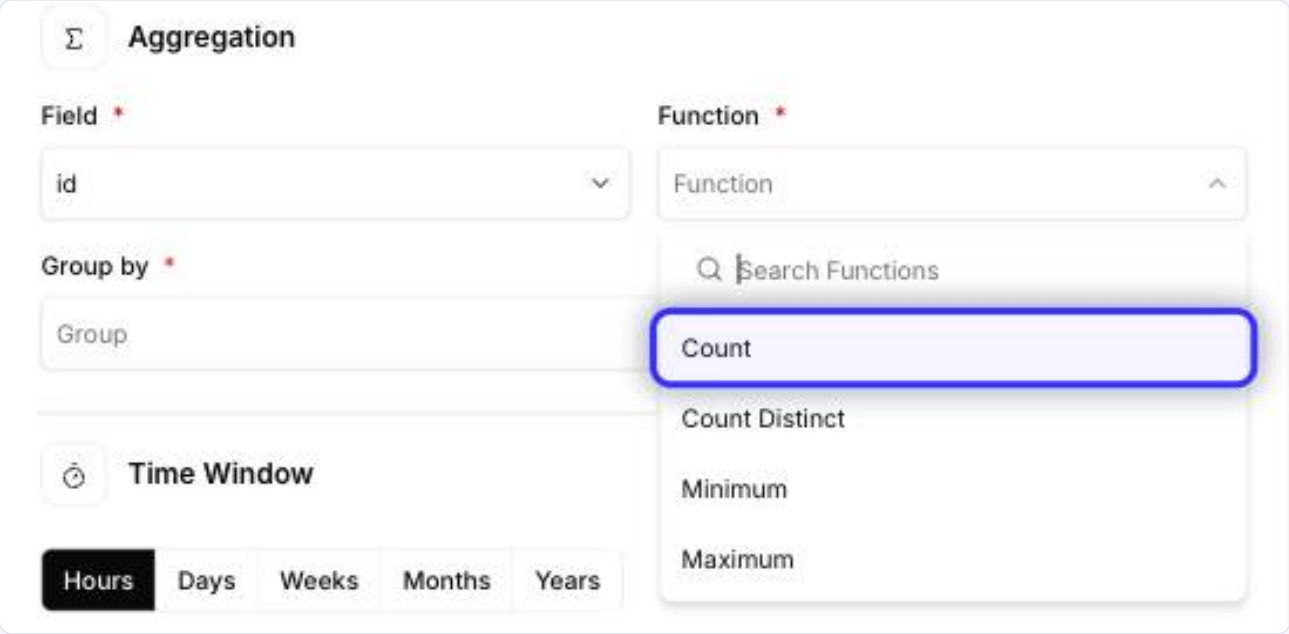


Figure 9.70 Variable A: Function Count

Step 4 **Choose Group by: sender_entity_id**

Search `sender_entity` and choose `sender_entity_id`.



Figure 9.71 Variable A: Group by sender_entity_id

Step 5 **Set the window: Days, 100 to 1**

Click **Days** (1), then enter 100 in **Analyze Transaction from** and 1 in **to** (2). The form accepts a window that ends before the trigger time, and the caption reads "1 day ago · Triggered at T (00:00)" (3). Ending at 1 leaves out the last day, so the payment that wakes the account up does not count against the quiet period.



Figure 9.72 Variable A: window 100 to 1 Days ago

Step 6 **Leave the filter row empty and save**

Leave the blank filter row (1) empty and click **Save Variable** (2).

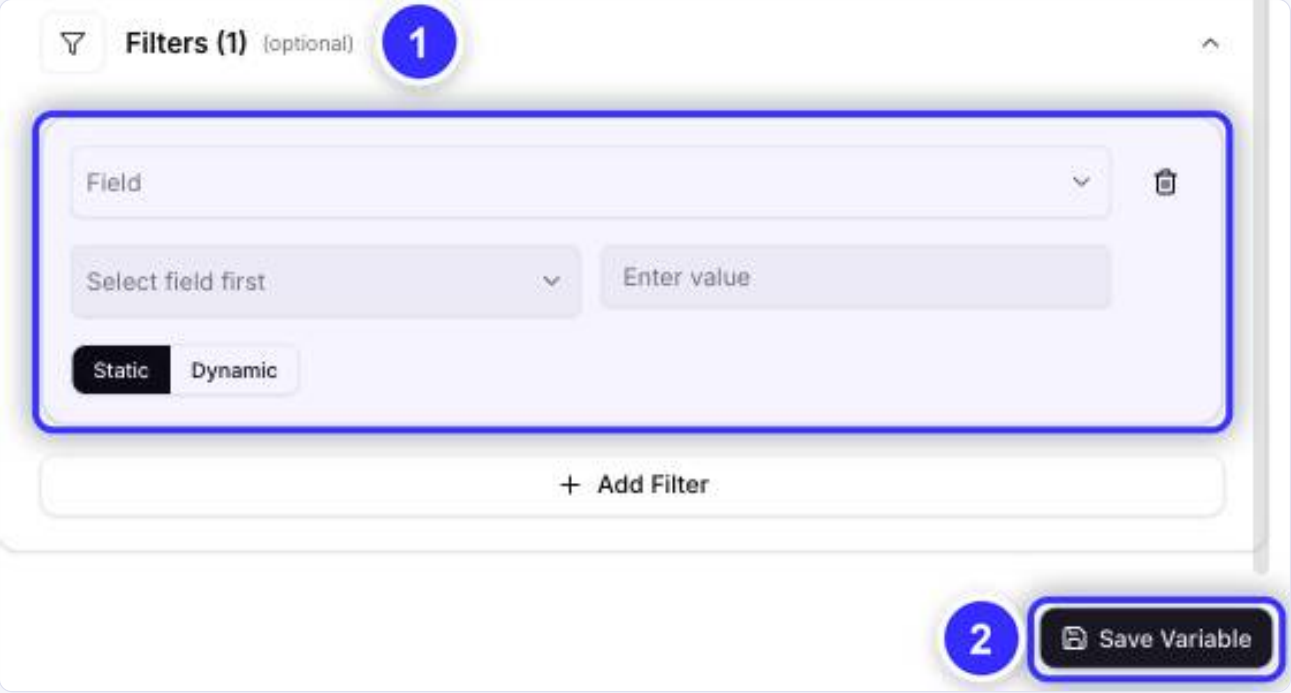


Figure 9.73 Variable A: blank filter row and Save Variable

Step 7 **Find variable A in the list**

Variable A is the first row, here VAR-08102026-000772.

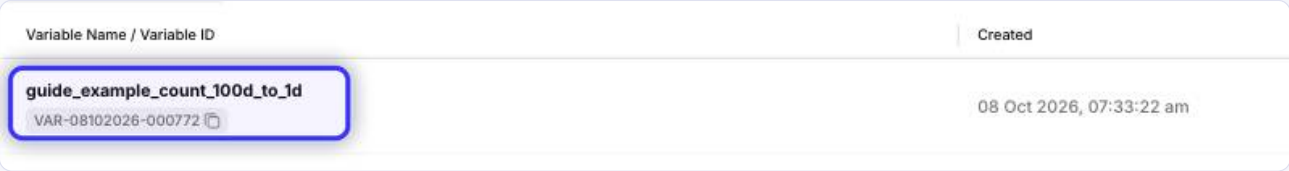


Figure 9.74 Variable A in the Variables list

Step 8 **Check variable A**

View Variable shows **STR_AGG_COUNT** (1), the created and updated details (2), 100 to 1 **Days ago** (3), **Filters (0)** (4) and the caption “1 day ago” (5): the end of the window was saved.

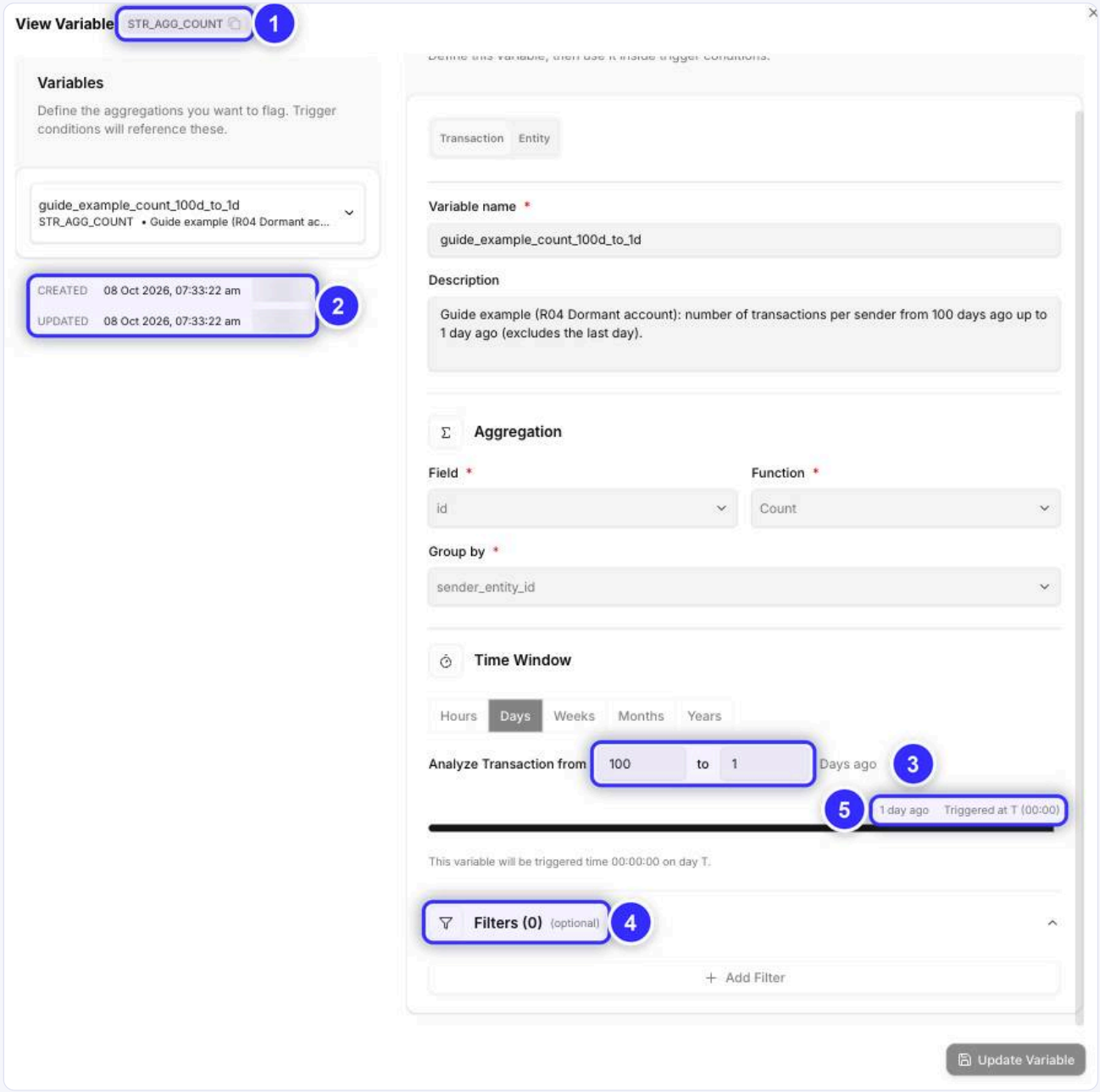


Figure 9.75 View Variable for variable A, window 100 to 1

Part B: Create variable B, the new activity

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 9 **Open the form and name variable B**

Click **+ New** again. Type `sent_sum_1d` (1) and a description such as “Total amount sent per sender in the last 1 day.” (2).

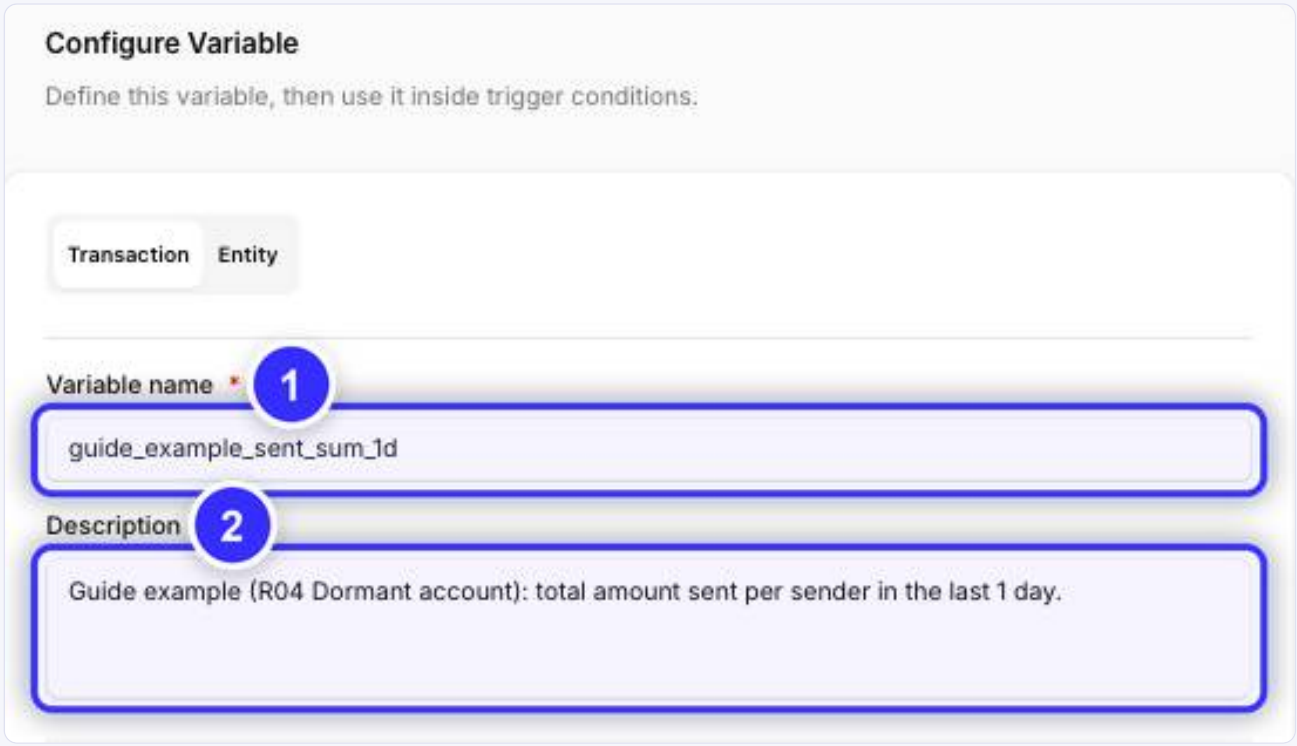


Figure 9.76 Variable B: name and description

Step 10 **Choose the Field: amount**

Open **Field** and choose `amount`.

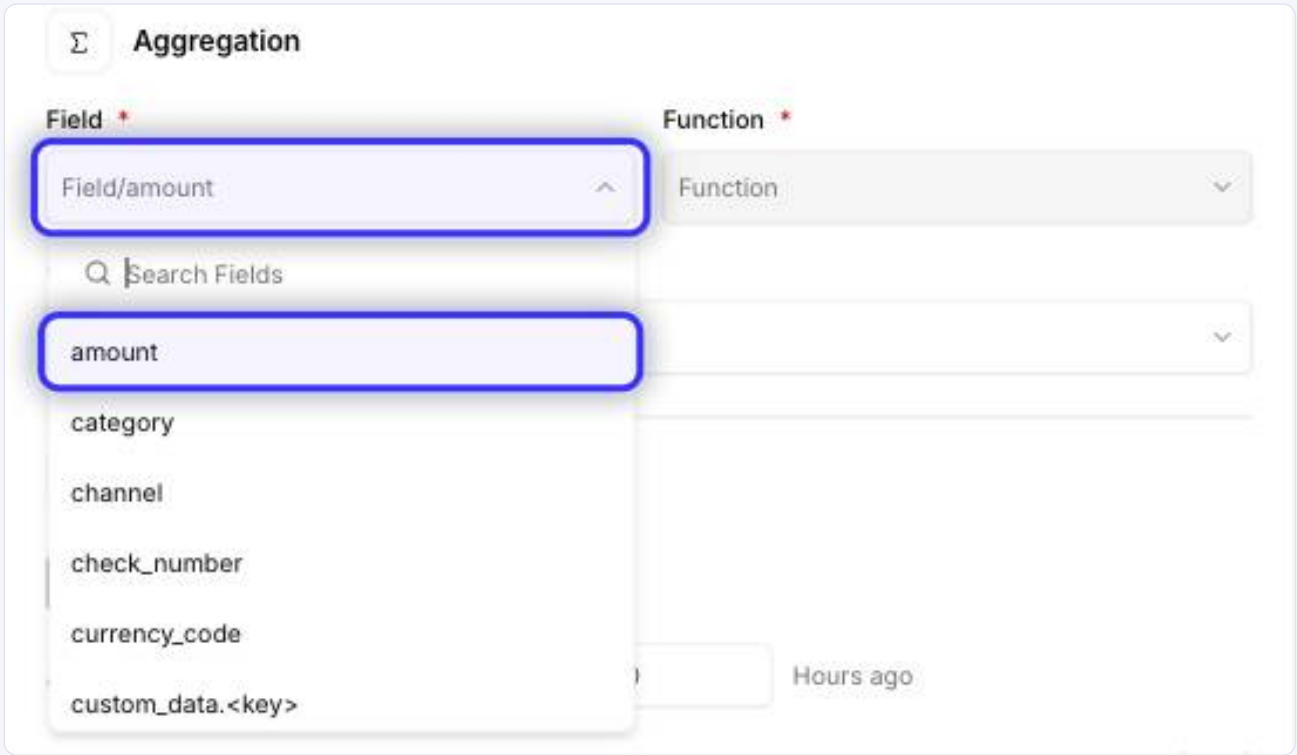


Figure 9.77 Variable B: Field amount

Step 11 **Choose the Function: Sum**

Choose **Sum** from the six functions offered for a numeric field.

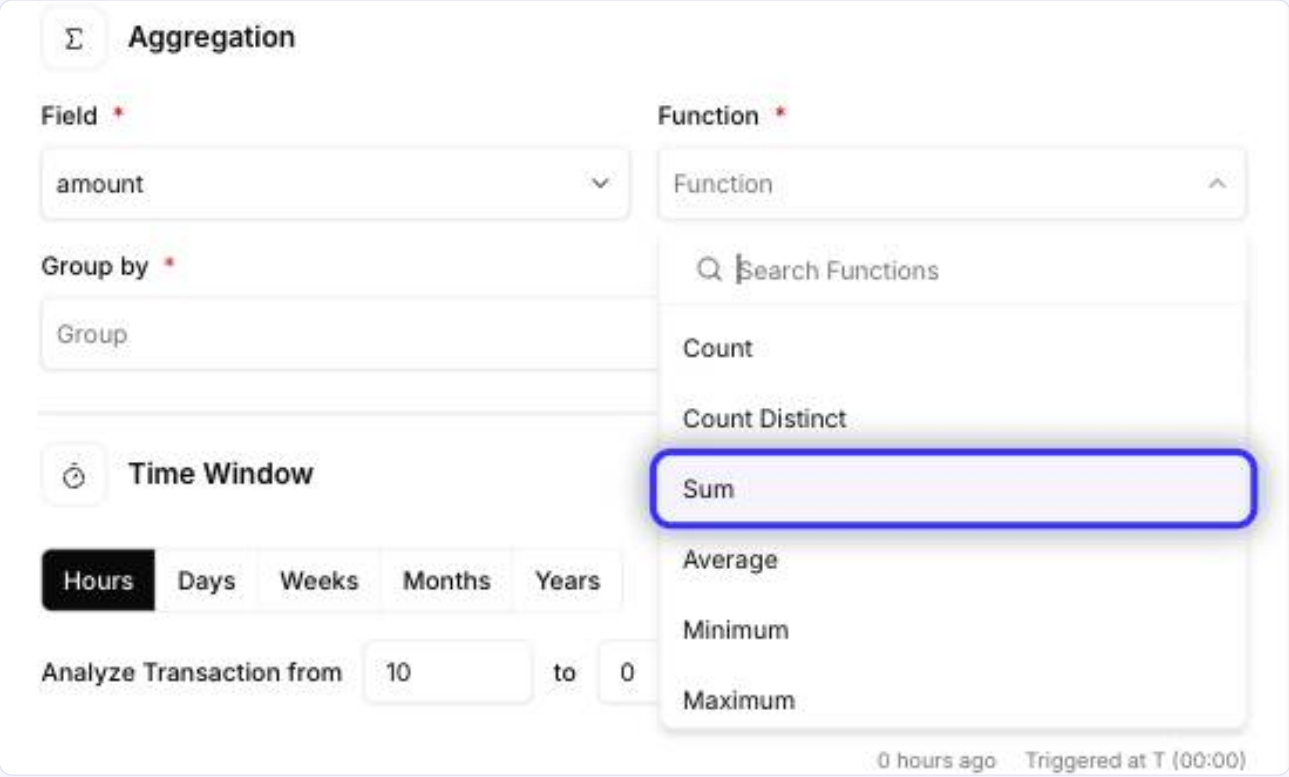


Figure 9.78 Variable B: Function Sum

Step 12 **Choose Group by: sender_entity_id**

Search `sender_entity` and choose `sender_entity_id`. Both variables must use the same Group by, so that the two conditions talk about the same sender.



Figure 9.79 Variable B: Group by sender_entity_id

Step 13 **Set the window: Days, 1 to 0**

Click **Days** (1) and set 1 **to** 0 (2): the last day, the part that variable A leaves out.



Figure 9.80 Variable B: window 1 to 0 Days ago

Step 14 **Leave the filter row empty and save**

Leave the blank filter row (1) empty and click **Save Variable** (2).

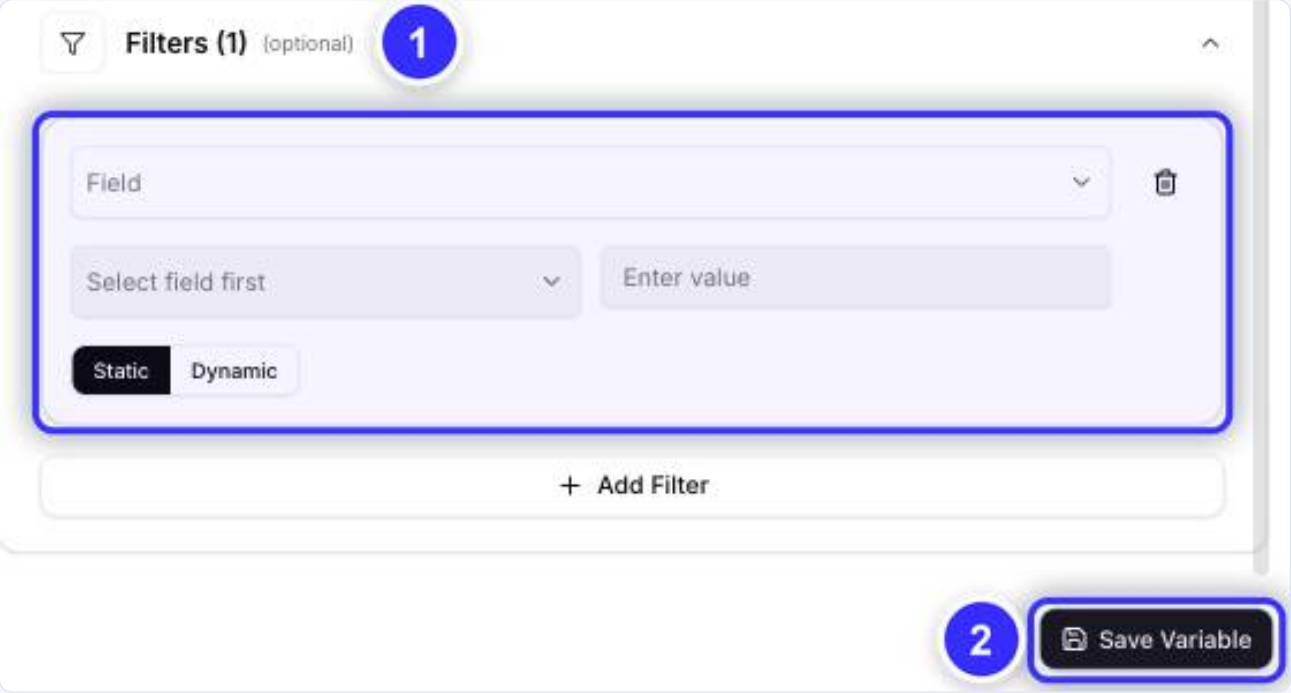


Figure 9.81 Variable B: blank filter row and Save Variable

Step 15 **Find variable B in the list**

Variable B is the first row, here VAR-08102026-000773.

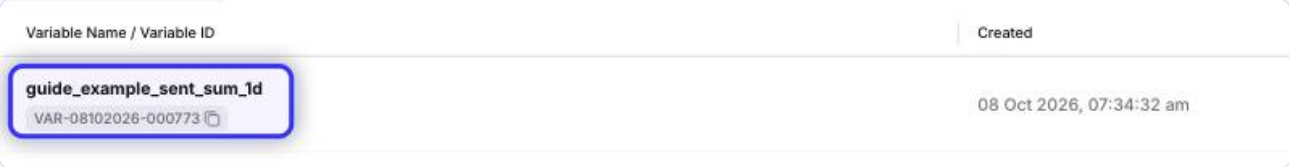


Figure 9.82 Variable B in the Variables list

Step 16 **Check variable B**

View Variable shows **NUM_AGG_SUM** (1), the created and updated details (2), 1 to 0 **Days ago** (3) and **Filters (0)** (4).

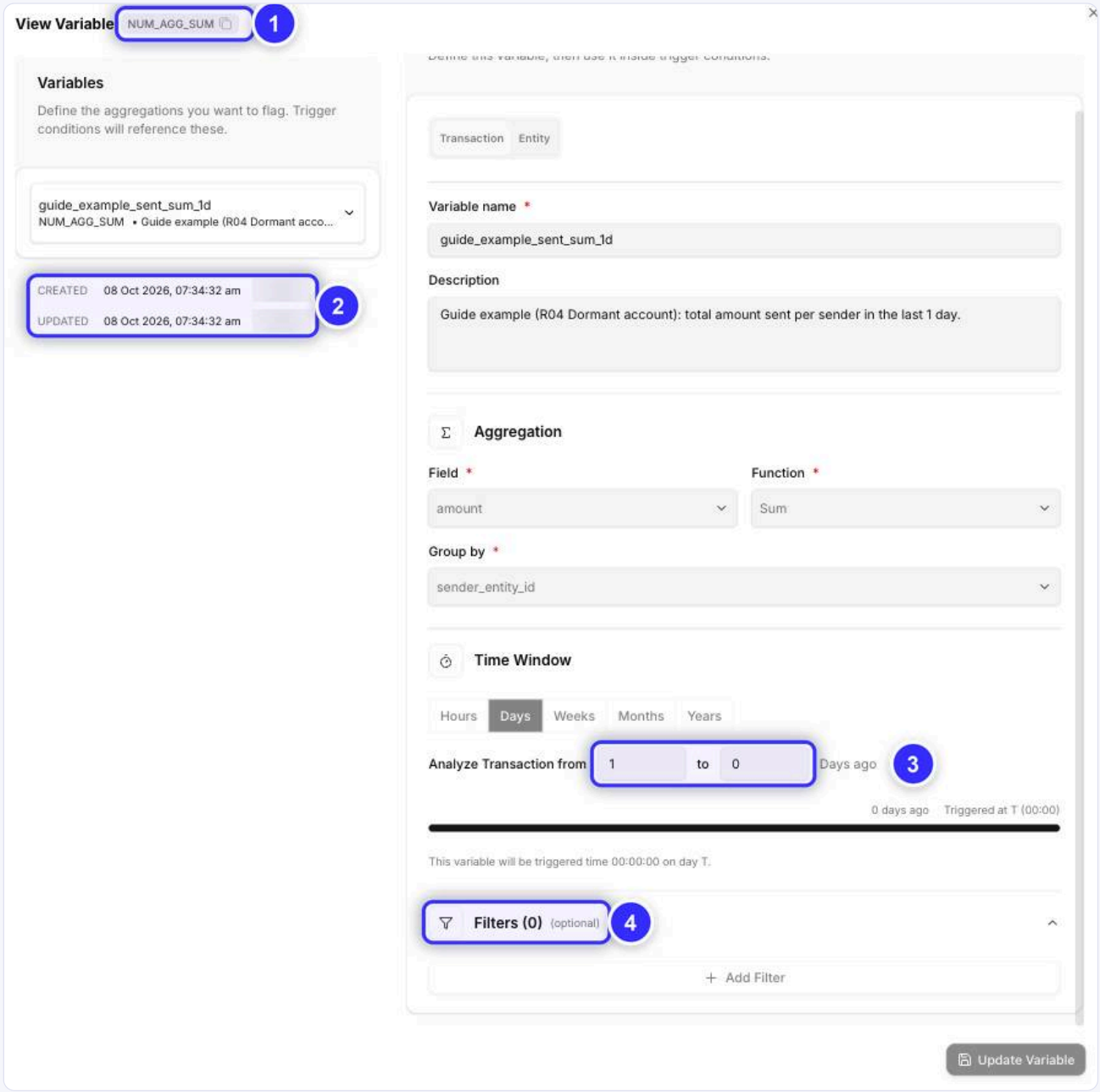


Figure 9.83 View Variable for variable B

Part C: Create the typology

Fyscal ARCX → Transaction Monitoring → Typology → + New

Step 17 **Fill in the details and choose Anomaly**

Click **+ New** on **Typology**. Type the name `R04 Dormant account - no activity for 100 days then PHP 5000 or more in 1 day` (1), set **Suppression Window** 1 **Day** (2), matching the 1-day activity window, and write a description (3). Open **Typology type** (4), type `Anomaly` and click **Anomaly** TP103.

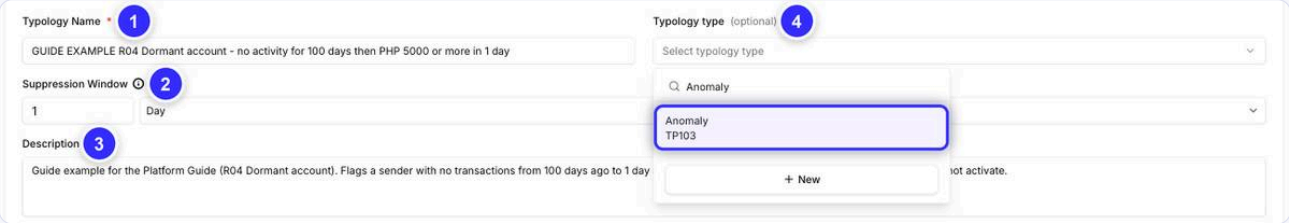


Figure 9.84 Rule 4 details and the Typology type search for Anomaly

Step 18 **Row 1: variable B Greater Than Equal 5000**

In **Group 1**, click **Select field** (1), type `sent_sum` in the search box (2) and click `sent_sum_1d` (3). Choose **Greater Than Equal**, keep **Static Value** and type 5000.

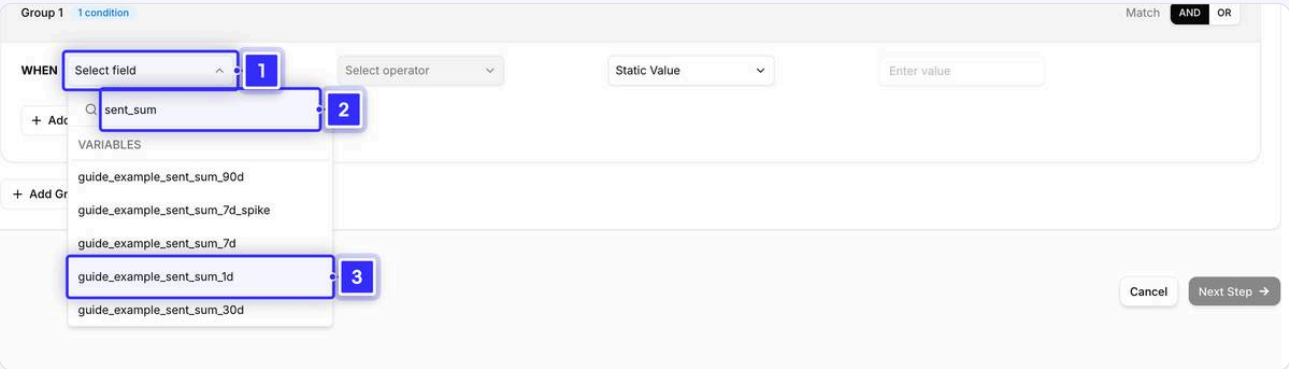


Figure 9.85 Row 1: Select field (1), the search sent_sum (2) and the variable sent_sum_1d (3)

Why not Is Null

A sender with no transactions from 100 days ago to 1 day ago has no value for variable A: it is empty, not 0, so **Equal** 0 never matches. **Is Null** is in the operator list, but it is not saved in a typology condition: an earlier version of this rule used it, and the saved rule contained only "`sent_sum_1d` ≥ 5000". On the same days that version created 1,727 alerts, against 279 for the rule below. Row 2 tests "no transactions" in a way that is saved: it compares variable B with variable A, and an empty value counts as 0 in that comparison.

Step 19 **Row 2: compare variable B with a variable**

Row 1 (1) now reads `sent_sum_1d` **Greater Than Equal** 5000. Click **Add Condition**. In row 2 choose `sent_sum_1d` again and **Greater Than Equal** (2). Open the value type, which reads **Static Value** (3), and choose **Variable** (4).

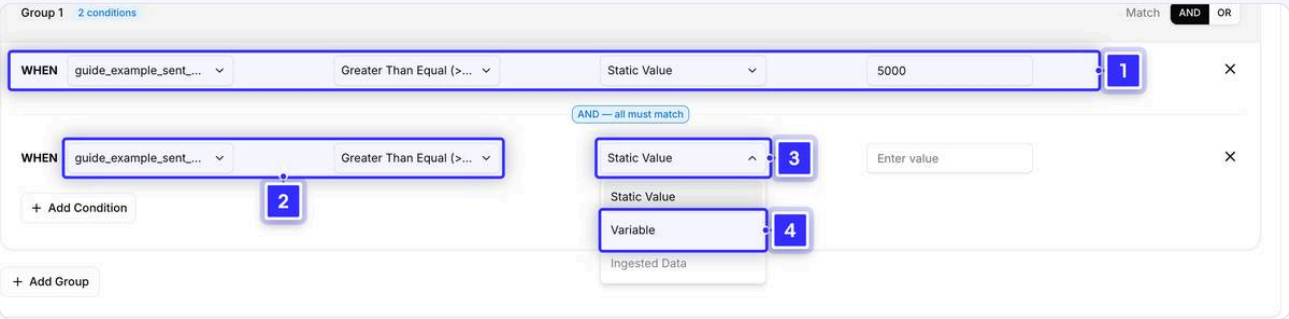


Figure 9.86 Row 1 complete (1); row 2 field and operator (2); the value type list (3) with Variable (4)

Step 20 **Row 2: choose variable A and the multiplier**

Click **Select variable**, type `count_100d` and click `count_100d_to_1d`. A **THAN MULTIPLIER** box appears under it: type 1000000000000 (one trillion). Row 2 now asks whether the amount sent in the last day is at least variable A × 1,000,000,000,000.

Step 21 **Check both rows and go to the next step**

Row 1 (1) reads `sent_sum_1d` **Greater Than Equal** 5000. **AND — all must match** (2) joins it to row 2: `sent_sum_1d` **Greater Than Equal** (3), compared with the **Variable** `count_100d_to_1d` (4) and the multiplier 1000000000000 (5). Keep **Match** on AND: with OR, every sender of ₱5,000 would alert on row 1 alone. Click **Next Step** at the bottom right.



Figure 9.87 Rule 4 conditions: row 1 (1), AND (2), row 2 field and operator (3), variable A (4) and the multiplier (5)

Part D: Choose the schedule and save

Step 22 **Select the existing schedule**

Open **Select Schedule**, search for `schedule_2027` and click it.

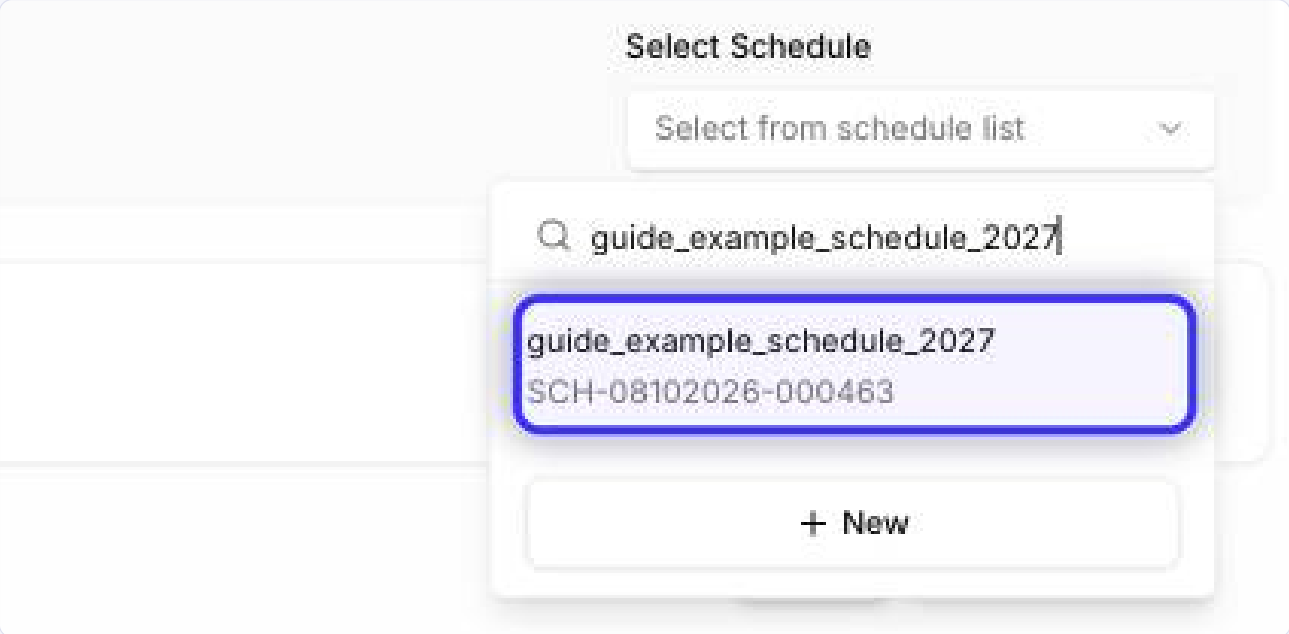


Figure 9.88 Select Schedule: the schedule from Rule 1

Step 23 **Check the start time and save the draft**

Select Schedule shows `schedule_2027` (1). The shared schedule's **Start Time** (2) must be in the future: if it is in the past, the form shows "Start time cannot be in the past" and **Save as Draft** stays greyed out. Pick a later date and time; here the start was moved to 16 Oct 2026, 10:00 AM. Two schedules with exactly the same interval and start cannot both exist: if another schedule already uses that start, the save does nothing, so choose a different time. Click **Save as Draft** (3).

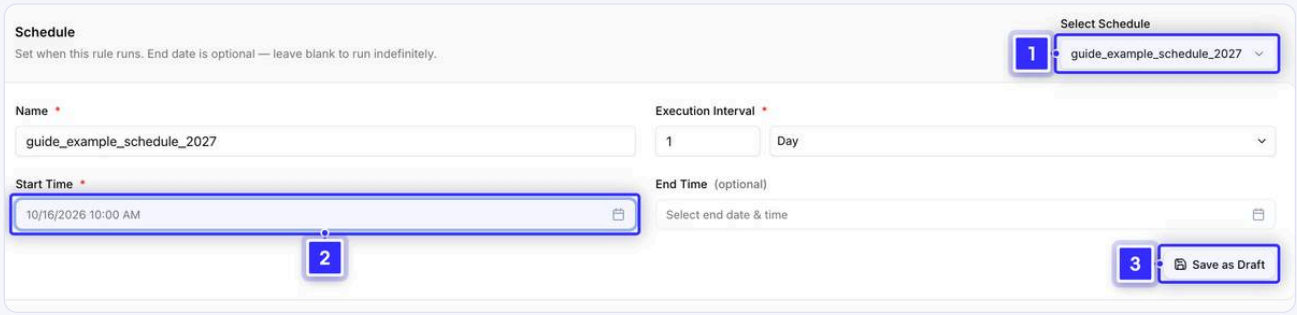


Figure 9.89 The selected schedule (1), its start time (2) and Save as Draft (3)

Note

A typology name must be unique. If another rule already has the name, **Save as Draft** does nothing and no message appears. The rebuilt example was saved with "(v2)" at the end of its name because the earlier version keeps the original one.

Step 24 **Check the saved draft**

The page becomes **Update Typology** (1), with the run sentence "This rule will run every 1 day starting 16 Oct 2026, 10:00:00 am" (2), **Dry Run** (3) and **Activate** (4).

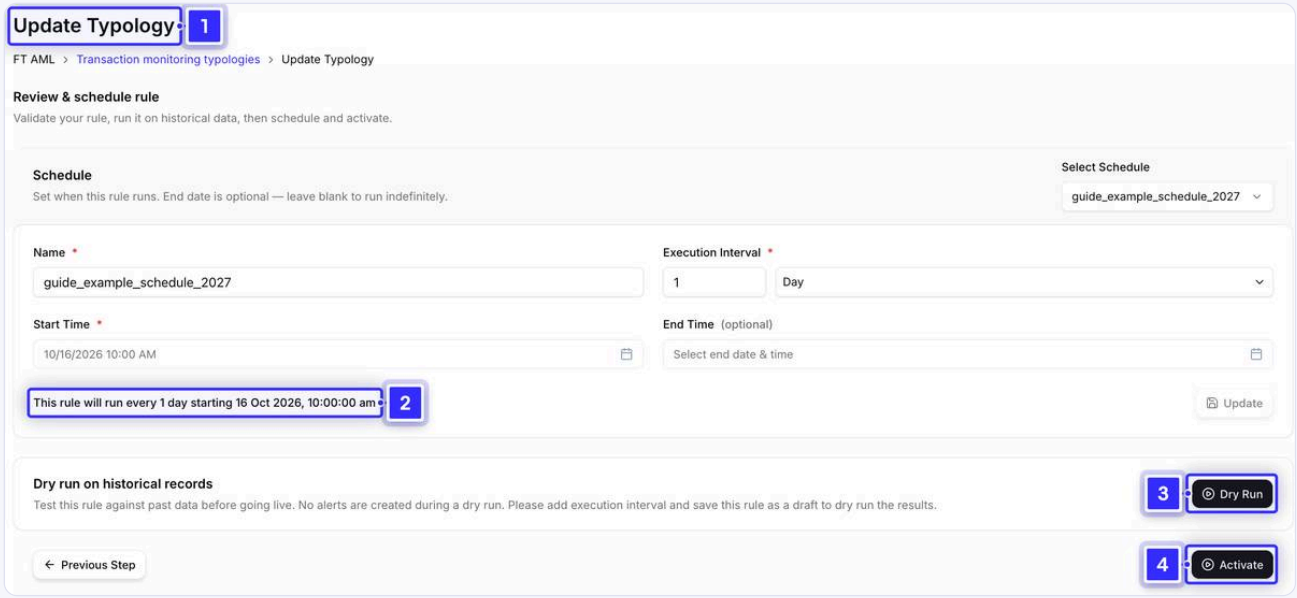


Figure 9.90 Rule 4 after Save as Draft: Update Typology (1), the run sentence (2), Dry Run (3) and Activate (4)

Step 25 **Check the saved conditions on the rule page**

Open the rule from **Transaction Monitoring → Typology**: **Draft**, TMR-15102026-001217 (1). **Group 1** shows both saved conditions: row 1 (2), `sent_sum_1d` **Greater Than Equal (>=)** 5000, and row 2 (3), `sent_sum_1d` **Greater Than Equal (>=)** `count_100d_to_1d` (multiplied by 1000000000000). Under **VARIABLES 2** (4) both variables are listed. Always check this page after saving: a condition that was not saved does not appear here.

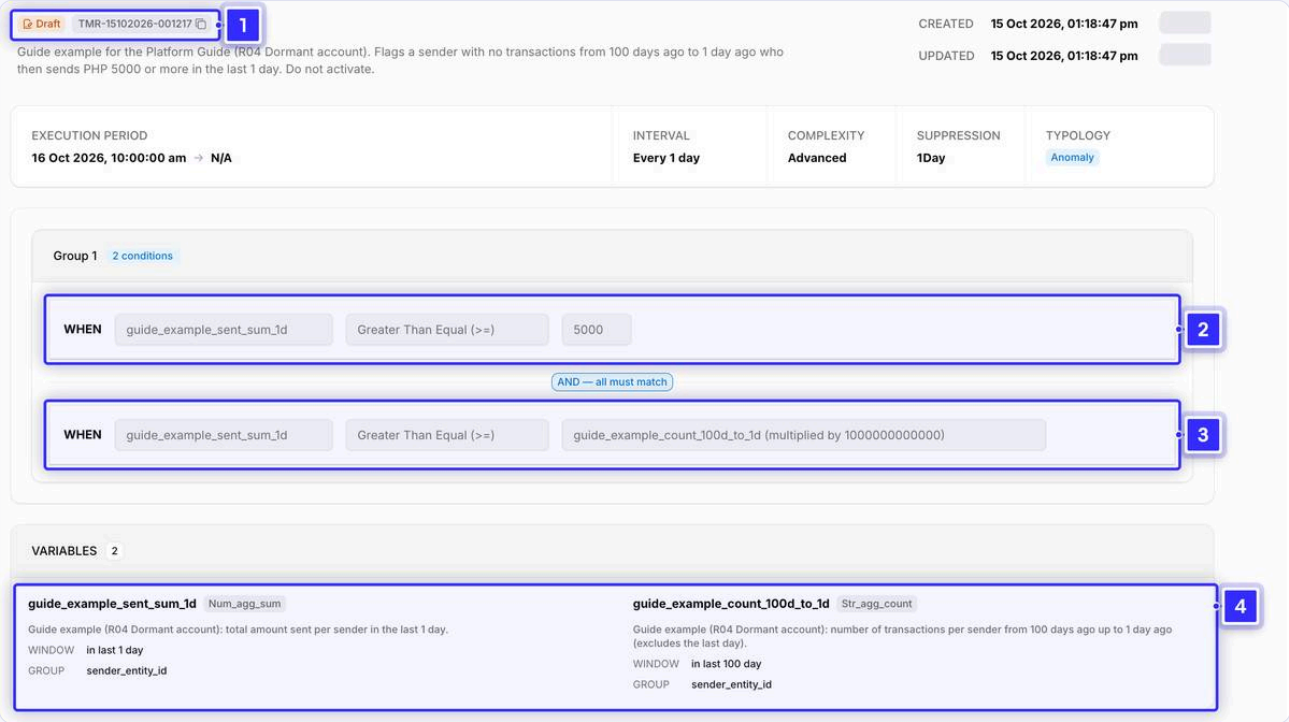


Figure 9.91 Rule 4 rule page: the draft ID (1), the two saved conditions (2) and (3), and the two variables (4)

Note

The variable card on the rule page summarises variable A's window as “in last 100 day” and does not show that the window ends 1 day ago. The saved setting is 100 to 1 Days ago, as **View Variable** shows in step 8. Check the window on **View Variable**, not on the card.

How it evaluates. At each daily run both variables are calculated for each sender, and both conditions must be true. Sender A last transacted 120 days ago and sent ₱20,000 in the last day: variable A (100 to 1 days ago) is empty and counts as 0 in row 2, so ₱20,000 >= 5000 and ₱20,000 >= 0 × 1,000,000,000,000 are both true: the rule raises an alert. Sender B also sent ₱20,000 in the last day but made one ₱500 payment 40 days ago: variable A is 1, and ₱20,000 is far below 1 × 1,000,000,000,000, so row 2 is false and there is no alert. Sender C was quiet for 100 days and sent ₱3,000 in the last day: row 1 is false, no alert. Because variable A stops 1 day ago, sender A's ₱20,000 payment does not count in variable A.

Dry-run result. In testing the rule created 279 alerts: 0 / 50 / 126 / 103 by window, newest first (1 to 4). On the same four days, the earlier version, saved without its “no transactions” condition, created 1,727: row 2 removes the senders who had transactions in the previous 100 days.

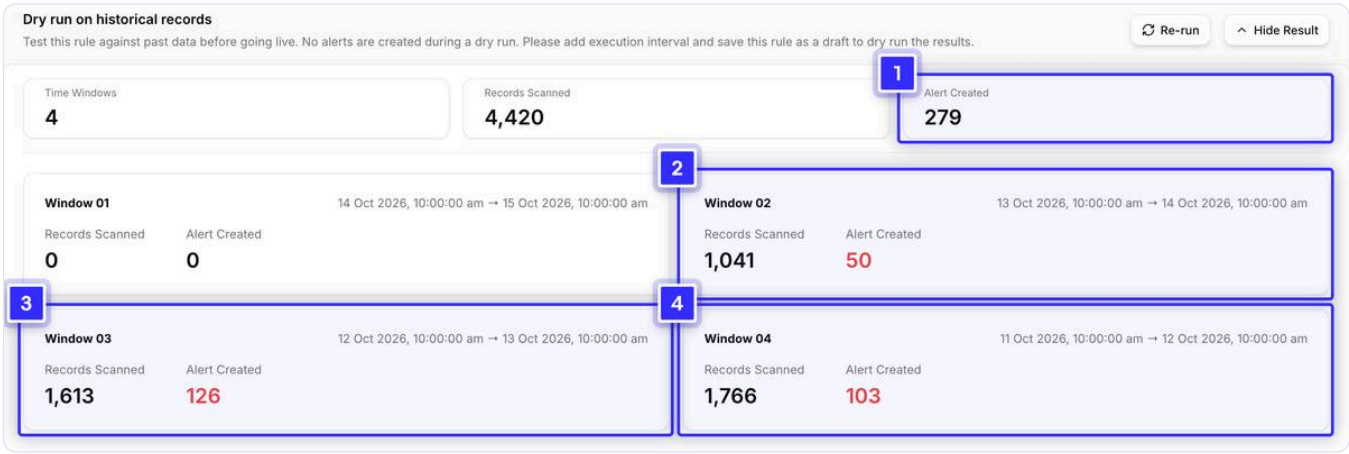


Figure 9.92 Rule 4 dry run: 279 alerts (1), and the windows with 50 (2), 126 (3) and 103 (4) alerts

Tuning. You can change the length of the quiet period (100 in variable A, keeping the end at 1 so it never overlaps variable B's window), the amount that counts as reactivation (5000), the activity window (variable B's 1 to 0, with variable A's end value moved to match) and the **Suppression Window** (1 Day). Keep the multiplier at 1000000000000: it only has to be larger than any amount a sender could send in a day. A shorter quiet period or a lower amount raises more alerts. Confirm the result with a **Dry Run**.

Rule 5 · Fan-out

RED FLAG **One sender paying many receivers**

LOGIC

Counts the different receivers the sender paid in the last 7 days.

WINDOW

7 to 0 Days

THRESHOLD

≥ 10 receivers

✓ Verified · 240 alerts

What it detects and why. One sender pays 10 or more different receivers within 7 days, for example ₱3,000 to each of twelve new accounts. Spreading funds across many receivers is a common way to move money onward quickly or to hide who finally receives it.

Item	Setting
Variable `distinct_receivers_7d`	The number of different receivers (**Count Distinct** of `receiver_entity_id`) each sender paid in the last 7 days (**Group by** `sender_entity_id`, from 7 to 0 Days ago). No filters.
Typology type	Cardinality (C-01)
Suppression Window	7 Day
Condition	`distinct_receivers_7d` **Greater Than Equal (>=)** 10
Schedule	Existing `schedule_2027` (created in Rule 1): every 1 Day, starting 09 Oct 2026, 09:00 AM, no end time

Note

The screenshots show the example objects with a *GUIDE EXAMPLE* / `guide_example_` prefix so they are easy to find on the test system. The text gives the values without the prefix. Use your own names. For a full description of each screen, see Build a typology from scratch.

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 1 **Open Create Variables and name the variable**

Go to **Transaction Monitoring → Variables** and click **+ New** (the empty form is shown in Part 2 of the walkthrough). Leave **Transaction** selected (1): the variable is calculated from transactions. In **Variable name** (2) type `distinct_receivers_7d`. In **Description** (3) type a note such as "Number of distinct receivers per sender in the last 7 days." The description appears on the variable card of every typology that uses the variable.



Figure 9.93 Transaction selected, Variable name distinct_receivers_7d and Description filled in

Step 2 **Choose the Field**

Open **Field** and type `receiver_entity` in **Search Fields**. Choose `receiver_entity_id`. This is the value the variable counts: the ID of the customer who received each transaction.

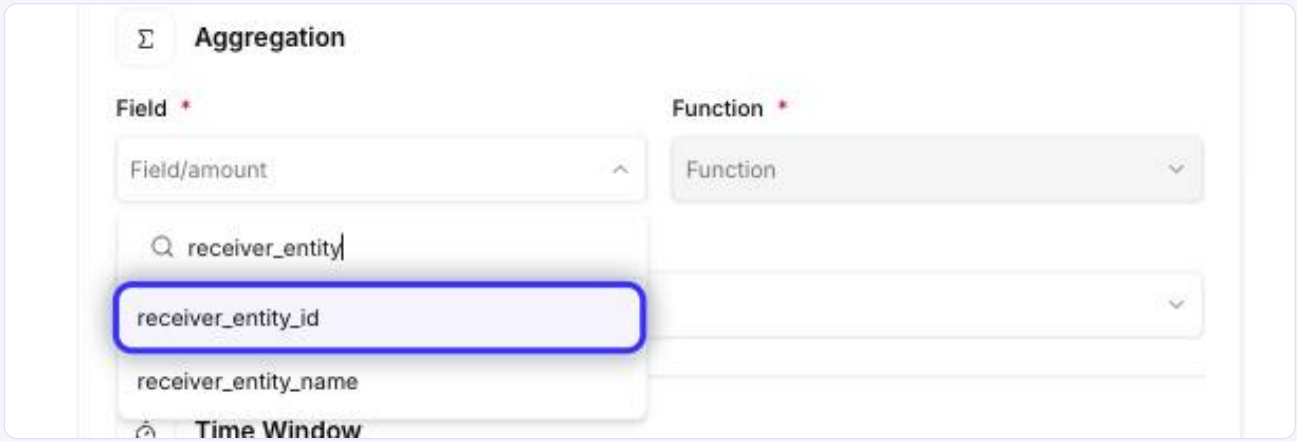


Figure 9.94 The Field list searched for receiver_entity: choose receiver_entity_id

Step 3 **Choose the Function**

Open **Function**. For `receiver_entity_id` the list offers **Count**, **Count Distinct**, **Minimum** and **Maximum** only (text and ID fields have no **Sum** or **Average**). Choose **Count Distinct**. **Count Distinct** counts each receiver once, so ten payments to the same receiver count as 1. **Count** would count transactions instead.

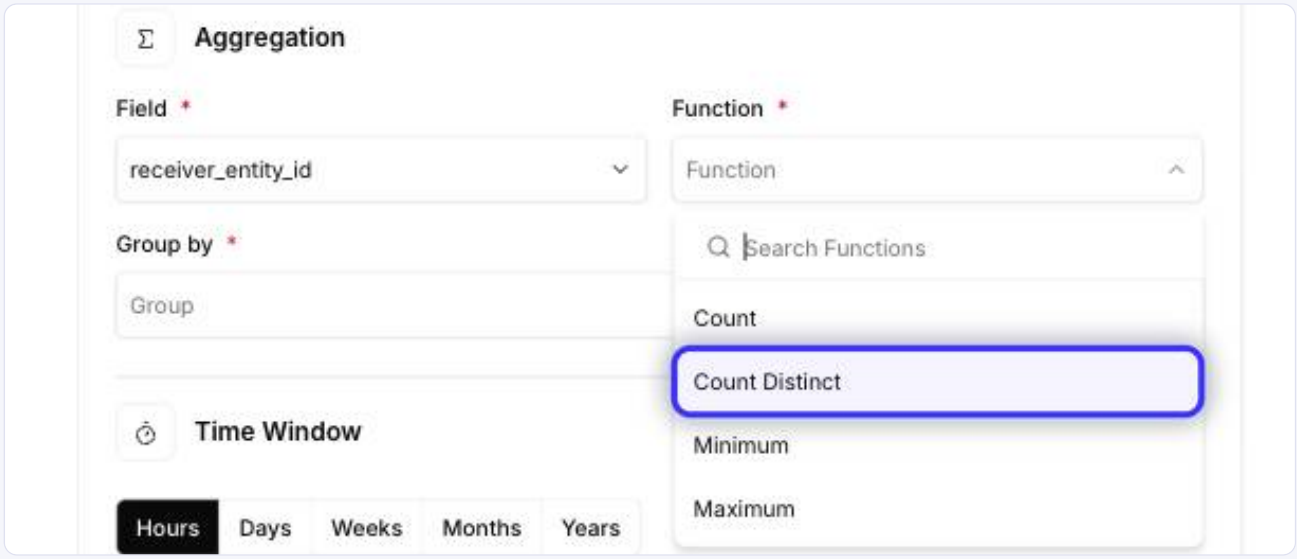


Figure 9.95 The Function list for receiver_entity_id: choose Count Distinct

Step 4 **Choose Group by**

Open **Group by** and type `sender_entity` in the search box. Choose `sender_entity_id`. The count is calculated separately for each sender, so the rule can flag the sender who fans out.



Figure 9.96 Group by searched for sender_entity: choose sender_entity_id

Step 5 **Set the time window and check the form**

Scroll down to **Time Window**. Click **Days** (1); the default is **Hours**. In **Analyze Transaction from** enter **7** and in **to** enter **0** (2). The line reads “from 7 to 0 Days ago”: the last 7 days up to the trigger time T. Leave the blank filter row under **Filters (1)** (3) empty, so every transaction counts; a blank row is not saved. Click **Save Variable** (4).

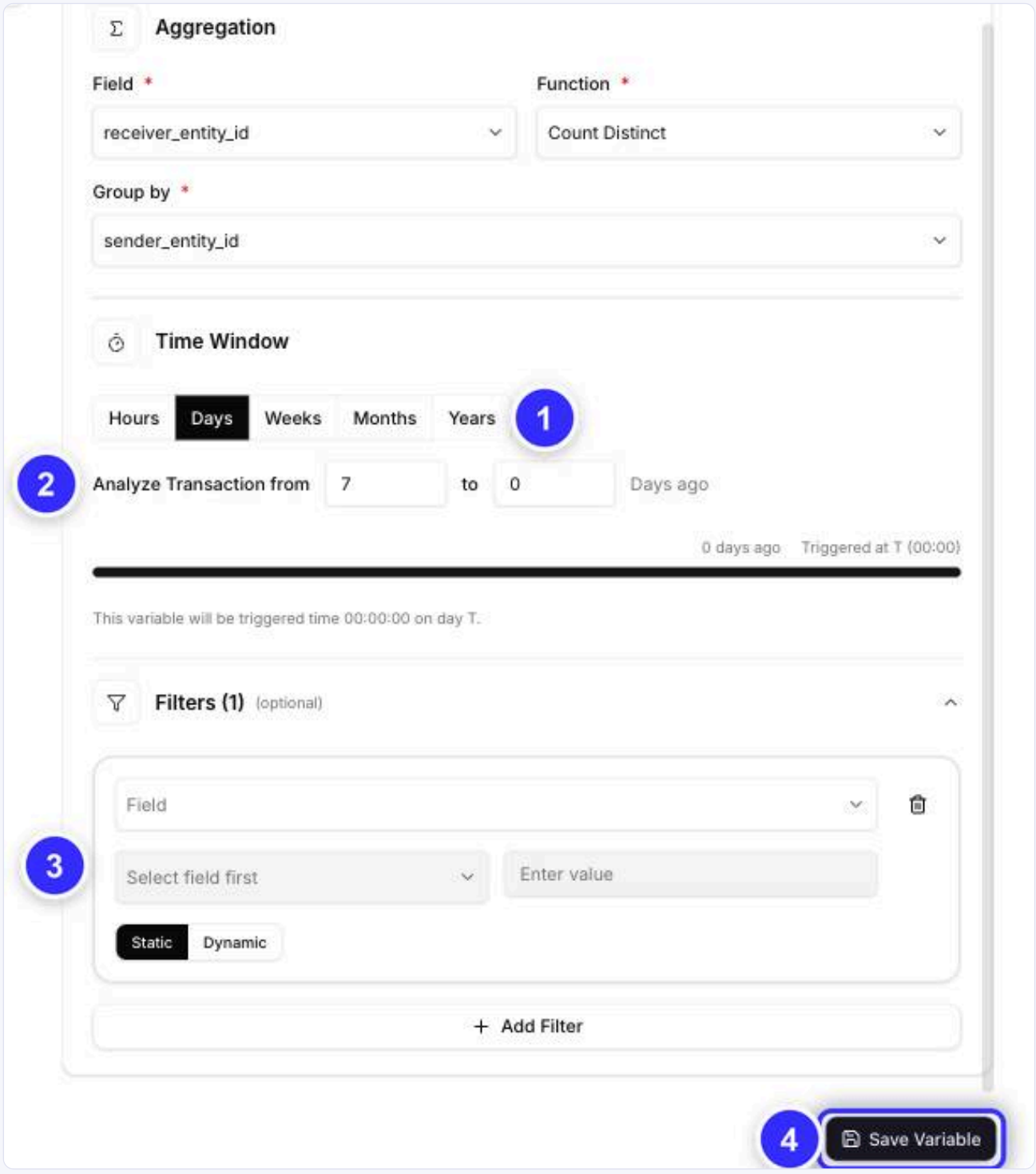


Figure 9.97 Time Window Days, from 7 to 0 Days ago, the blank filter row and Save Variable

Step 6 **Find the saved variable**

The dialog closes. The new variable is the first row of the **Variables** list, with its Variable ID (VAR-08102026-000774 in the example) and its created time.

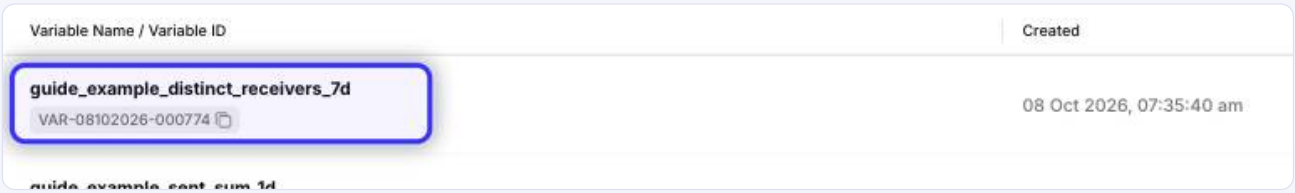


Figure 9.98 The new variable distinct_receivers_7d at the top of the Variables list

Step 7 **Check the View Variable page**

Click the row to open **View Variable**. Check the type tag (1), **STR_AGG_COUNT_DISTINCT**; the **CREATED** and **UPDATED** lines (2), with the date and time and the user who saved it; **Field**, **Function** and **Group by** (3): `receiver_entity_id` , **Count Distinct**, `sender_entity_id` ; the window (4), 7 to 0 **Days** ago; and the filters heading (5). Close the dialog with ×.

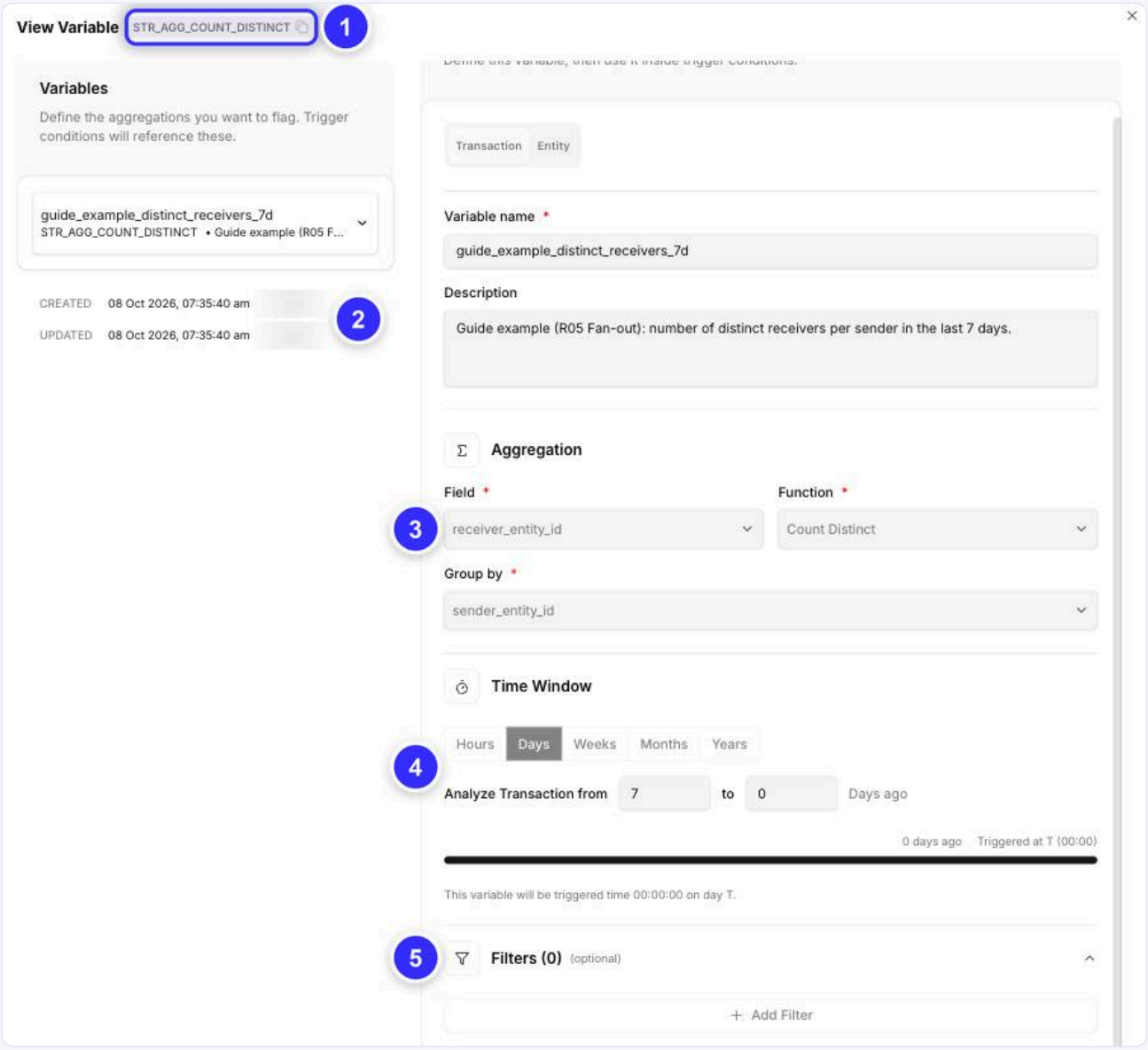


Figure 9.99 View Variable for distinct_receivers_7d: type STR_AGG_COUNT_DISTINCT, receiver_entity_id / Count Distinct / sender_entity_id

Fyscal ARCX → Transaction Monitoring → Typology → + New

Step 8 **Open Create Typology, name the rule and choose the type**

Go to **Transaction Monitoring → Typology** and click **+ New**. In **Typology Name** (1) type **R05 Fan-out - one sender to 10 or more receivers in 7 days** (letters, digits, spaces, hyphens, underscores and parentheses only). In **Suppression Window** (2) type **7** and choose **Day**. Type the description in **Description** (3). Open **Typology type**, type `Cardin` in **Search typology type** and click **Cardinality** (C-01).



Figure 9.100 Name, Suppression Window 7 Day and description entered; Typology type searched for Cardin

Step 9 **Check the details card**

The type shows as a chip, **Cardinality (C-01)**, with × to remove it. **Typology type** is a multi-select: after you pick a type the list stays open, hides the type you chose and shows “No typologies found” for the same search. Click anywhere outside the list to close it. A suitable description is “Flags a sender who pays 10 or more distinct receivers in 7 days.”



Figure 9.101 The Cardinality (C-01) chip in Typology type

Step 10 **Choose the variable in row 1**

Below the card, **Combine groups with** is **AND** and Group 1 has **Match AND**; one condition needs no change. In Group 1 click **Select field** next to **WHEN**, type part of the name, for example `distinct`, and click `distinct_receivers_7d`.

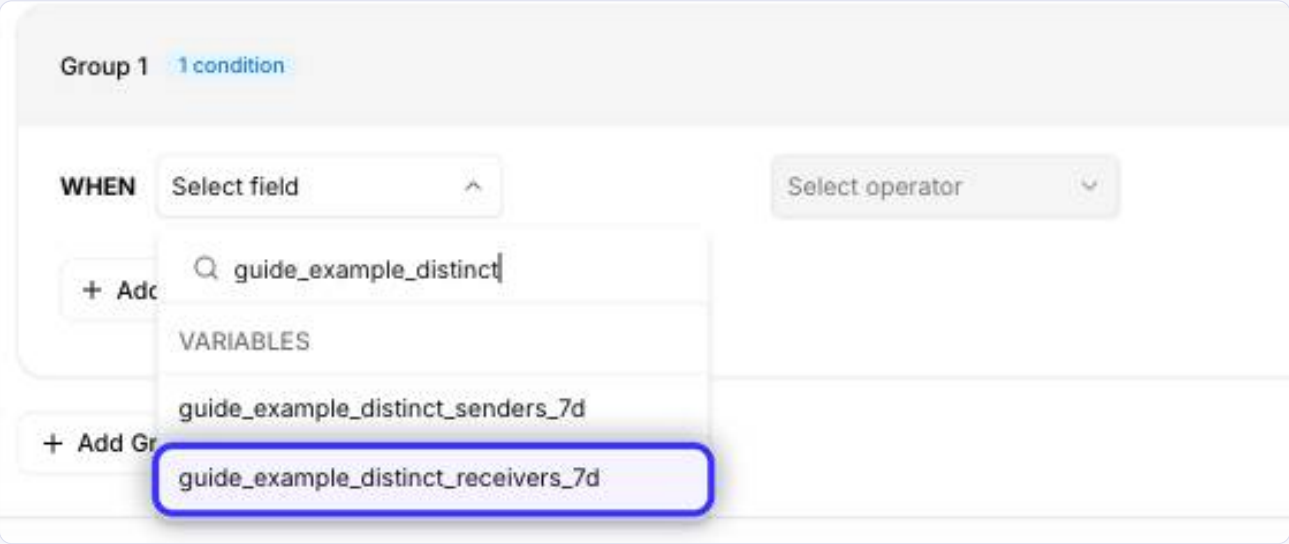


Figure 9.102 The Select field list searched by name: both distinct-count variables

Step 11 **Choose the operator**

Open **Select operator** and choose **Greater Than Equal**. The row shows it as “Greater Than Equal (>...”. **Greater Than Equal** includes the threshold itself in the alert. The full operator list is in Part 4 of the walkthrough.

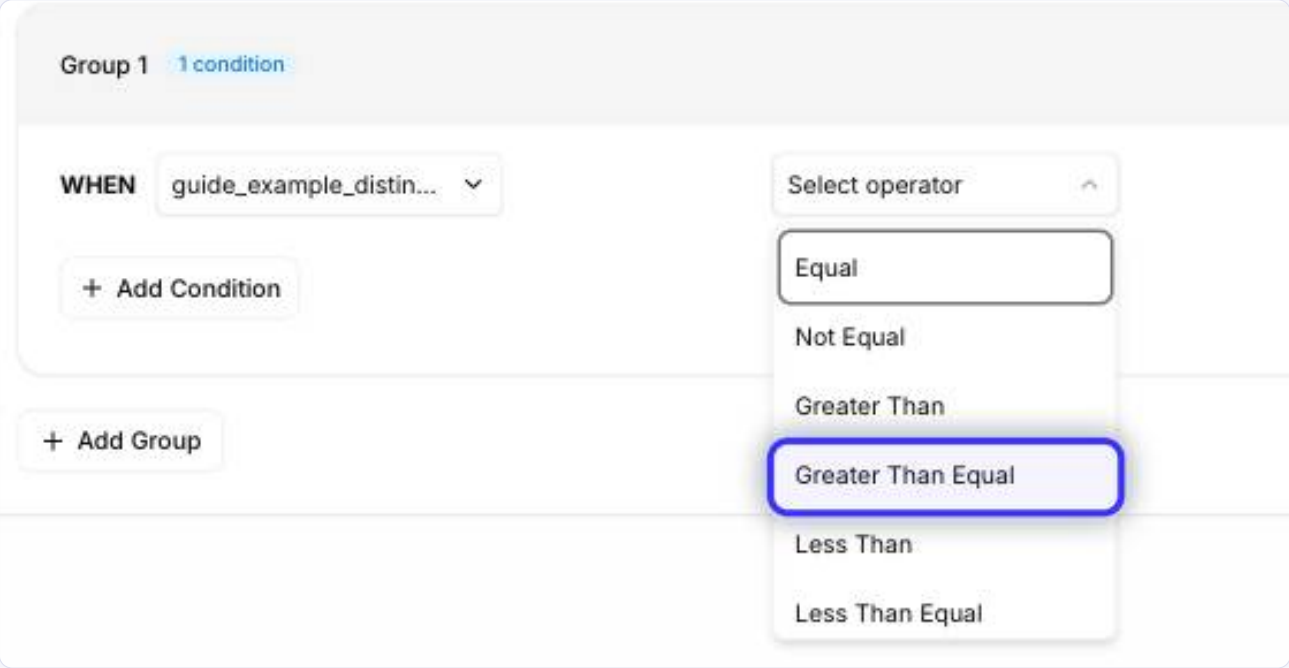


Figure 9.103 The operator list: choose Greater Than Equal

Step 12 **Keep Static Value and enter the threshold**

Open the compare-to list: **Static Value**, **Variable**, and **Ingested Data** greyed out. Keep **Static Value**, because the threshold is a fixed number, and type **10** in **Enter value**. A sender with 10 or more different receivers in the window meets the condition.

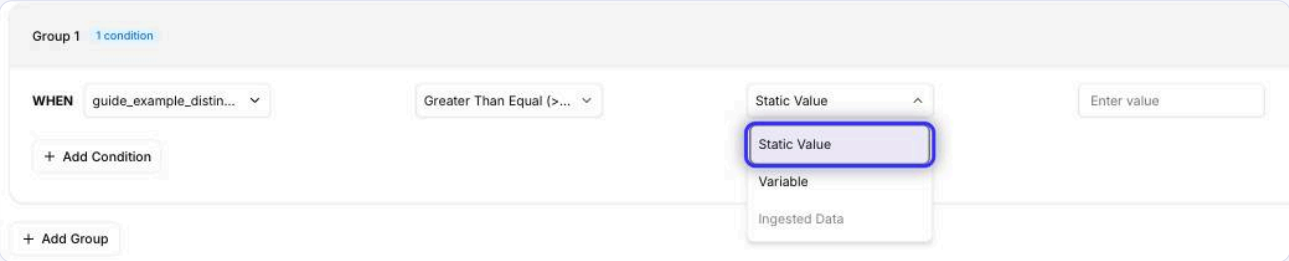


Figure 9.104 The compare-to list: Static Value, Variable, Ingested Data greyed out

Step 13 **Check the whole form and click Next Step**

The first page is complete: name (1), type chip (2), **Suppression Window** (3), description (4) and the condition (5). **Next Step** (6) is now available. Click it.

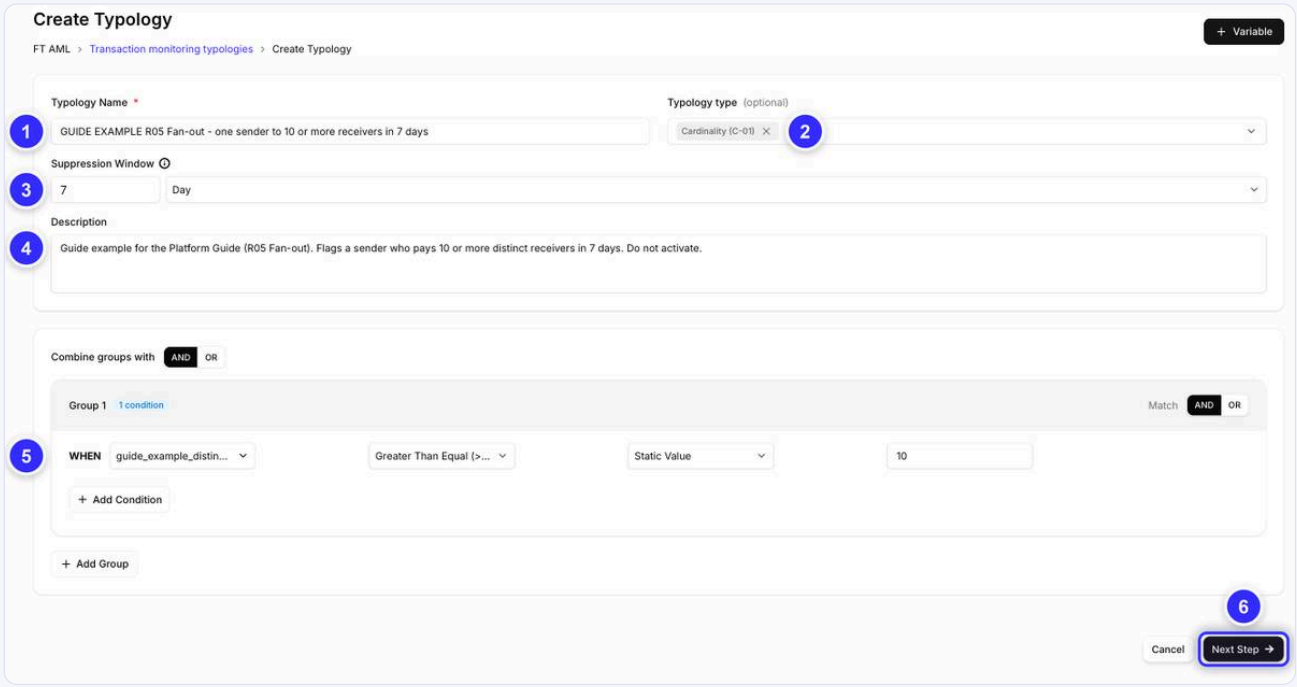


Figure 9.105 Create Typology complete: distinct_receivers_7d Greater Than Equal 10; Next Step available

Step 14 **Select the shared schedule**

Review & schedule rule opens. Open **Select Schedule**, type the schedule name in **Search Schedule** and click the schedule created in Rule 1 (`schedule_2027` , SCH-08102026-000463 in the example). One schedule can drive many rules, so every example rule reuses it.

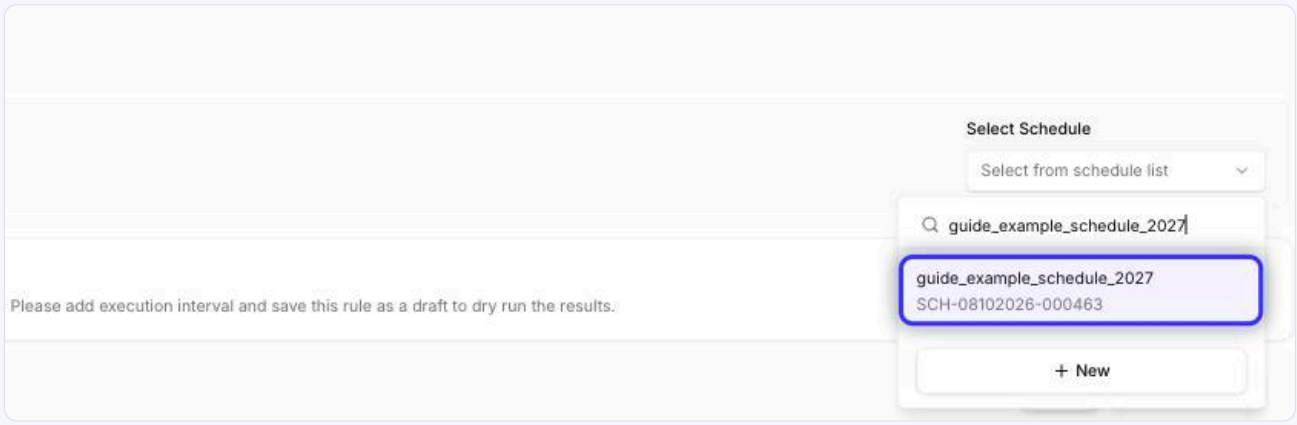


Figure 9.106 Select Schedule searched: the shared schedule and its SCH-ID

Step 15 **Check the schedule and save the draft**

The schedule shows in **Select Schedule** (1). Its fields (2) are filled from the schedule: **Execution Interval** 1 **Day**, **Start Time** 01/01/2027 09:00 AM (the start at the time of the screenshot), no **End Time**. Leave them unchanged: they belong to the shared schedule. Click **Save as Draft** (3).

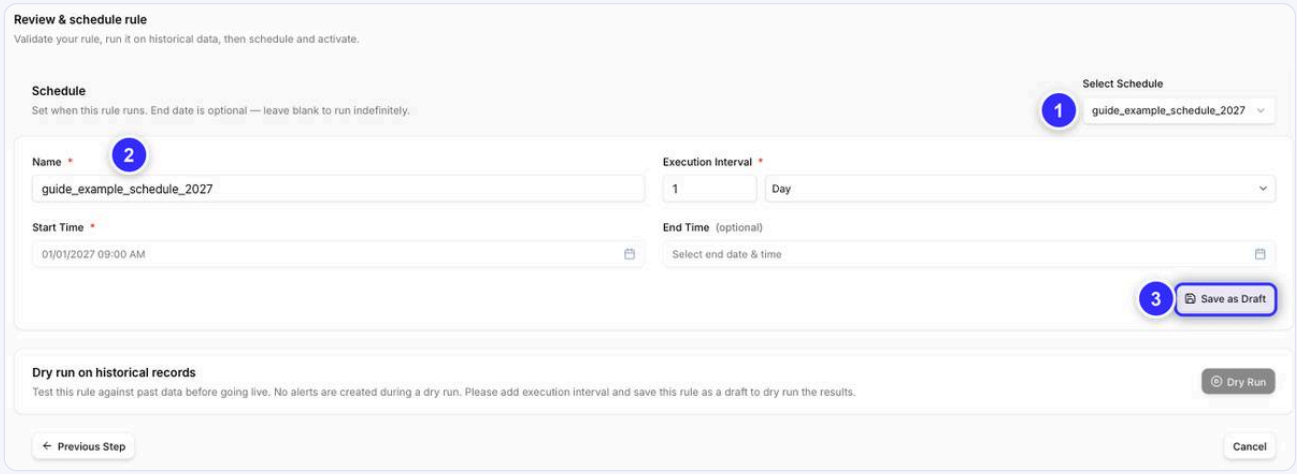


Figure 9.107 The shared schedule selected; Save as Draft available

Step 16 **Read the result**

Wait a few seconds: the page title changes to **Update Typology** (1) and the card shows “This rule will run every 1 day starting 01 Jan 2027, 09:00:00 am” (2). **Save as Draft** is replaced by **Update** (3); **Dry Run** (4) and **Activate** (5) are now available. The rule is a Draft and does not run until it is activated; to test it, see Test a typology with Dry Run.

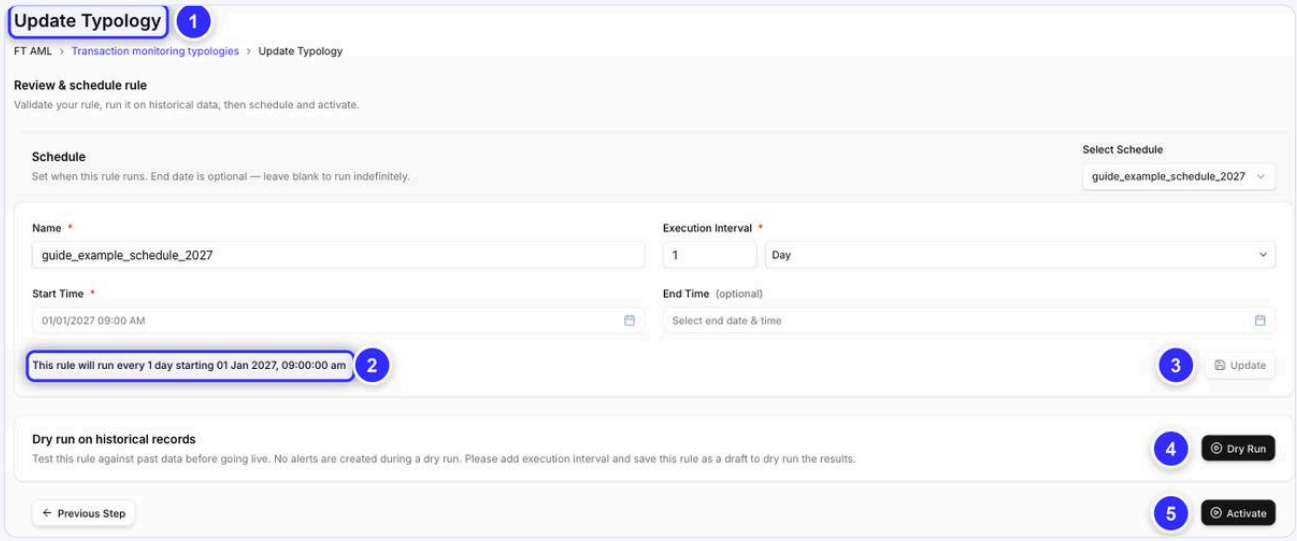


Figure 9.108 After Save as Draft: Update Typology, the run summary, Update, Dry Run and Activate

Step 17 **Check the rule page**

Open the rule from **Transaction Monitoring → Typology**. The page shows the **Draft** chip and rule ID (1), TMR-08102026-001127, created 08 Oct 2026, 11:50:20 am. The summary strip (2) reads **EXECUTION PERIOD** 01 Jan 2027, 09:00:00 am → N/A, **INTERVAL** Every 1 day, **COMPLEXITY** Advanced, **SUPPRESSION** 7Day and **TYPOLOGY** Cardinality. Group 1 (3) shows `distinct_receivers_7d` **Greater Than Equal (>=)** 10. **VARIABLES** (4) shows the variable card: Str_agg_count_distinct, **WINDOW** in last 7 day, **GROUP** `sender_entity_id`.

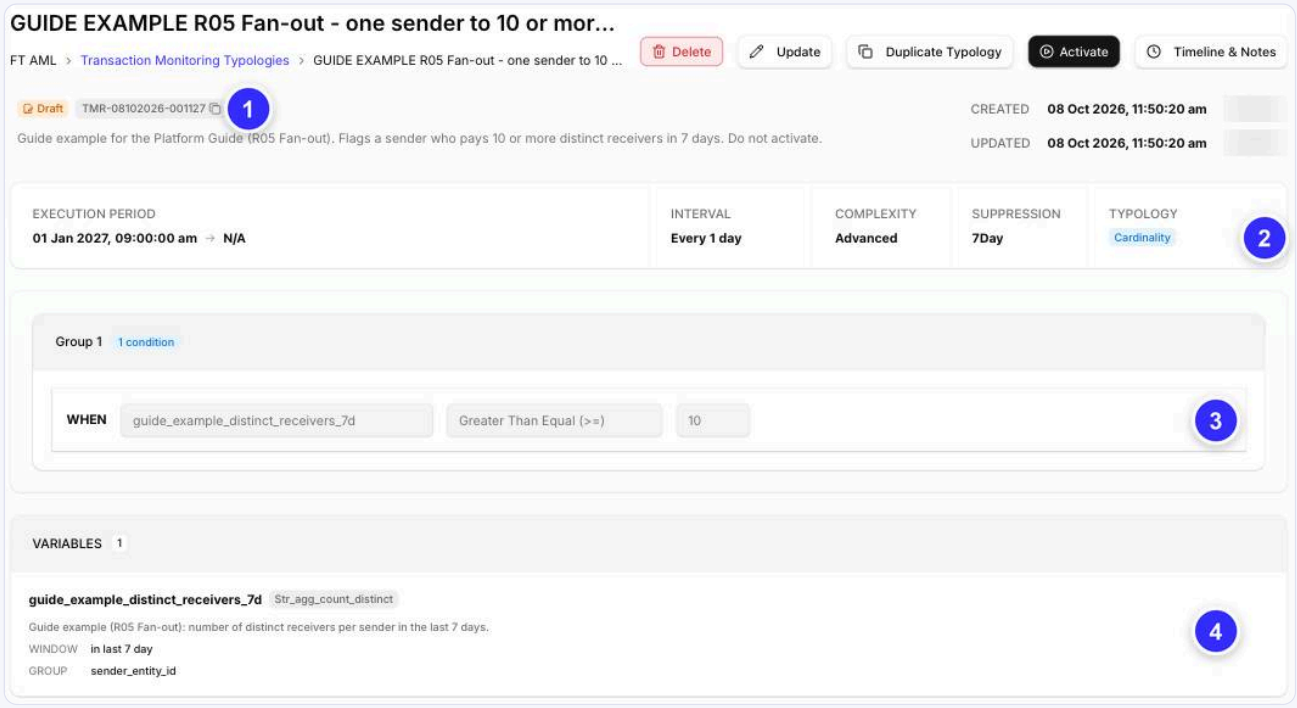


Figure 9.109 The draft rule page: TMR-08102026-001127, Draft

How it evaluates. At each run the variable counts, for each sender, the different receivers paid in the last 7 days. Example: in the 7 days before a run:

Sender	Payments in the window	distinct_receivers_7d	Result
A	12 payments of ₱3,000, each to a different receiver	12	12 >= 10: alert
B	25 payments totalling ₱75,000, all to the same 4 receivers	4	4 >= 10 is false: no alert
C	10 payments to 10 different receivers	10	10 >= 10: alert (the threshold is included)

Amounts play no part in this rule: sender B moves more money than A but pays only 4 receivers.

Dry-run result. In testing, the rule created 240 alerts at its real threshold, 60 in each of the four windows.

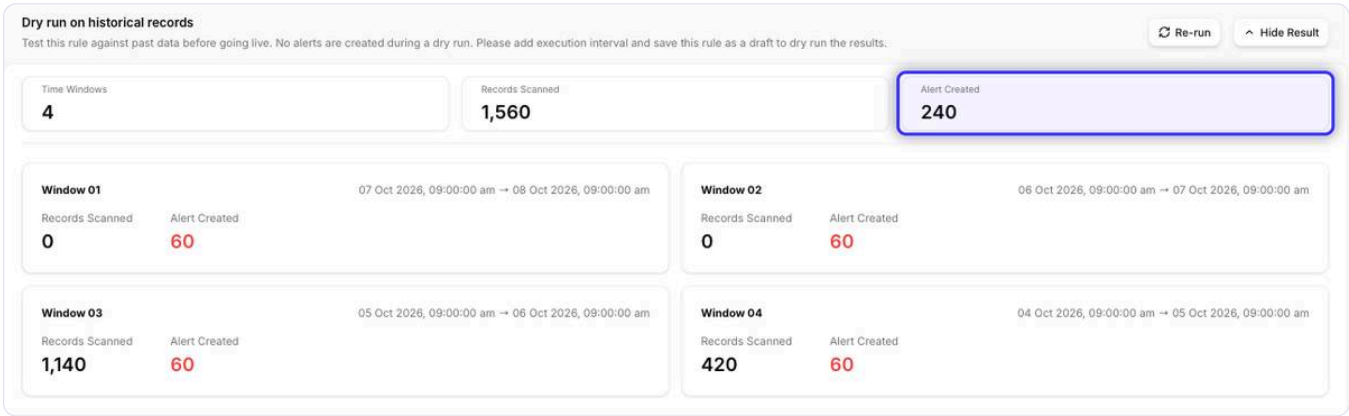


Figure 9.110 Rule 5 dry run at >= 10: 240 alerts

Tuning. Choose the threshold (10) to suit how many receivers your customers normally pay: a remittance business that pays many beneficiaries may need a higher number, and a retail book a lower one. Choose the window (7 Days in the variable) and keep **Suppression Window** the same length or longer, as in the example. To ignore very small payments, add a filter to the variable, for example `amount` **Greater Than Equal** a value you choose; filters are shown in Rule 8.

Rule 6 · Fan-in

RED FLAG **Many senders paying one receiver**

LOGIC

Counts the different senders that paid the receiver in the last 7 days.

WINDOW

7 to 0 Days

THRESHOLD

≥ 10 senders

✓ Verified · 240 alerts

What it detects and why. One receiver is paid by 10 or more different senders within 7 days, for example ₱2,000 from each of fifteen unrelated people. Collecting funds from many sources into one account is typical of money-mule and pooling accounts.

Item	Setting
Variable `distinct_senders_7d`	The number of different senders (**Count Distinct** of `sender_entity_id`) that paid each receiver in the last 7 days (**Group by** `receiver_entity_id`, from 7 to 0 Days ago). No filters.
Typology type	Cardinality (C-01)
Suppression Window	7 Day
Condition	`distinct_senders_7d` **Greater Than Equal (>=)** 10
Schedule	Existing `schedule_2027` (created in Rule 1): every 1 Day, starting 09 Oct 2026, 09:00 AM, no end time

This rule is the mirror of Rule 5: the counted field and the **Group by** field swap places. For a full description of each screen, see Build a typology from scratch.

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 1 **Open Create Variables and name the variable**

Go to **Transaction Monitoring → Variables** and click **+ New** (the empty form is shown in Part 2 of the walkthrough). Leave **Transaction** selected (1): the variable is calculated from transactions. In **Variable name** (2) type `distinct_senders_7d`. In **Description** (3) type a note such as “Number of distinct senders per receiver in the last 7 days.” The description appears on the variable card of every typology that uses the variable.



Figure 9.111 Transaction selected, Variable name distinct_senders_7d and Description filled in

Step 2 **Choose the Field**

Open **Field** and type `sender_entity` in **Search Fields**. Choose `sender_entity_id`. This is the value the variable counts: the ID of the customer who sent each transaction.

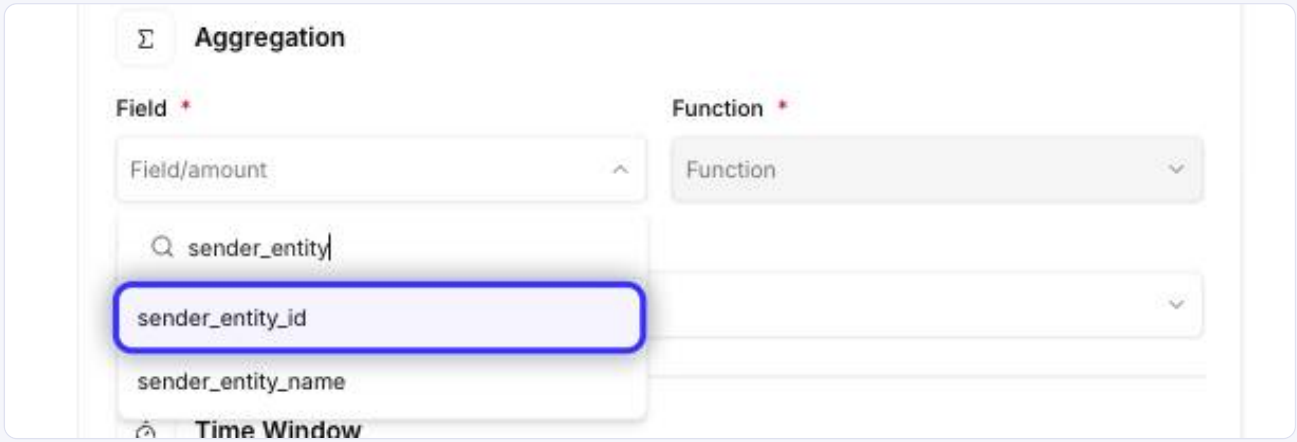


Figure 9.112 The Field list searched for sender_entity: choose sender_entity_id

Step 3 **Choose the Function**

Open **Function**. For `sender_entity_id` the list offers **Count**, **Count Distinct**, **Minimum** and **Maximum** only. Choose **Count Distinct**. Each sender is counted once, however many times they paid the receiver.

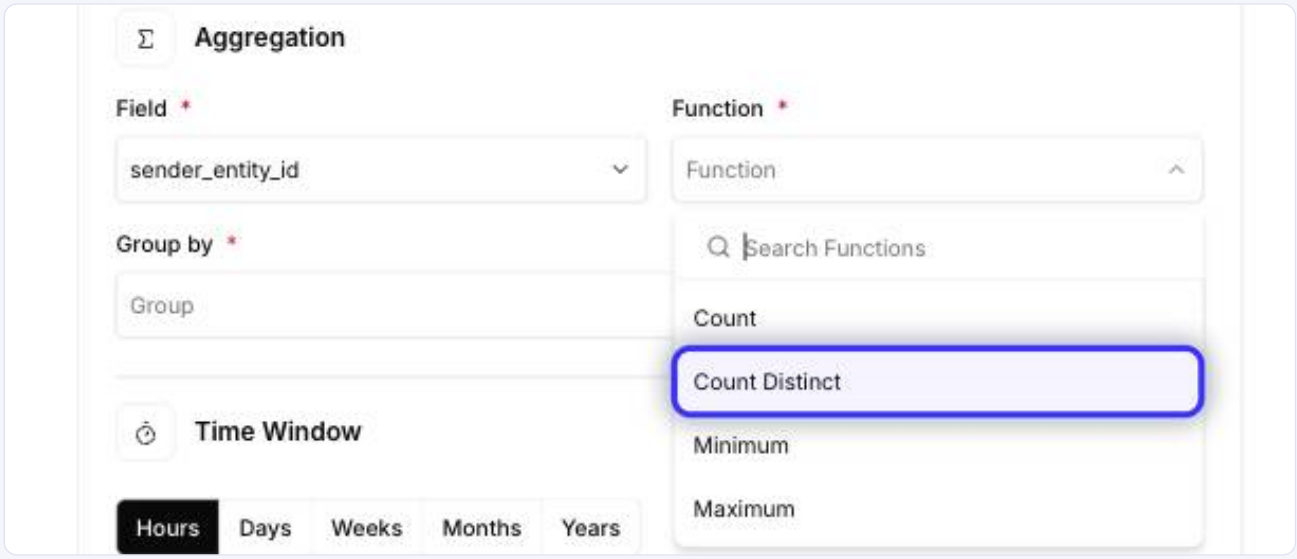


Figure 9.113 The Function list for sender_entity_id: choose Count Distinct

Step 4 **Choose Group by**

Open **Group by** and type `receiver_entity` in the search box. Choose `receiver_entity_id`. The count is calculated separately for each receiver, so the rule flags the receiving customer.



Figure 9.114 Group by searched for receiver_entity: choose receiver_entity_id

Step 5 **Set the time window and check the form**

Scroll down to **Time Window**. Click **Days** (1); the default is **Hours**. In **Analyze Transaction from** enter **7** and in **to** enter **0** (2). The line reads “from 7 to 0 Days ago”: the last 7 days up to the trigger time T. Leave the blank filter row under **Filters (1)** (3) empty, so every transaction counts; a blank row is not saved. Click **Save Variable** (4).

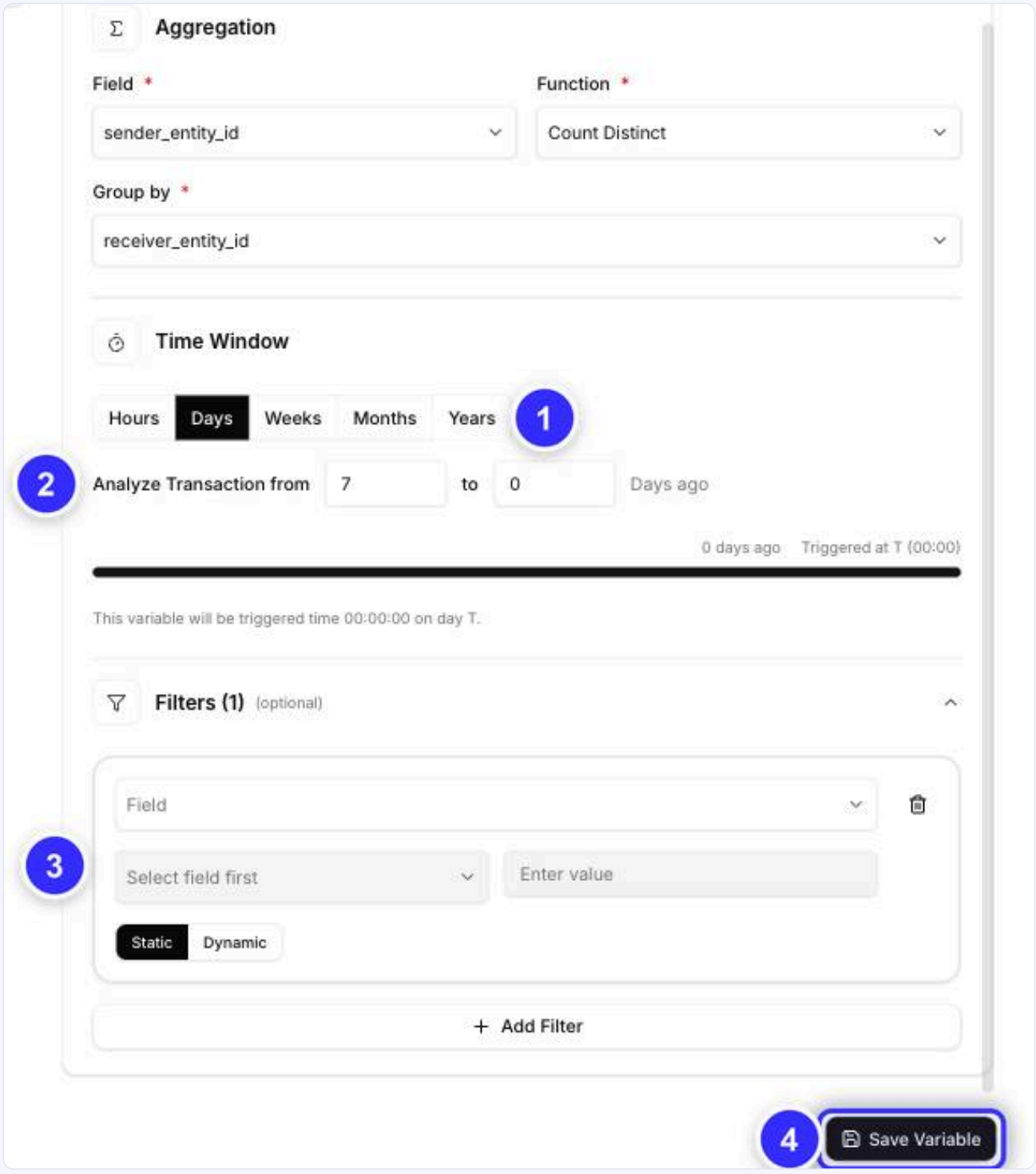


Figure 9.115 Time Window Days, from 7 to 0 Days ago, the blank filter row and Save Variable

Step 6 **Find the saved variable**

The dialog closes. The new variable is the first row of the **Variables** list, with its Variable ID (VAR-08102026-000775 in the example) and its created time.

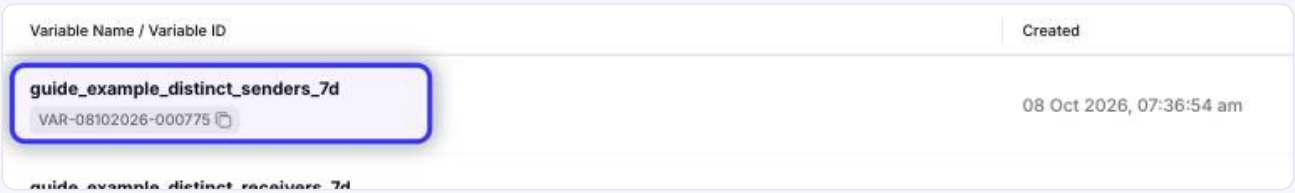


Figure 9.116 The new variable distinct_senders_7d at the top of the Variables list

Step 7 **Check the View Variable page**

Click the row to open **View Variable**. Check the type tag (1), **STR_AGG_COUNT_DISTINCT**; the **CREATED** and **UPDATED** lines (2), with the date and time and the user who saved it; **Field**, **Function** and **Group by** (3): `sender_entity_id` , **Count Distinct**, `receiver_entity_id` ; the window (4), 7 to 0 **Days** ago; and the filters heading (5). Close the dialog with ×.

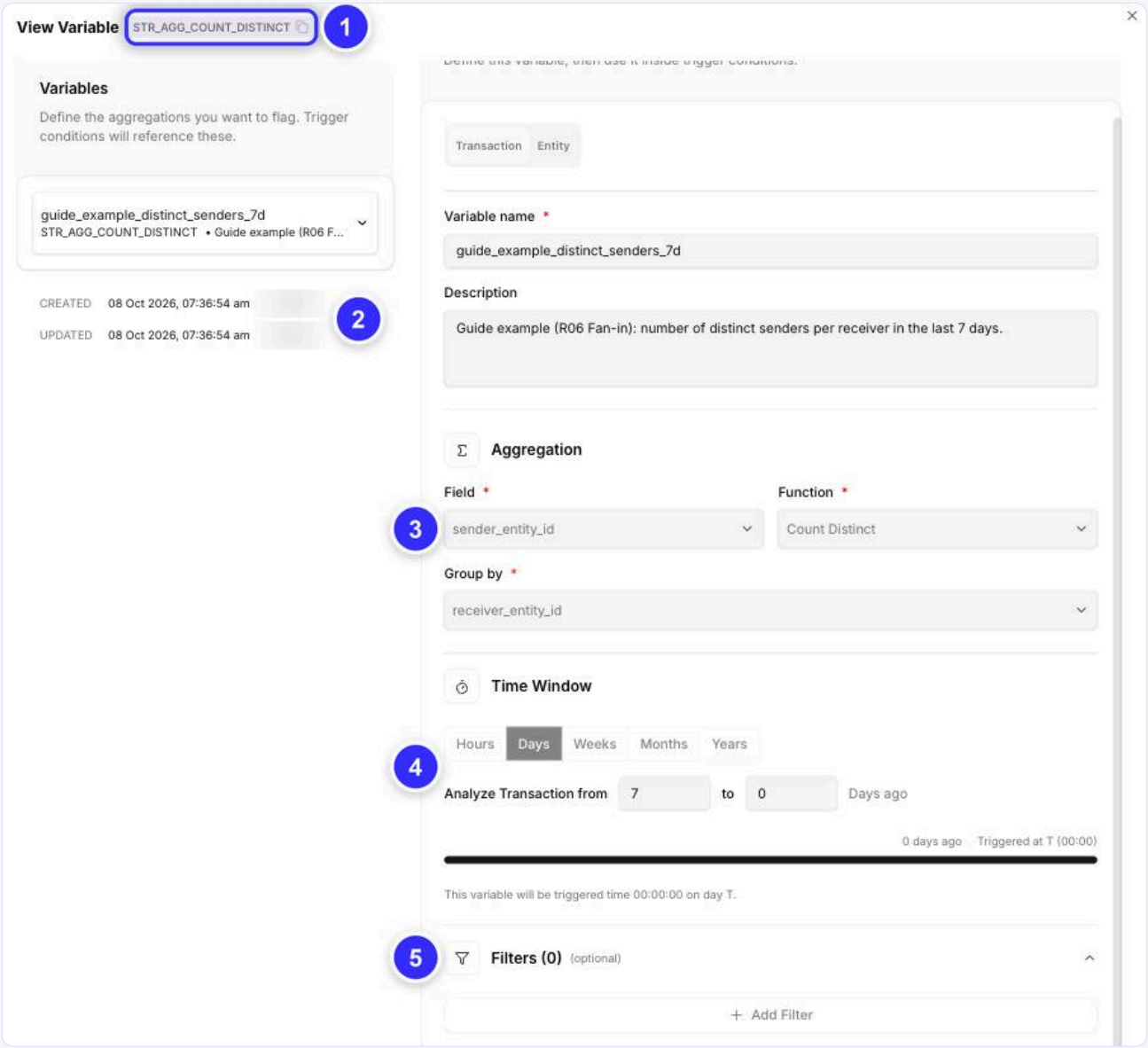


Figure 9.117 View Variable for distinct_senders_7d: type STR_AGG_COUNT_DISTINCT, sender_entity_id / Count Distinct / receiver_entity_id

Fyscal ARCX → Transaction Monitoring → Typology → + New

Step 8 **Open Create Typology, name the rule and choose the type**

Go to **Transaction Monitoring → Typology** and click **+ New**. In **Typology Name** (1) type **R06 Fan-in - 10 or more senders to one receiver in 7 days** (letters, digits, spaces, hyphens, underscores and parentheses only). In **Suppression Window** (2) type **7** and choose **Day**. Type the description in **Description** (3). Open **Typology type**, type `Cardin` in **Search typology type** and click **Cardinality** (C-01).



Figure 9.118 Name, Suppression Window 7 Day and description entered; Typology type searched for Cardin

Step 9 **Check the details card**

The type shows as a chip, **Cardinality (C-01)**, with × to remove it. **Typology type** is a multi-select: after you pick a type the list stays open, hides the type you chose and shows “No typologies found” for the same search. Click anywhere outside the list to close it. A suitable description is “Flags a receiver paid by 10 or more distinct senders in 7 days.”



Figure 9.119 The Cardinality (C-01) chip in Typology type

Step 10 **Choose the variable in row 1**

Below the card, **Combine groups with** is **AND** and Group 1 has **Match AND**; one condition needs no change. In Group 1 click **Select field** next to **WHEN**, type part of the name, for example `distinct`, and click `distinct_senders_7d`.

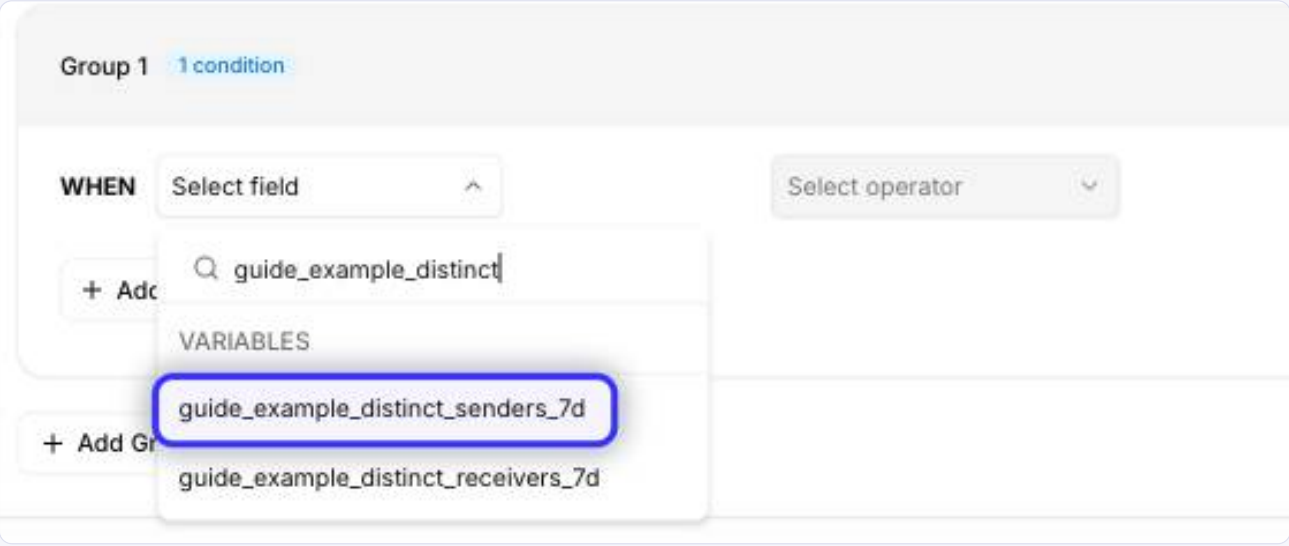


Figure 9.120 The Select field list searched by name: both distinct-count variables

Step 11 **Choose the operator**

Open **Select operator** and choose **Greater Than Equal**. The row shows it as “Greater Than Equal (>...”. **Greater Than Equal** includes the threshold itself in the alert. The full operator list is in Part 4 of the walkthrough.

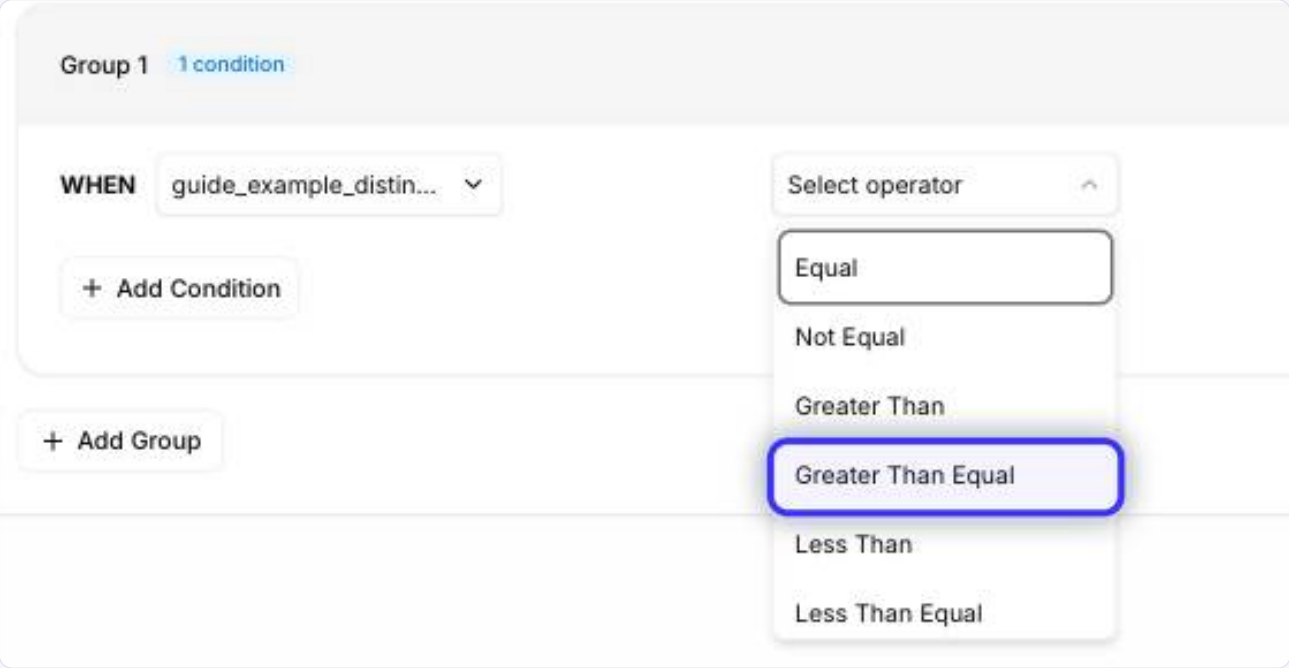


Figure 9.121 The operator list: choose Greater Than Equal

Step 12 **Keep Static Value and enter the threshold**

Open the compare-to list: **Static Value**, **Variable**, and **Ingested Data** greyed out. Keep **Static Value**, because the threshold is a fixed number, and type **10** in **Enter value**. A receiver paid by 10 or more different senders in the window meets the condition.

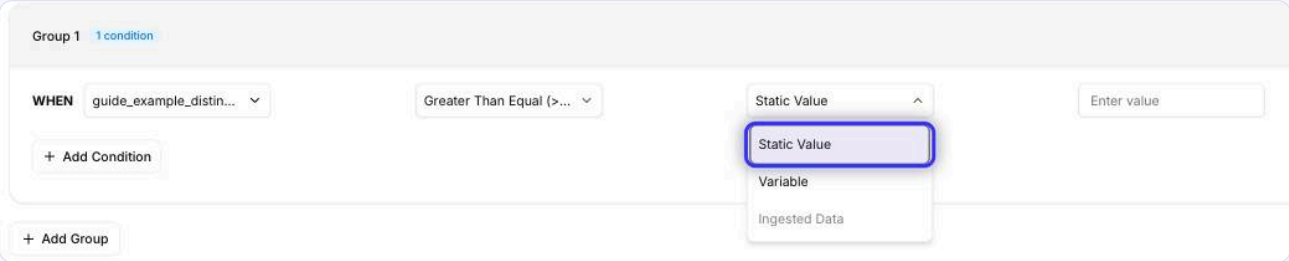


Figure 9.122 The compare-to list: Static Value, Variable, Ingested Data greyed out

Step 13 **Check the whole form and click Next Step**

The first page is complete: name (1), type chip (2), **Suppression Window** (3), description (4) and the condition (5). **Next Step** (6) is now available. Click it.

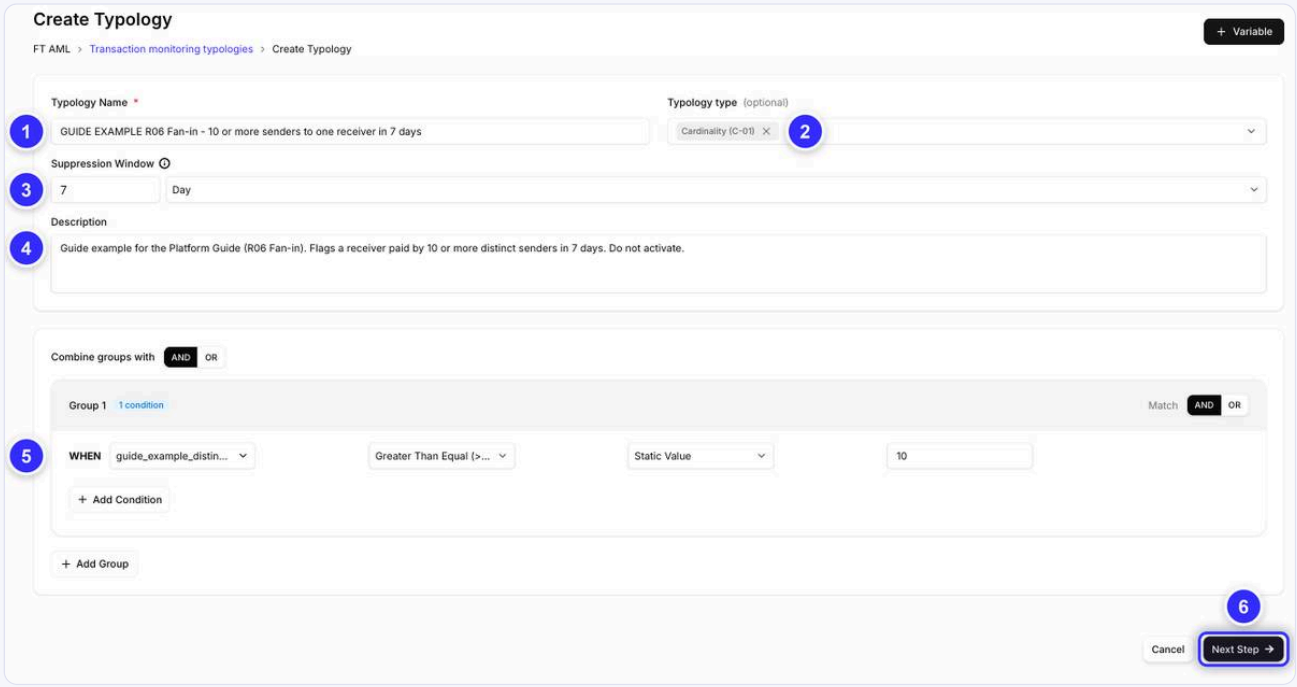


Figure 9.123 Create Typology complete: distinct_senders_7d Greater Than Equal 10; Next Step available

Step 14 **Select the shared schedule**

Review & schedule rule opens. Open **Select Schedule**, type the schedule name in **Search Schedule** and click the schedule created in Rule 1 (`schedule_2027` , SCH-08102026-000463 in the example). One schedule can drive many rules, so every example rule reuses it.

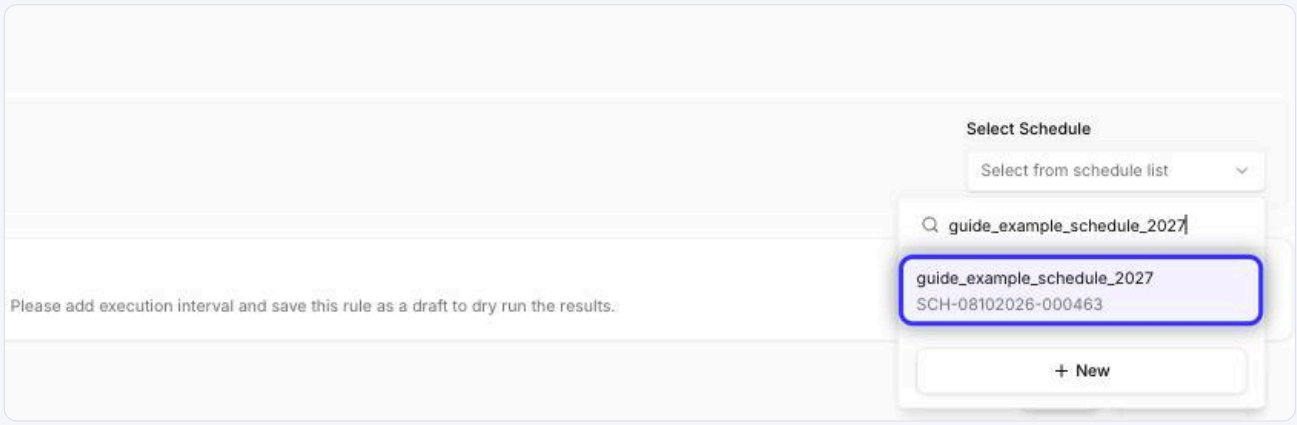


Figure 9.124 Select Schedule searched: the shared schedule and its SCH-ID

Step 15 **Check the schedule and save the draft**

The schedule shows in **Select Schedule** (1). Its fields (2) are filled from the schedule: **Execution Interval** 1 **Day**, **Start Time** 01/01/2027 09:00 AM (the start at the time of the screenshot), no **End Time**. Leave them unchanged: they belong to the shared schedule. Click **Save as Draft** (3).

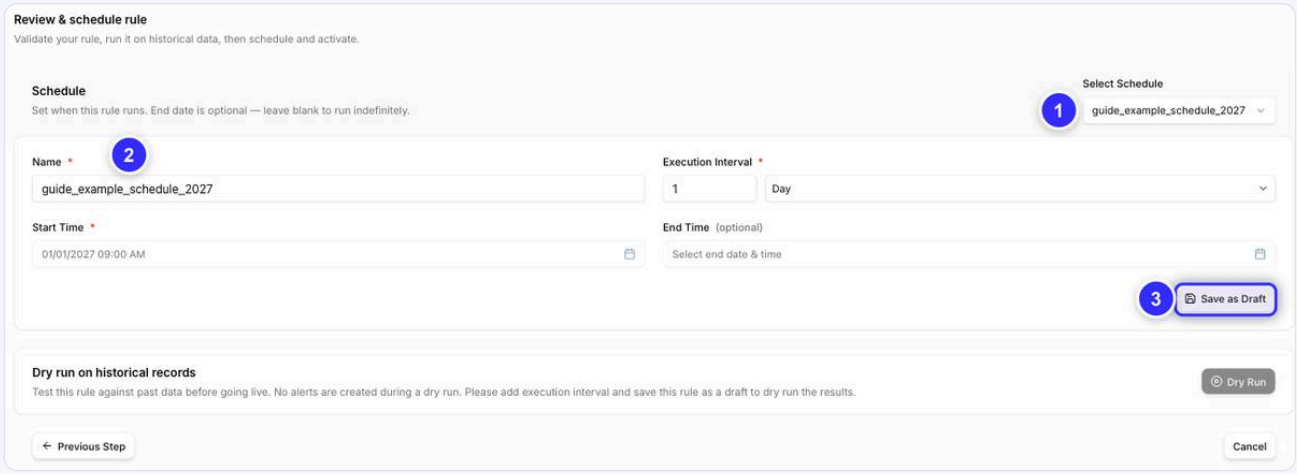


Figure 9.125 The shared schedule selected; Save as Draft available

Step 16 **Read the result**

Wait a few seconds: the page title changes to **Update Typology** (1) and the card shows “This rule will run every 1 day starting 01 Jan 2027, 09:00:00 am” (2). **Save as Draft** is replaced by **Update** (3); **Dry Run** (4) and **Activate** (5) are now available. The rule is a Draft and does not run until it is activated; to test it, see Test a typology with Dry Run.

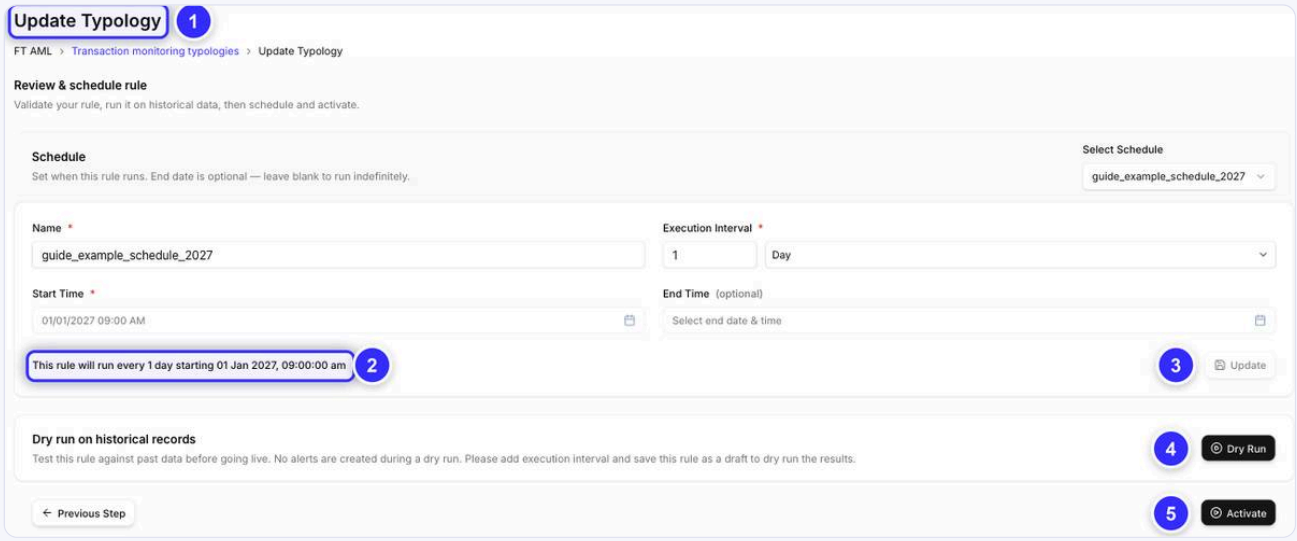


Figure 9.126 After Save as Draft: Update Typology, the run summary, Update, Dry Run and Activate

Step 17 **Check the rule page**

Open the rule from **Transaction Monitoring → Typology**. The page shows the **Draft** chip and rule ID (1), TMR-08102026-001128, created 08 Oct 2026, 11:51:57 am. The summary strip (2) reads **EXECUTION PERIOD** 01 Jan 2027, 09:00:00 am → N/A, **INTERVAL** Every 1 day, **COMPLEXITY** Advanced, **SUPPRESSION** 7Day and **TYPOLOGY** Cardinality. Group 1 (3) shows `distinct_senders_7d` **Greater Than Equal (>=)** 10. **VARIABLES** (4) shows Str_agg_count_distinct, **WINDOW** in last 7 day, **GROUP** `receiver_entity_id`.

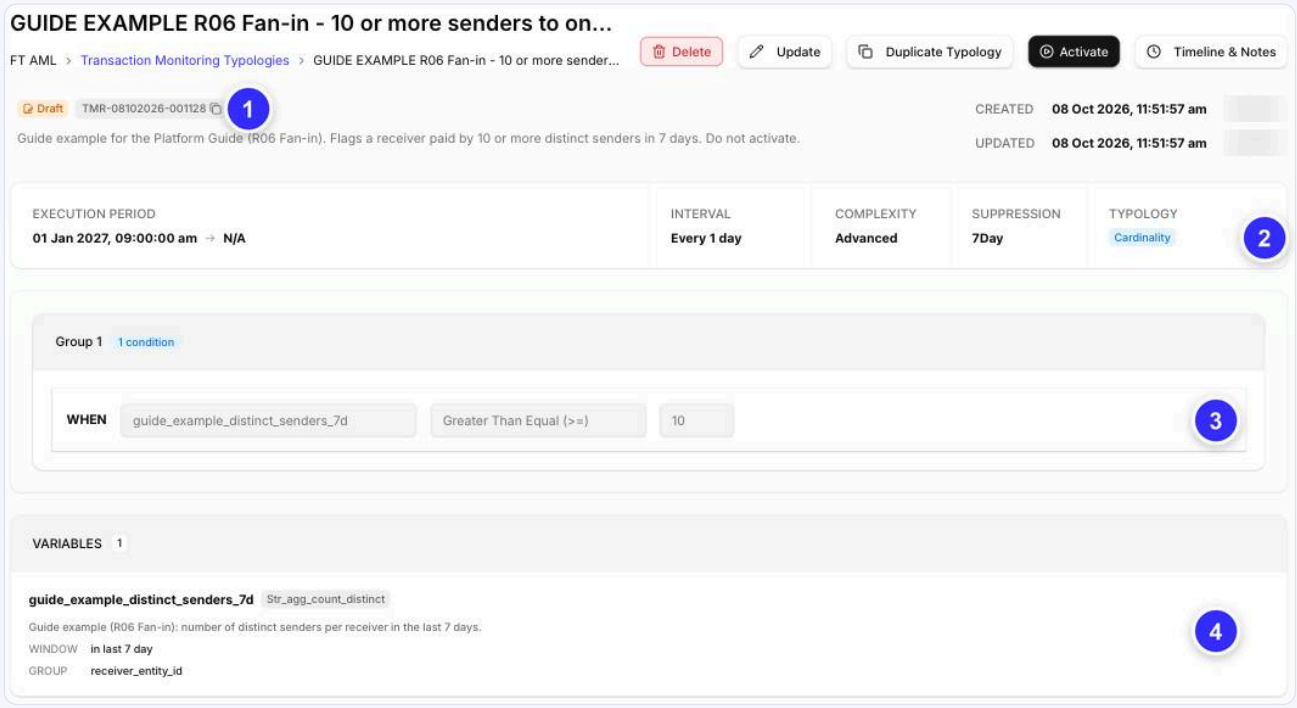


Figure 9.127 The draft rule page: TMR-08102026-001128, Draft

How it evaluates. At each run the variable counts, for each receiver, the different senders that paid it in the last 7 days.

Receiver	Payments in the window	distinct_senders_7d	Result
D	15 payments of about ₱2,000, from 15 different senders	15	15 >= 10: alert
E	A salary of ₱40,000 from one employer and 6 transfers from 3 relatives	4	4 >= 10 is false: no alert

Dry-run result. In testing, the rule created 240 alerts at its real threshold, 60 in each of the four windows.

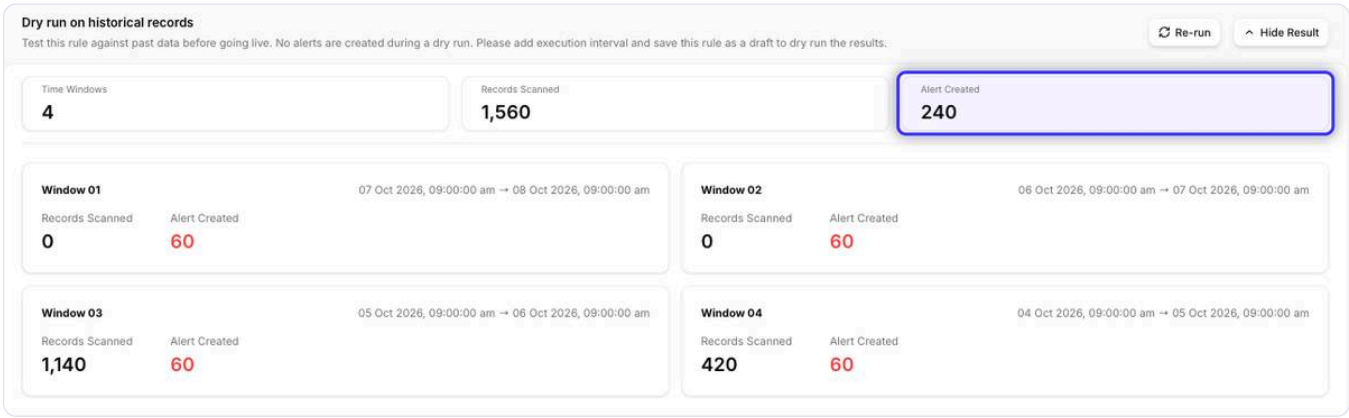


Figure 9.128 Rule 6 dry run at >= 10: 240 alerts

Tuning. Choose the threshold (10) from how many senders your receiving customers normally have; merchants, collection accounts and charities receive from many payers, so you may exclude them with a filter or use a higher number. Choose the window length and keep the suppression window at least as long. To count only payments above a size you choose, add an `amount` filter to the variable.

Rule 7 · Large single transaction

RED FLAG **One very large payment**

LOGIC

Takes the sender's largest single amount in the last day.

WINDOW

1 to 0 Days

THRESHOLD

≥ ₱1,000,000

✓ Verified by positive control

What it detects and why. This rule flags a sender who makes one transaction of ₱1,000,000 or more within a day. One very large payment is reviewed on its own, whatever else the customer does, which is why the variable takes the largest amount rather than the total (Rule 3 looks at totals).

Item	Setting
Variable `max_amount_1d`	**Maximum** of `amount`, grouped by `sender_entity_id`, **Days** from 1 to 0, no filters
Typology type	Large Transaction (LT-01)
Suppression Window	1 Day
Condition	Group 1, Match AND: `max_amount_1d` **Greater Than Equal (>=)** Static Value 1000000
Schedule	Existing `schedule_2027` (created in Rule 1): every 1 Day, starting 09 Oct 2026, 09:00 AM, no end time

Part A: Create the variable

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 1 **Open the form and name the variable**

Click **+ New** on **Variables** and leave **Transaction** selected. Type `max_amount_1d` in **Variable name** (1) and a description such as "Largest single transaction amount per sender in the last 1 day." (2).

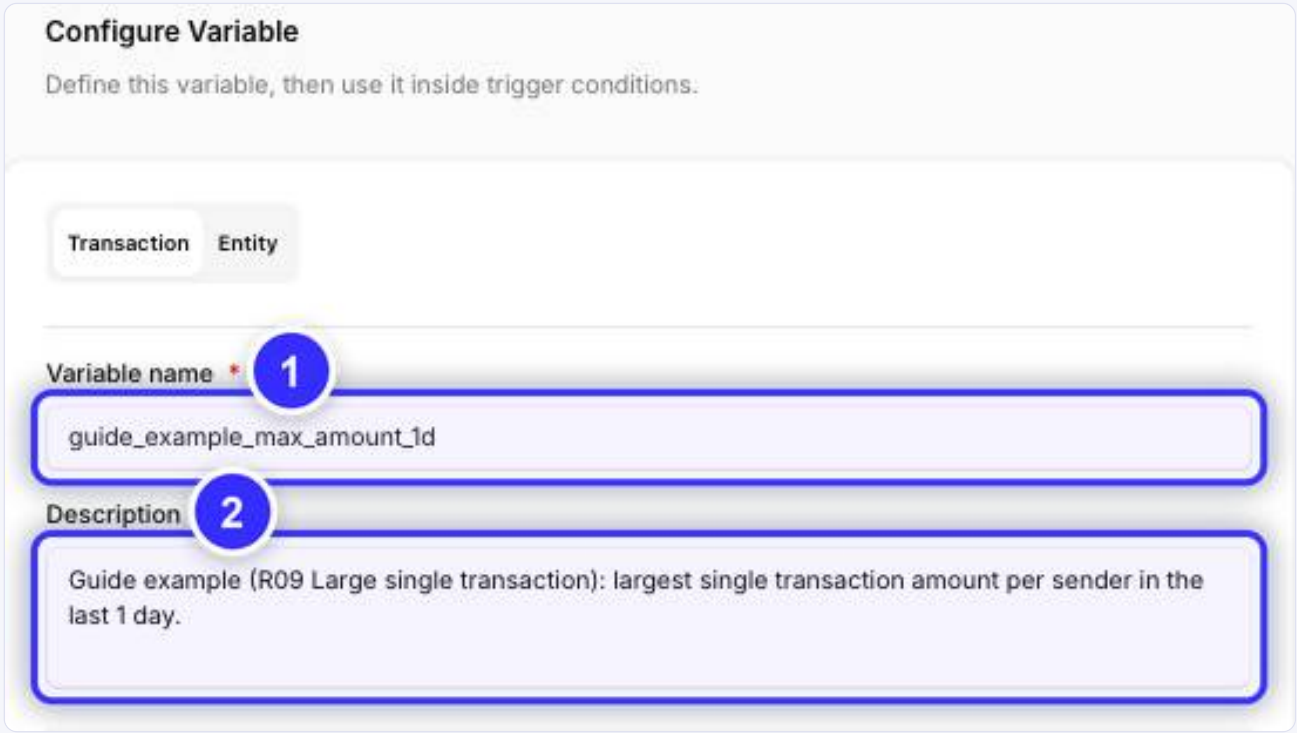


Figure 9.129 Rule 7 variable: name and description

Step 2 **Choose the Field: amount**

Open **Field**, type `amount` and choose `amount`, the first of four matches.

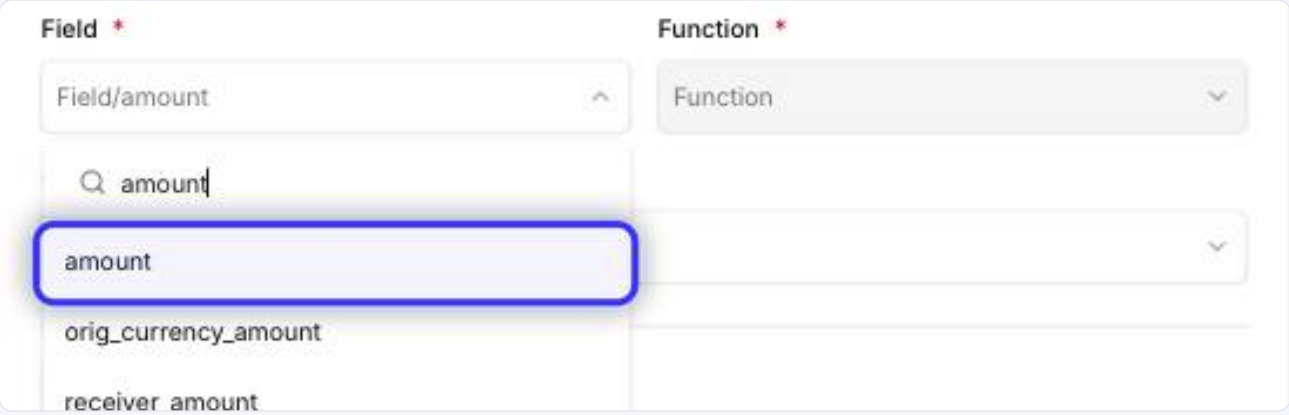


Figure 9.130 Field search for amount

Step 3 **Choose the Function: Maximum**

Open **Function**. For a numeric field the list offers **Count**, **Count Distinct**, **Sum**, **Average**, **Minimum** and **Maximum**. Choose **Maximum**: the variable keeps the largest single amount, not the total.

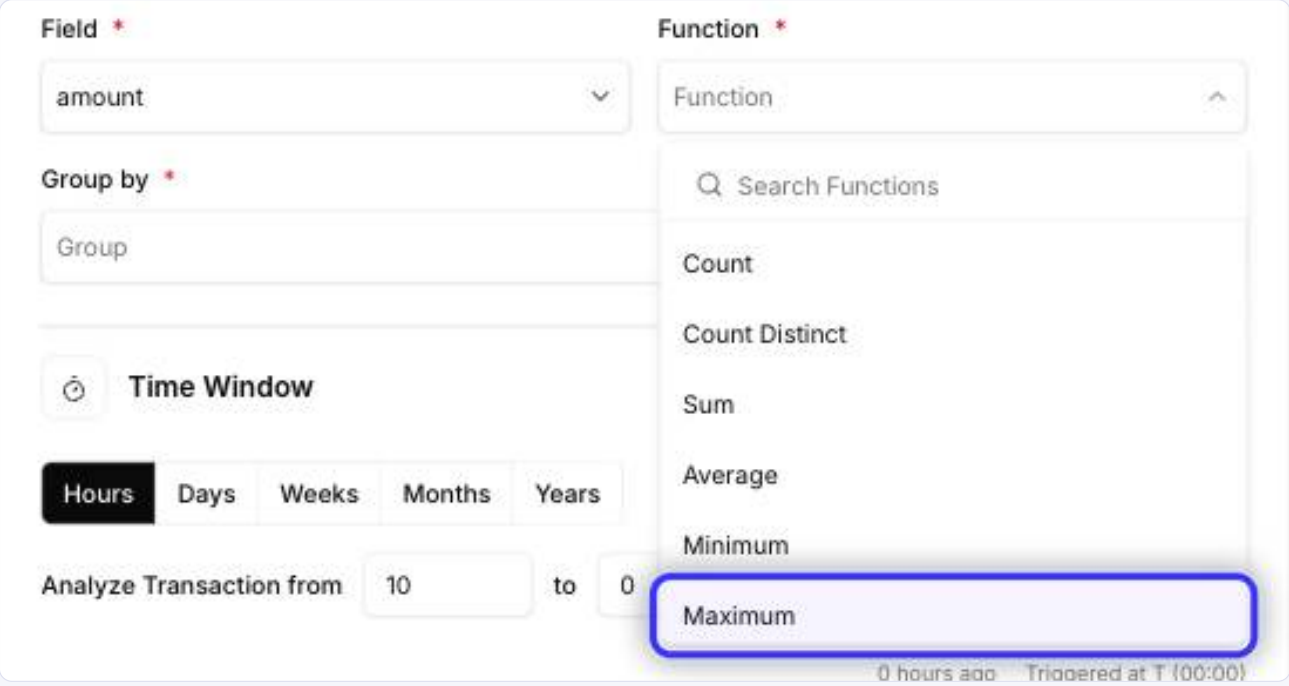


Figure 9.131 Function: Maximum

Step 4 **Choose Group by: sender_entity_id**

Open **Group by**, type `sender_entity` in **Search Fields** and choose `sender_entity_id`, so the largest amount is calculated separately for each sender.



Figure 9.132 Group by search: sender_entity_id

Step 5 **Set the time window: Days, 1 to 0, and save**

Scroll down. Click **Days** (1); the default is **Hours**. Enter 1 in **Analyze Transaction from** and 0 in **to** (2): the 1 day up to the trigger time T. Leave the blank row under **Filters (1)** (3) empty: a blank row is dropped when you save. Click **Save Variable** (4).

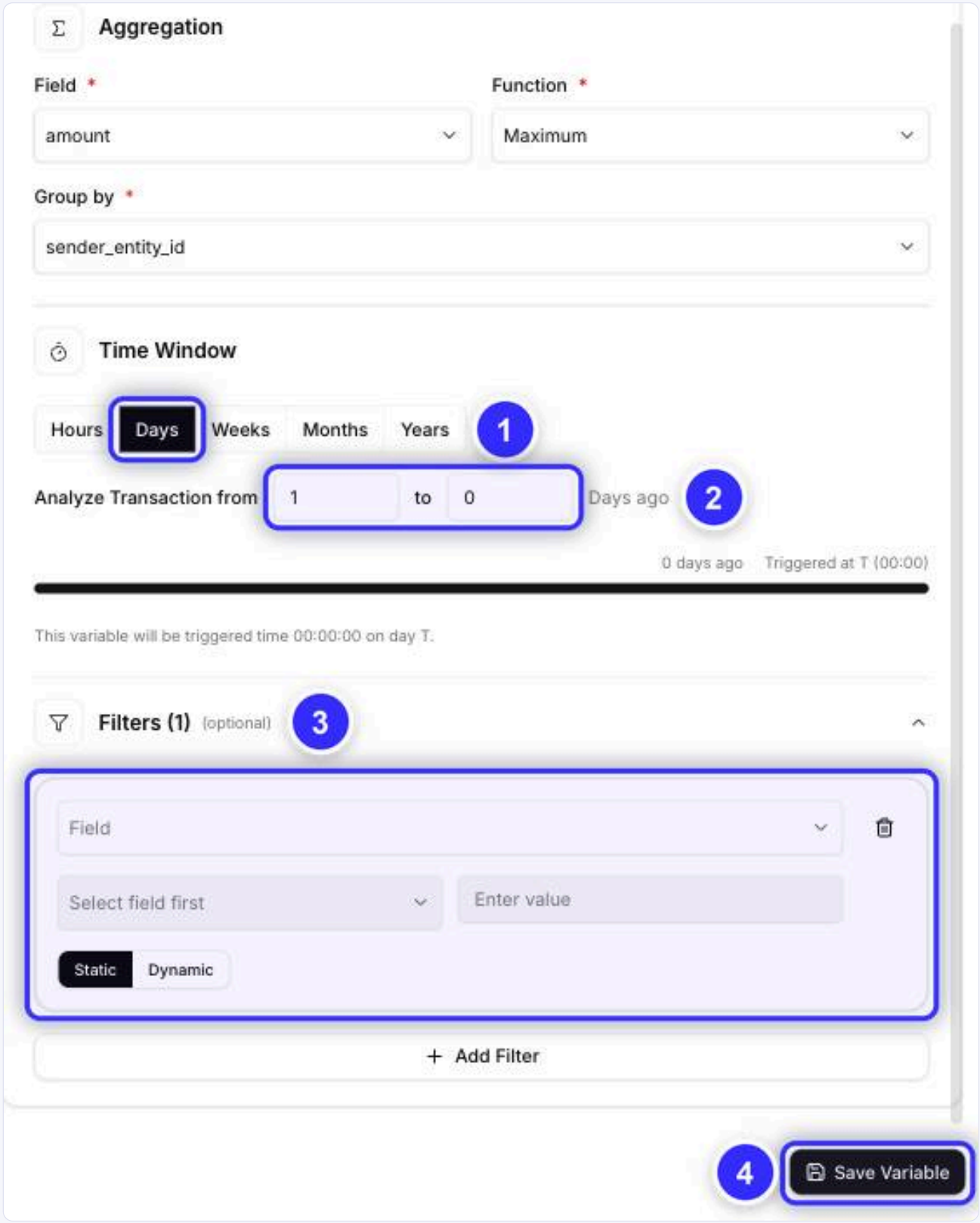


Figure 9.133 Time window 1 to 0 Days ago, blank filter row and Save Variable

Step 6 **Find the variable in the list**

The dialog closes and the variable is the first row of the **Variables** list, here VAR-08102026-000796.

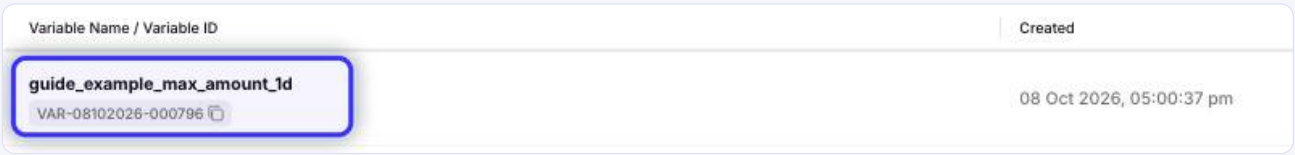


Figure 9.134 Rule 7 variable in the Variables list

Step 7 **Check the saved variable**

Click the row. **View Variable** shows the type tag **NUM_AGG_MAX** (1), the **CREATED** and **UPDATED** times and user (2), `amount` / **Maximum** / `sender_entity_id` (3), 1 to 0 **Days ago** (4) and **Filters (0)** (5).

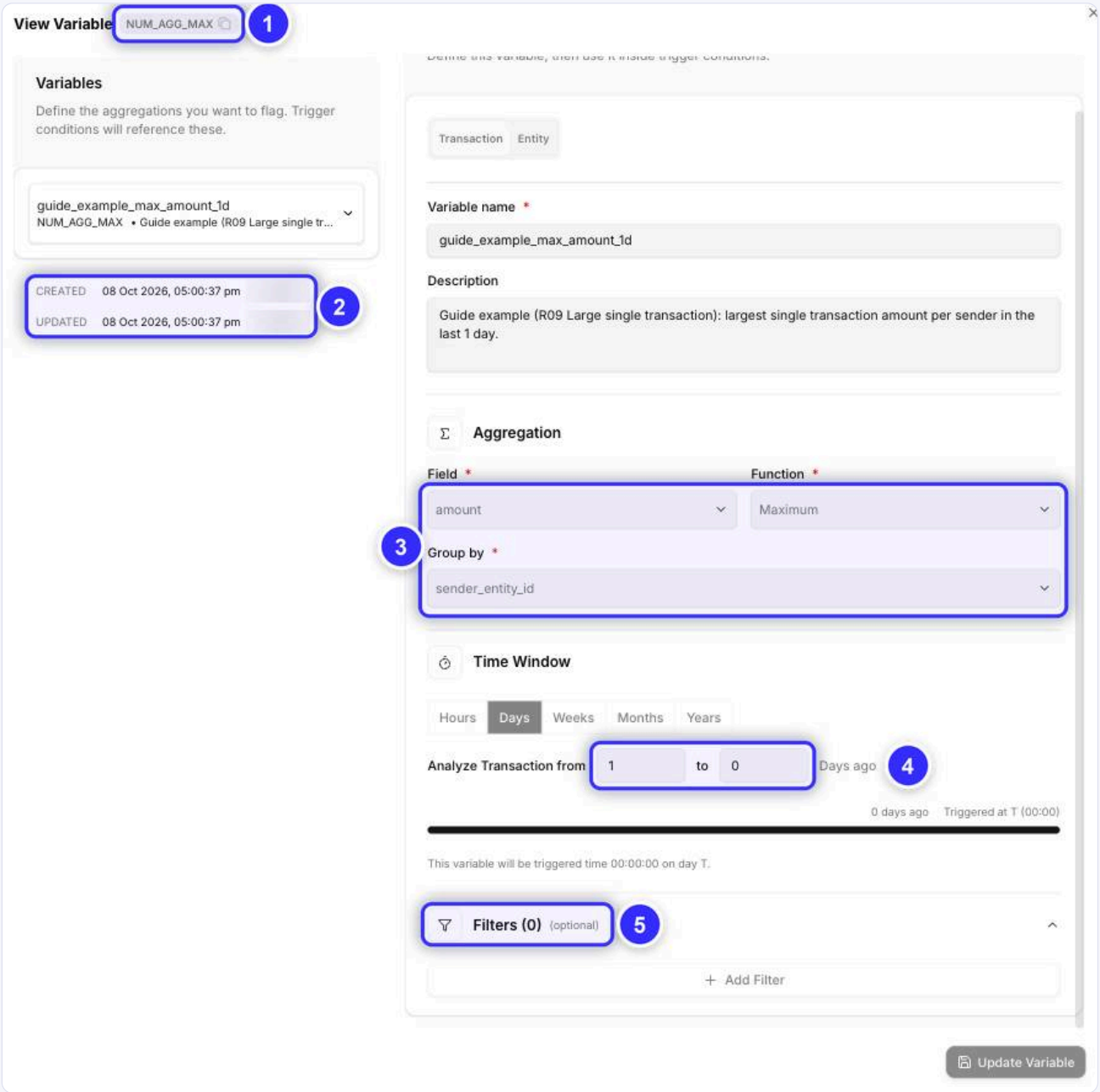


Figure 9.135 View Variable for max_amount_1d

Part B: Create the typology

Fyscal ARCX → Transaction Monitoring → Typology → + New

Step 8 **Fill in the details and choose Large Transaction**

Click **+ New** on **Typology**. Type the name `R09 Large single transaction - PHP 1000000 or more in one transaction in 1 day` (1). Set **Suppression Window** to 1 and choose **Day** (2): the window is one day. Write a description (3). Open **Typology type** (4), type `Large` and click **Large Transaction LT-01**.



Figure 9.136 Rule 7 details and the Typology type search

Step 9 **Choose the variable in row 1**

In **Group 1**, click **Select field** next to **WHEN**, type part of the name and click `max_amount_1d` .

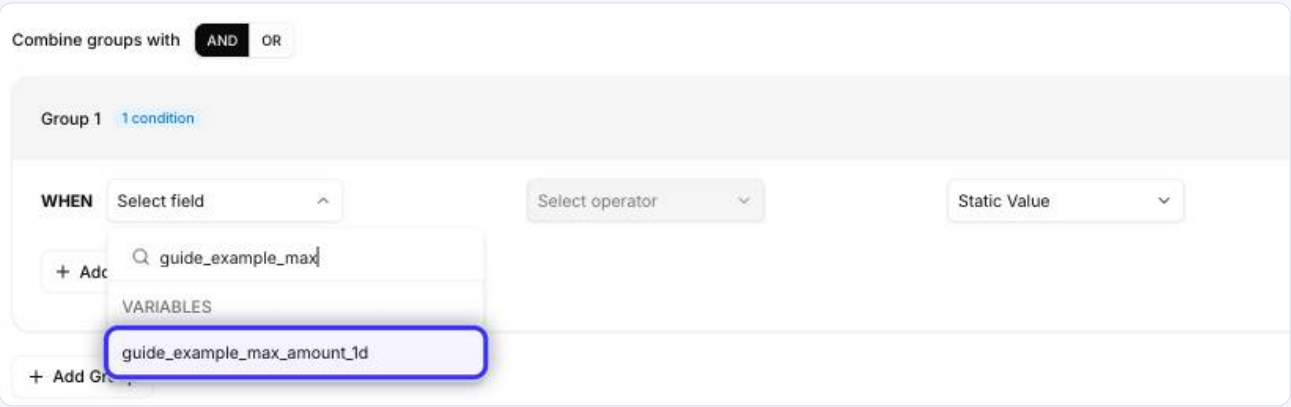


Figure 9.137 Rule 7 row 1: variable search

Step 10 **Choose Greater Than Equal and keep Static Value**

Open **Select operator** and choose **Greater Than Equal**. Keep **Static Value** in the compare-to list: the threshold is a fixed number.

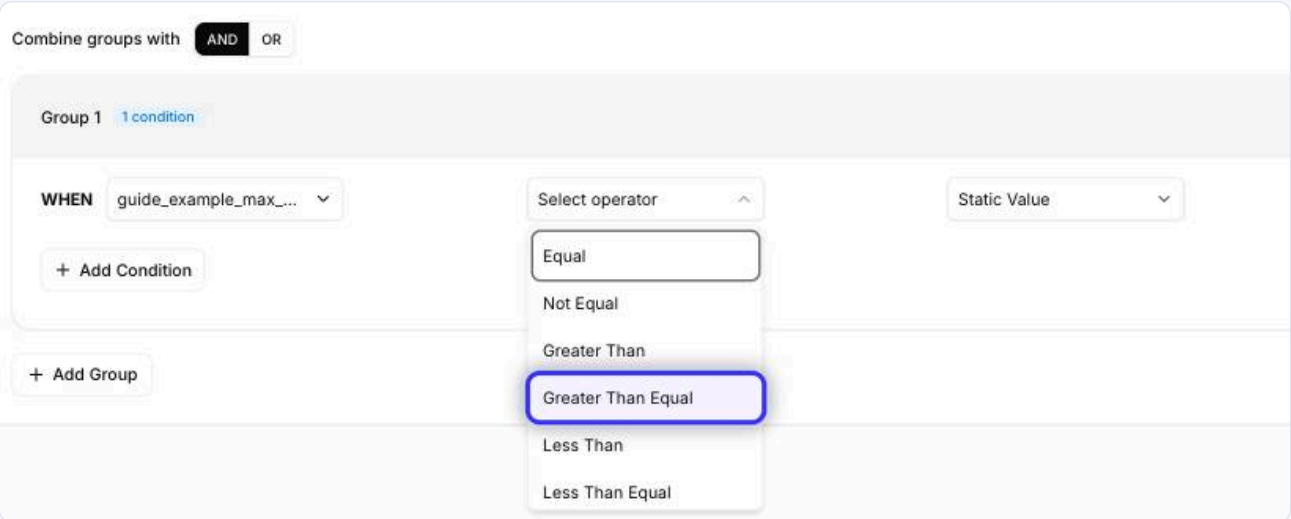


Figure 9.138 Rule 7 row 1: operator list

Step 11 **Enter 1000000 and go to the next step**

Type 1000000 in **Enter value**. Check the name (1), the type chip **Large Transaction (LT-01)** (2), **1 Day** (3), the description (4), **Match** AND (5) and the row (6). Click **Next Step** (7).

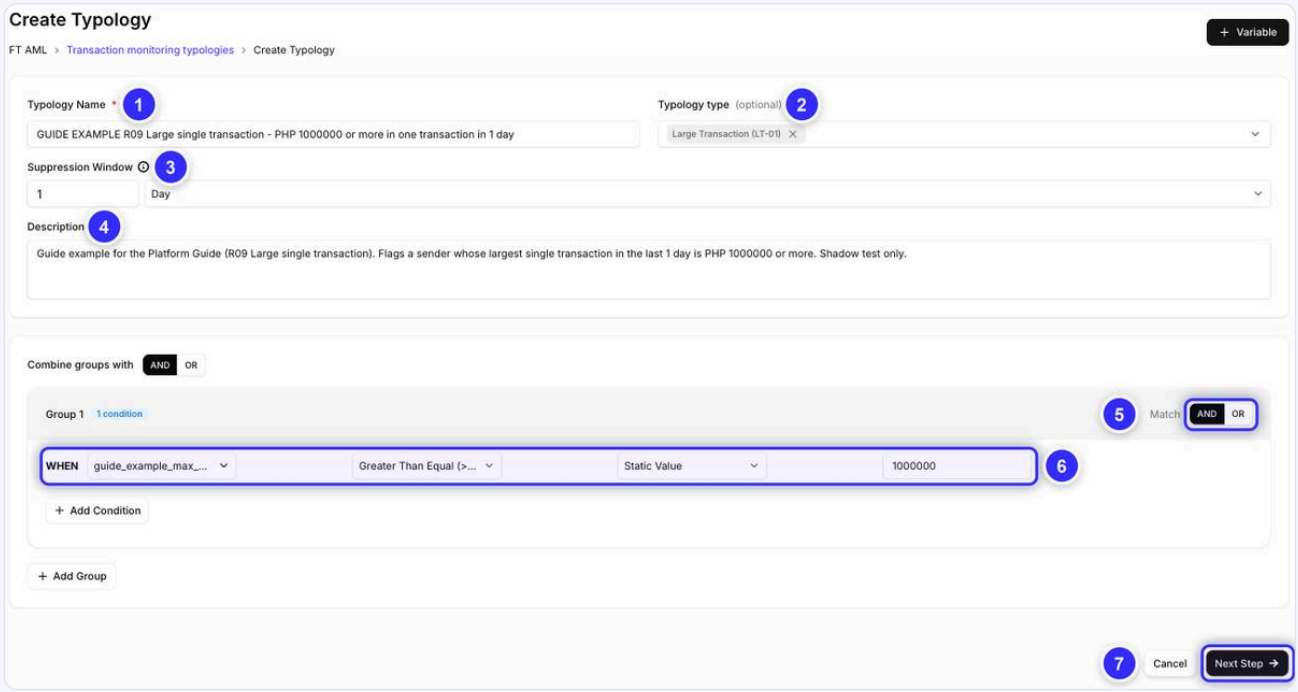


Figure 9.139 The completed Rule 7 page

Part C: Choose the schedule and save

Step 12 **Select the shared schedule and save the draft**

On **Review & schedule rule**, open **Select Schedule** (1), search for `schedule_2027` and click it. Its fields fill in (2); leave them unchanged, because they belong to the shared schedule. The screenshot was taken before the start was moved to 09 Oct 2026, so it shows 01/01/2027. Click **Save as Draft** (3).

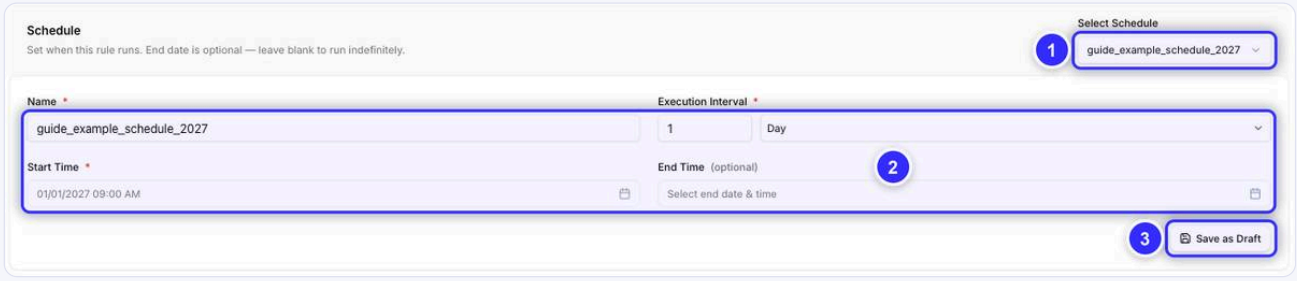


Figure 9.140 The shared schedule selected; Save as Draft

Step 13 **Check the saved draft**

Wait a few seconds: the page becomes **Update Typology** (1) with the schedule (2), the run sentence (3), **Update** (4), **Dry Run** (5) and **Activate** (6). The screenshot shows the start in force when it was taken (01 Jan 2027).

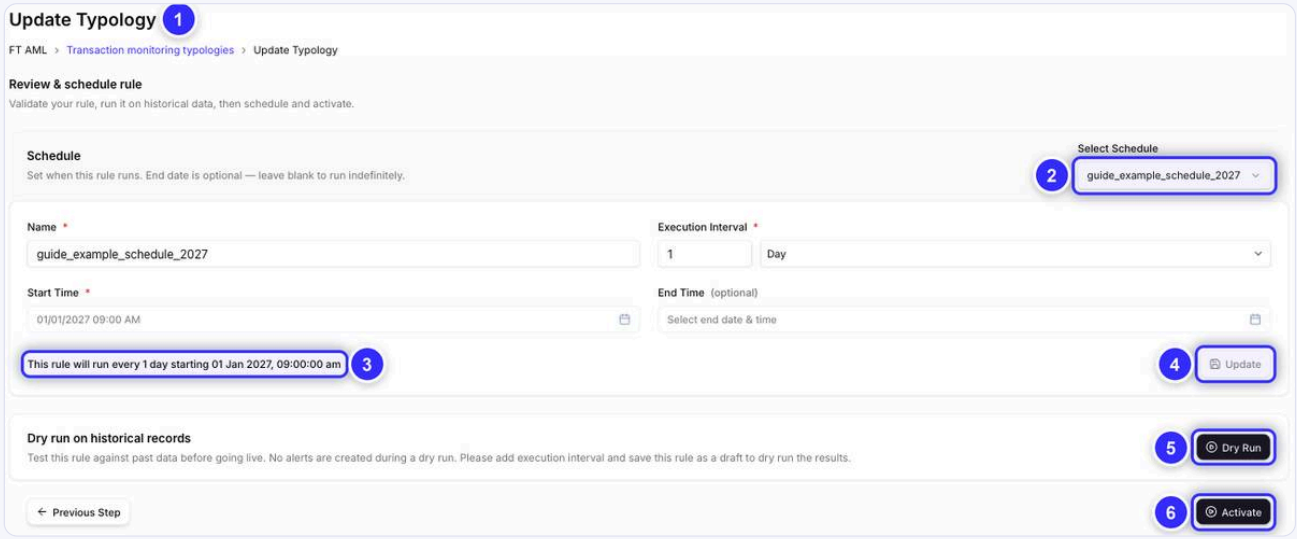


Figure 9.141 Rule 7 after Save as Draft

Step 14 **Check the rule page**

Open the rule from **Transaction Monitoring → Typology**. It shows **Draft** and the rule ID TMR-08102026-001131, created 08 Oct 2026, 05:15:18 pm (1); the summary with **INTERVAL** Every 1 day, **SUPPRESSION** 1Day and **TYPOLOGY** Large Transaction (2); the condition, with the operator shown as **Greater Than Equal (>=)** (3); and the variable card `max_amount_1d`, Num_agg_max, **WINDOW** in last 1 day, **GROUP** `sender_entity_id` (4).

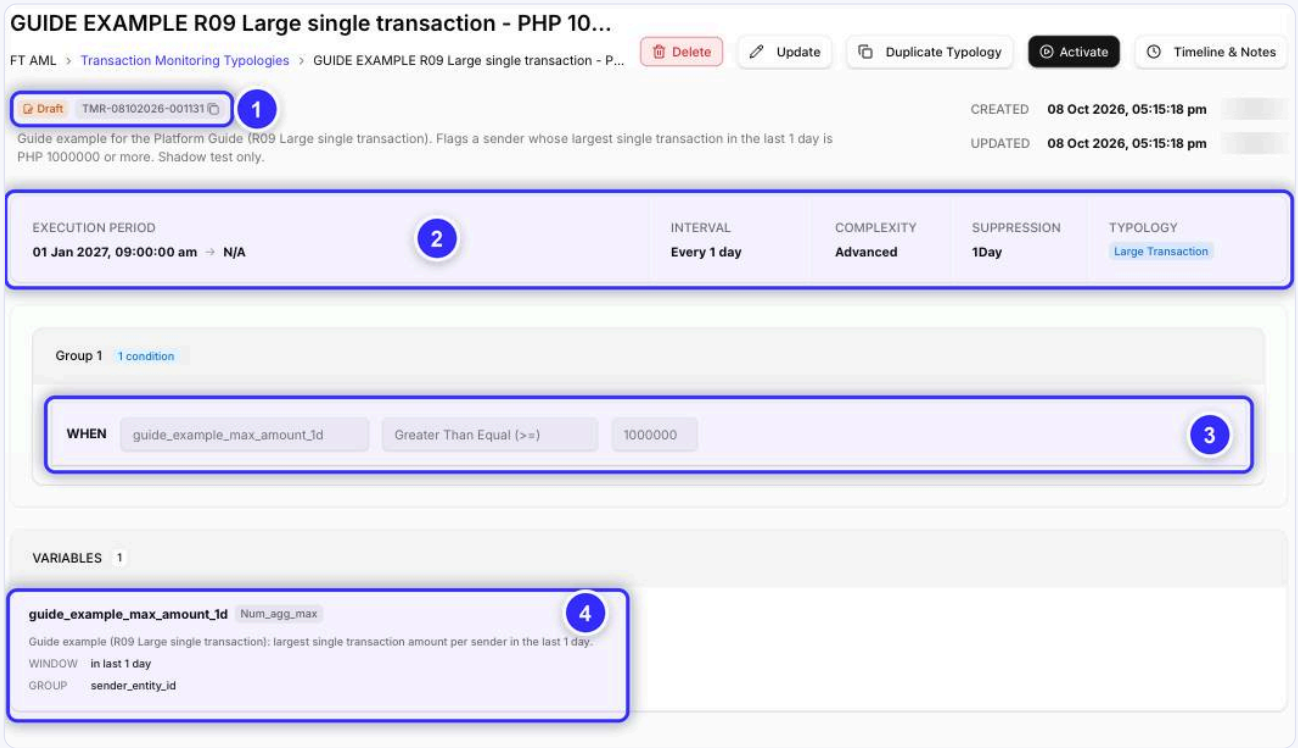


Figure 9.142 The saved Rule 7 as a Draft, TMR-08102026-001131

How it evaluates. At each daily run the variable takes, for each sender, the largest single amount in the last day. Sender A sent ₱1,200,000 once and ₱5,000 twice: the maximum is ₱1,200,000, so the rule alerts. Sender B sent ₱600,000 twice (₱1,200,000 in total): the maximum is ₱600,000, so there is no alert from this rule.

Dry-run result. In testing, the rule created 0 alerts at its real threshold (>= 1000000) in all four windows: the test data has no single transaction of ₱1,000,000 or more. To prove the rule works, the threshold was lowered to >= 1 for one dry run. That created 764 alerts (0 / 0 / 500 / 264 by window, newest first), then the threshold was restored and a new dry run returned 0 again. See Test a typology with Dry Run for the method.

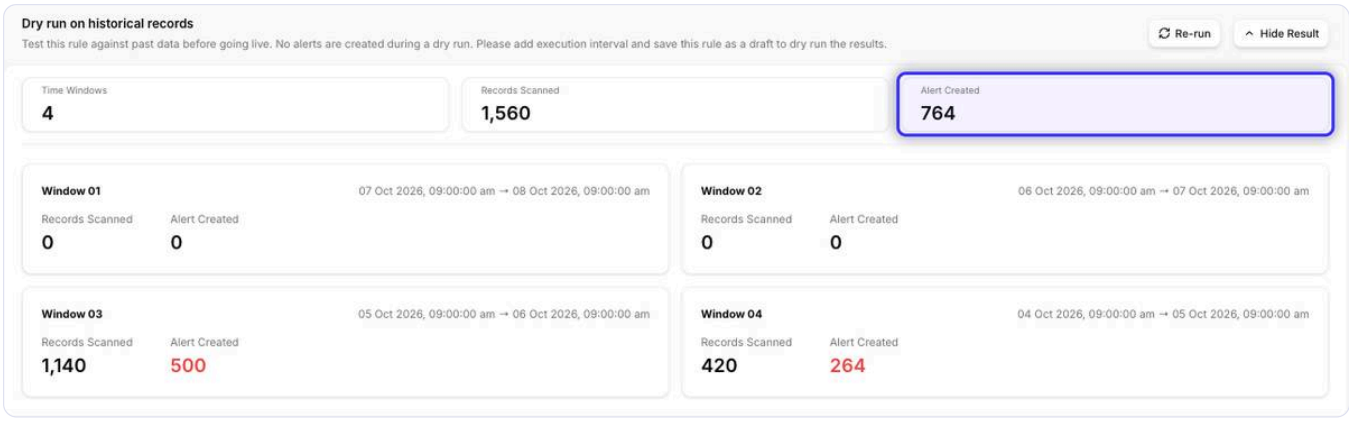


Figure 9.143 Rule 7 positive control (threshold temporarily >= 1): 764 alerts

Tuning. Set the amount (1000000) from the size of payment you want reviewed individually. A longer window (for example 7 to 0 Days) catches the same payment on more runs, so keep the **Suppression Window** at least as long as the window.

Rule 8 · Smurfing

RED FLAG **Many very small payments in a day**

LOGIC

Counts the sender's transactions under ₱1,000 in the last day.

WINDOW

1 to 0 Days

THRESHOLD

≥ 20 under ₱1,000

✓ Verified by positive control

What it detects and why. This rule flags a sender who makes 20 or more transactions under ₱1,000 in one day. Many very small payments in a short time can be a way to move money in amounts that do not stand out one by one.

Item	Setting
Variable `small_txn_count_1d`	**Count** of `id`, grouped by `sender_entity_id`, **Days** from 1 to 0, filter `amount` **Less Than** 1000
Typology type	Structuring (TP100)
Suppression Window	1 Day
Condition	Group 1, Match AND: `small_txn_count_1d` **Greater Than Equal (>=)** Static Value 20
Schedule	Existing `schedule_2027` (created in Rule 1): every 1 Day, starting 09 Oct 2026, 09:00 AM, no end time

Part A: Create the variable

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 1 **Open the form and name the variable**

Click **+ New** on **Variables** and leave **Transaction** selected. Type `small_txn_count_1d` in **Variable name** (1) and a description such as “Number of transactions under PHP 1000 per sender in the last 1 day.” (2).

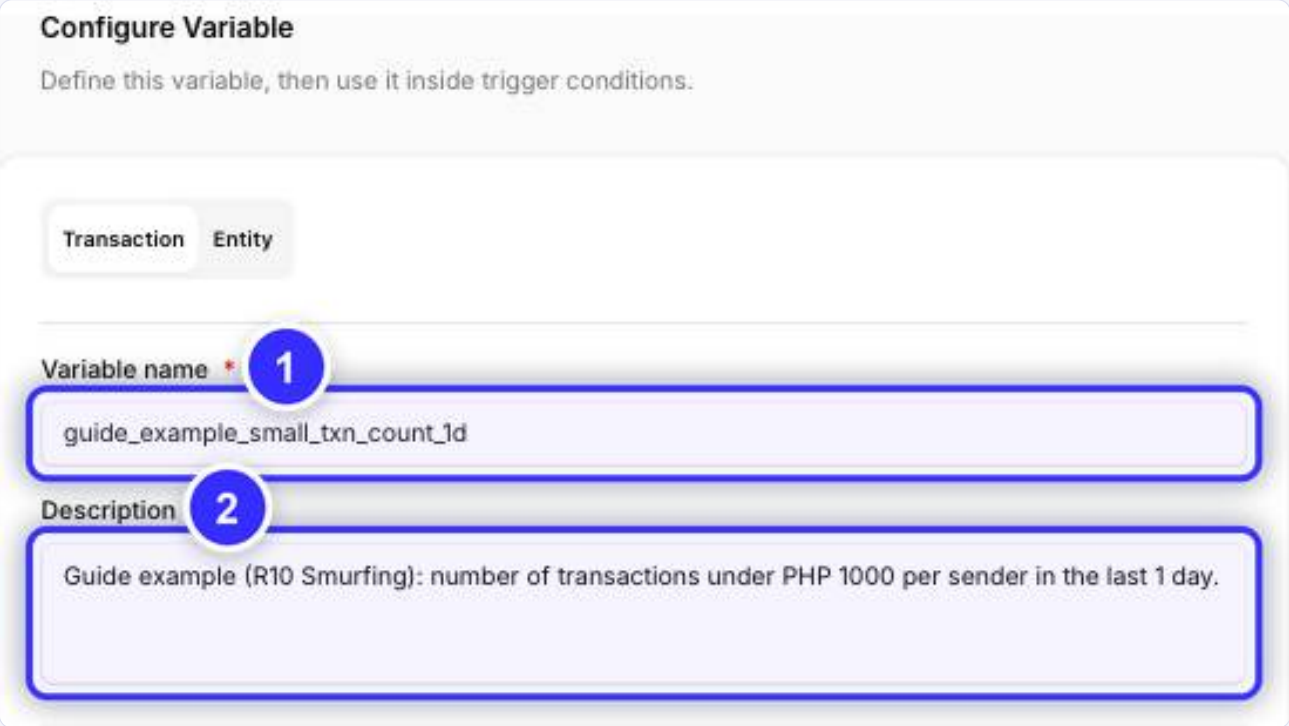


Figure 9.144 Rule 8 variable: name and description

Step 2 **Choose the Field: id**

Open **Field**, type `id` and choose `id`, the first match. Counting `id` counts transactions.

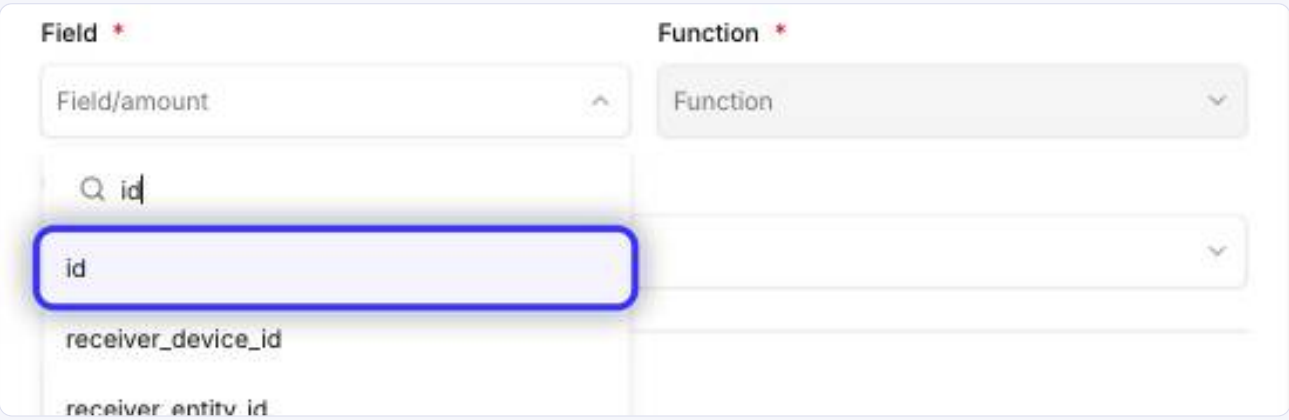


Figure 9.145 Field search for id

Step 3 **Choose the Function: Count**

Open **Function**. For an ID or text field the list offers **Count**, **Count Distinct**, **Minimum** and **Maximum**. Choose **Count**.

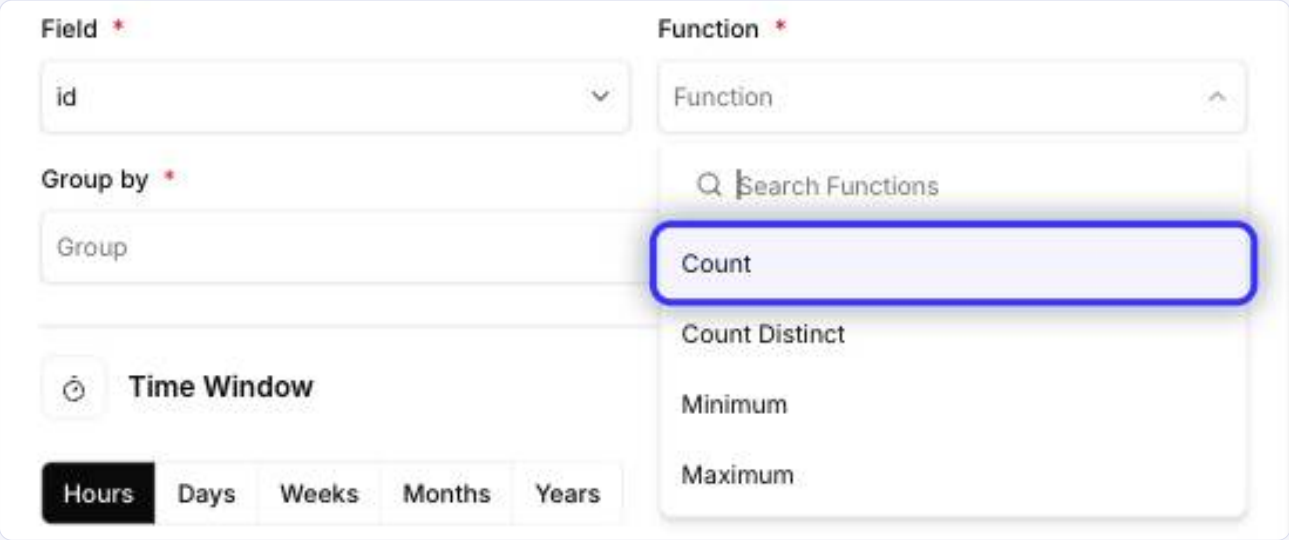


Figure 9.146 Function: Count

Step 4 **Choose Group by: sender_entity_id**

Open **Group by**, type `sender_entity` in **Search Fields** and choose `sender_entity_id`, so the count is calculated separately for each sender.



Figure 9.147 Group by search: sender_entity_id

Step 5 **Add the filter: choose the amount field**

Scroll to **Filters (1)**. In the blank row open **Field** (1), type `amount` and choose `amount`. The filter decides which transactions are counted.

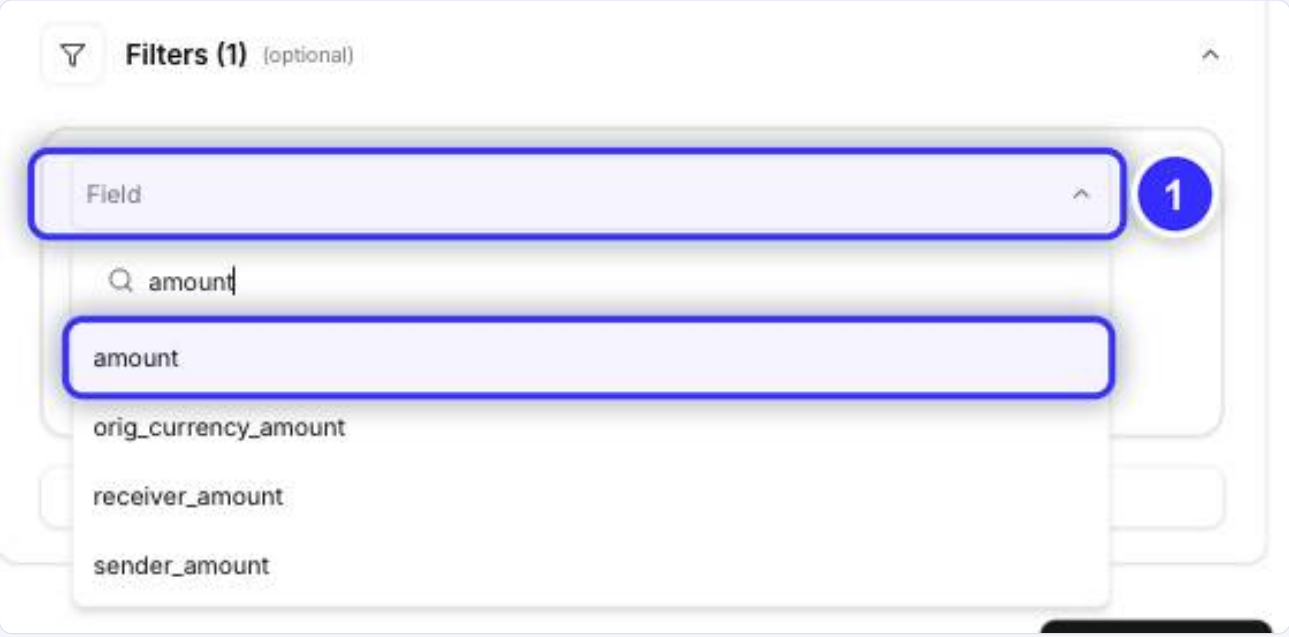


Figure 9.148 Filter row: the field search for amount

Step 6 **Choose Less Than and type 1000**

Open **Operator...** and choose **Less Than**, then type 1000 in **Enter value** and keep **Static**. ₱1,000 itself is not counted.

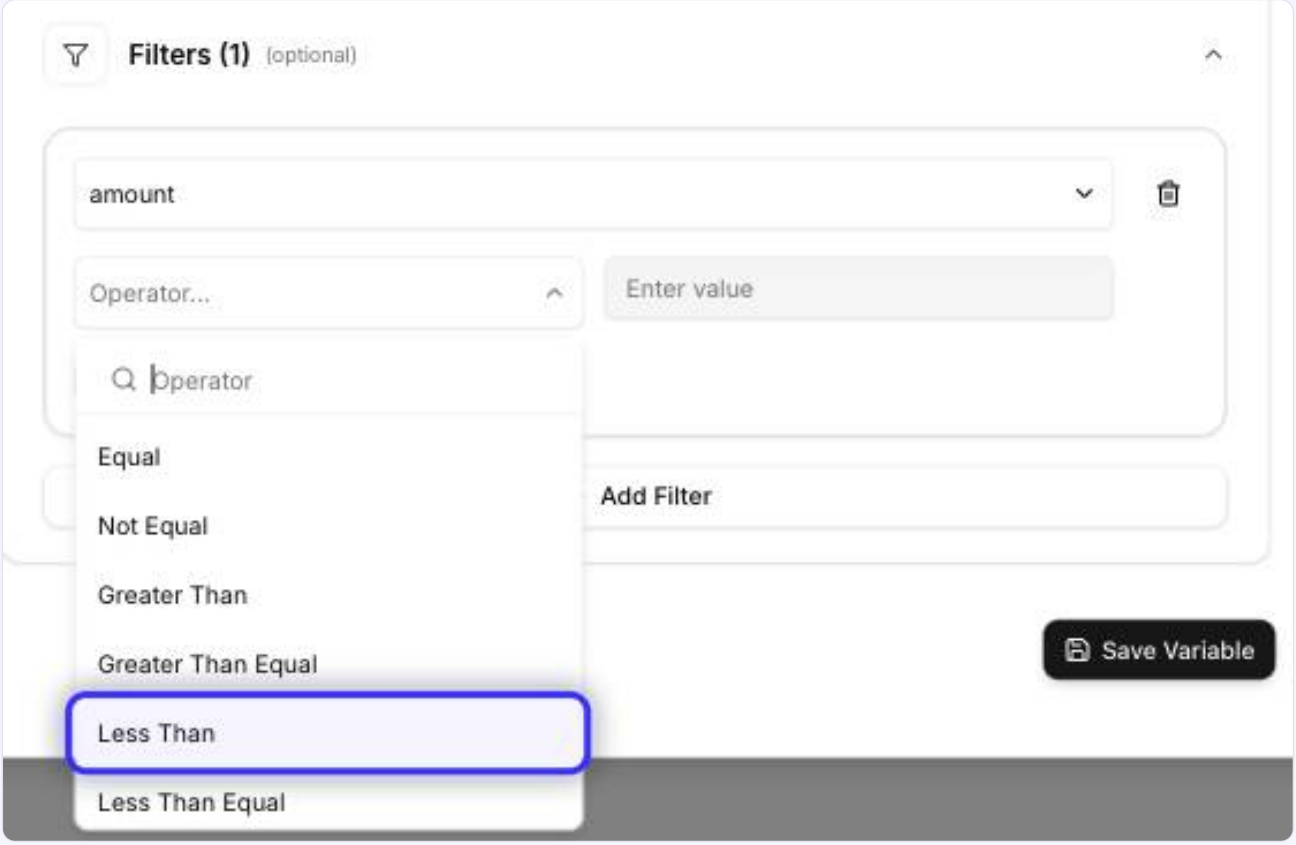


Figure 9.149 Filter operators: Less Than

Step 7 **Set the time window: Days, 1 to 0, and save**

Scroll down. Click **Days** (1); the default is **Hours**. Enter 1 in **Analyze Transaction from** and 0 in **to** (2): the 1 day up to the trigger time T. The filter row (3) reads `amount` **Less Than** 1000, **Static**. Click **Save Variable** (4).

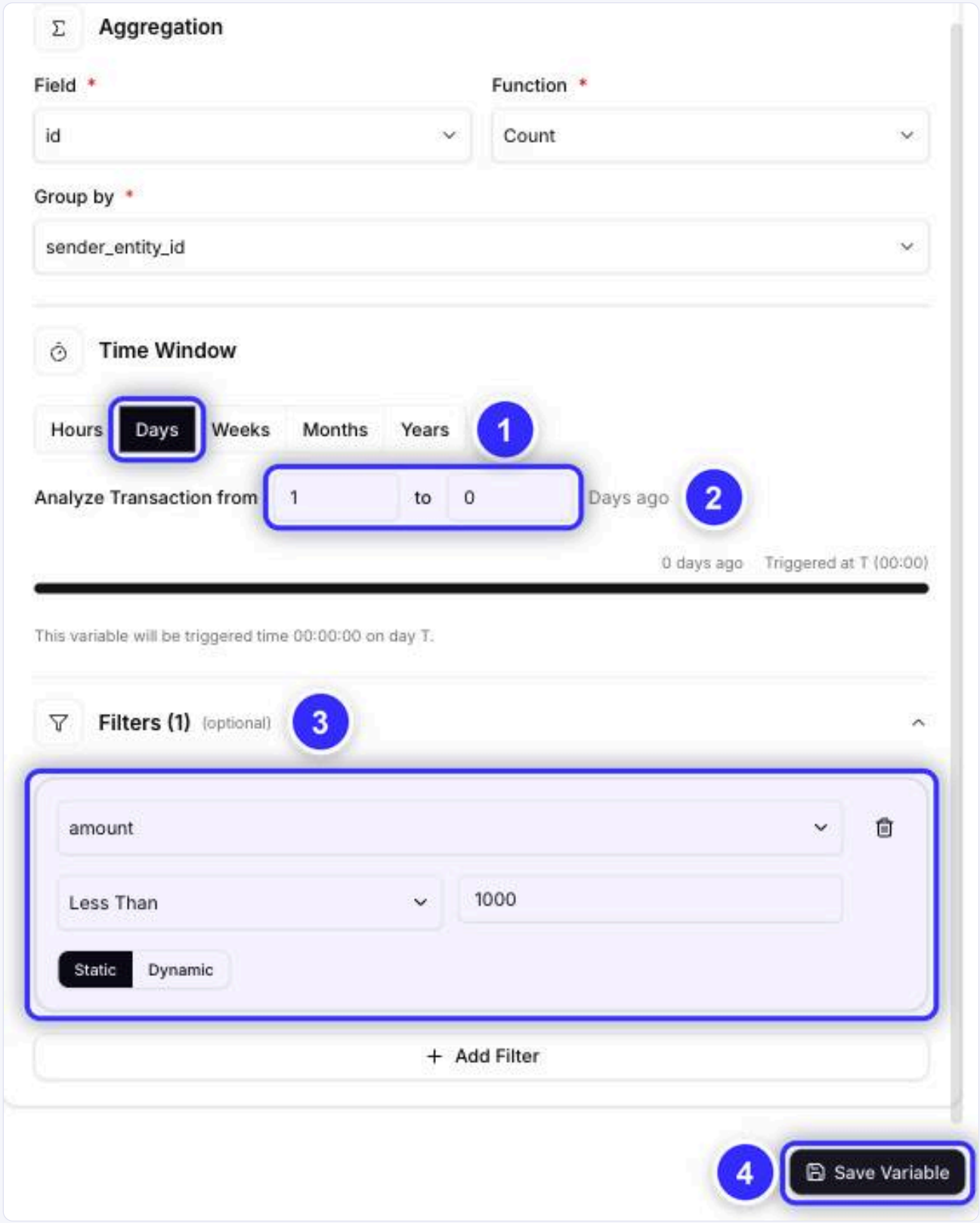


Figure 9.150 Time window 1 to 0 Days ago, the amount filter and Save Variable

Step 8 **Find the variable in the list**

The dialog closes and the variable is the first row of the **Variables** list, here VAR-08102026-000797.

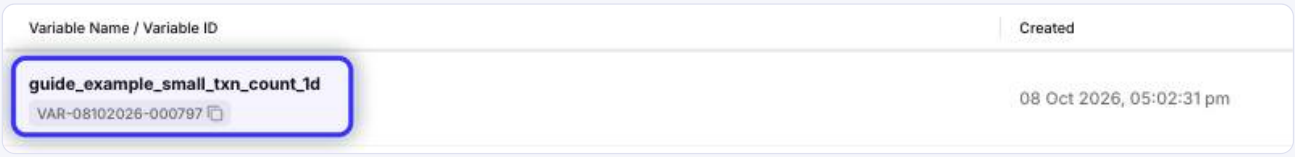


Figure 9.151 Rule 8 variable in the Variables list

Step 9 **Check the saved variable**

Click the row. **View Variable** shows the type tag **STR_AGG_COUNT** (1), the **CREATED** and **UPDATED** times and user (2), `id` / **Count** / `sender_entity_id` (3), 1 to 0 **Days ago** (4) and the saved filter, `amount` **Less Than** 1000 (5).

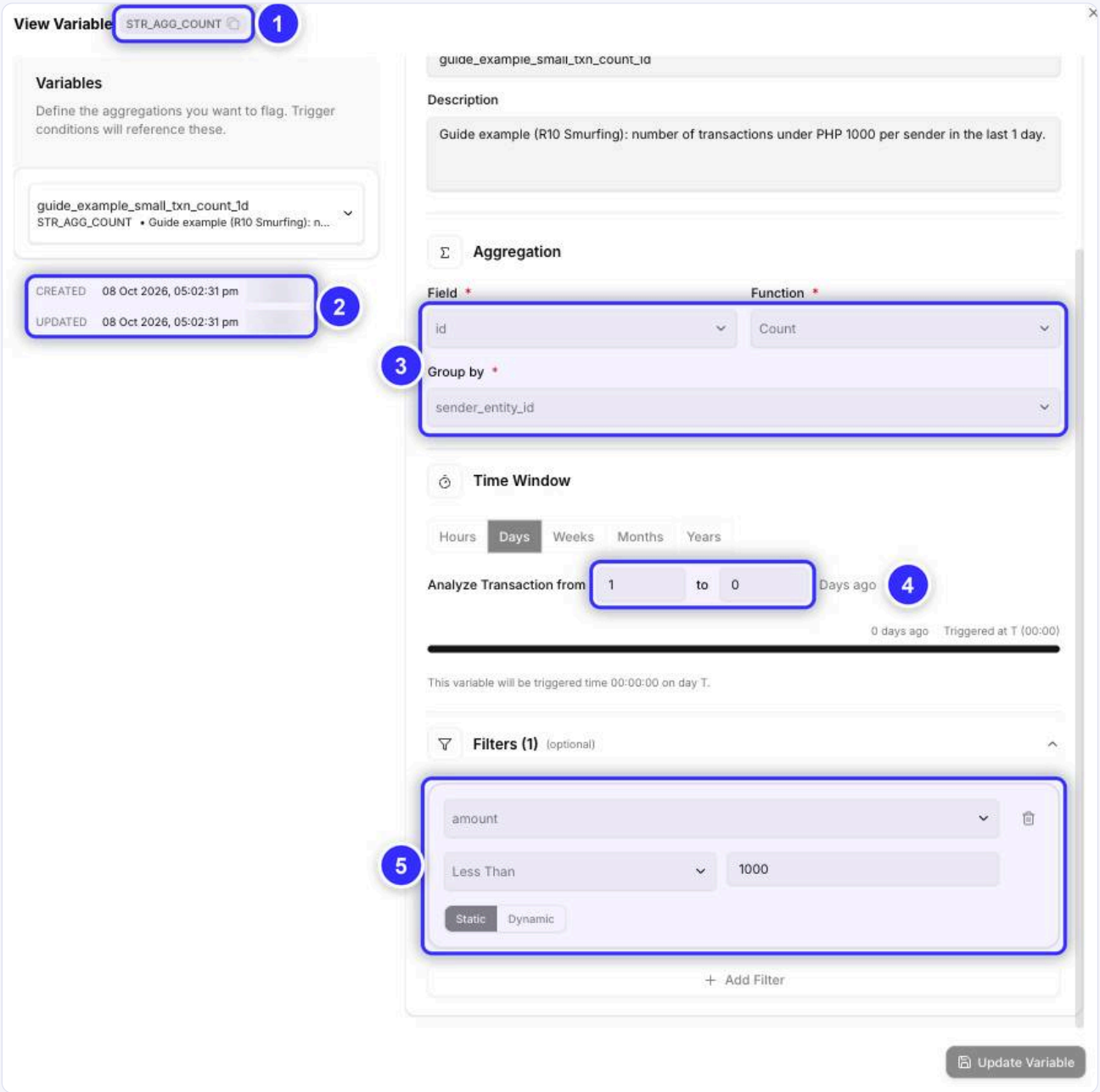


Figure 9.152 View Variable for small_txn_count_1d

Part B: Create the typology

Fyscal ARCX → Transaction Monitoring → Typology → + New

Step 10 **Fill in the details and choose Structuring**

Click **+ New** on **Typology**. Type the name `R10 Smurfing - 20 or more transactions under PHP 1000 in 1 day` (1). Set **Suppression Window** to 1 and choose **Day** (2): the window is one day. Write a description (3). Open **Typology type** (4), type `Struct` and click **Structuring TP100**.

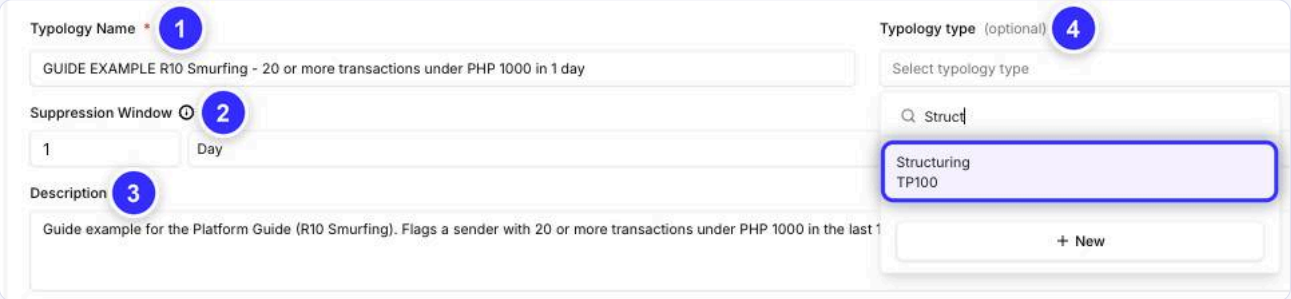


Figure 9.153 Rule 8 details and the Typology type search

Step 11 **Choose the variable in row 1**

In **Group 1**, click **Select field** next to **WHEN**, type part of the name and click `small_txn_count_1d`.

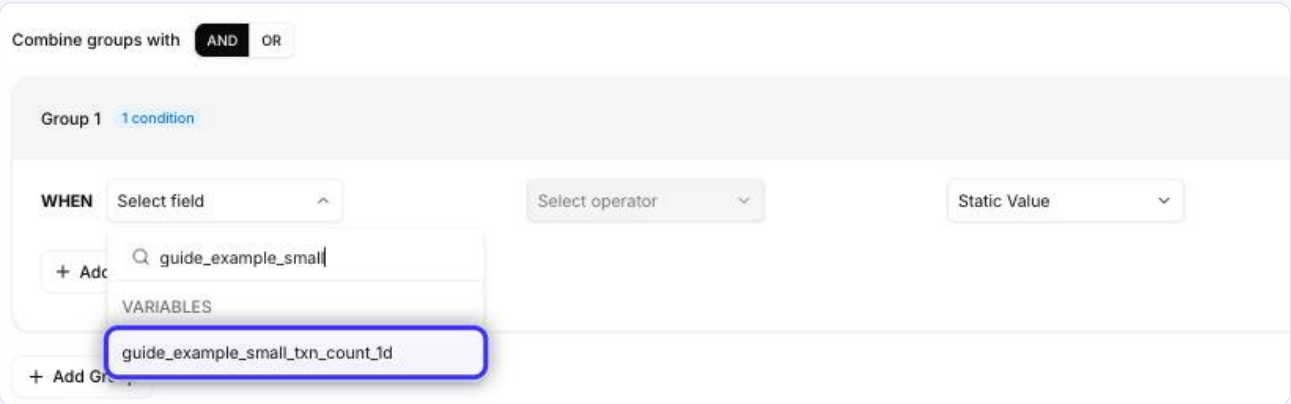


Figure 9.154 Rule 8 row 1: variable search

Step 12 **Choose Greater Than Equal and keep Static Value**

Open **Select operator** and choose **Greater Than Equal**. Keep **Static Value** in the compare-to list: the threshold is a fixed number.

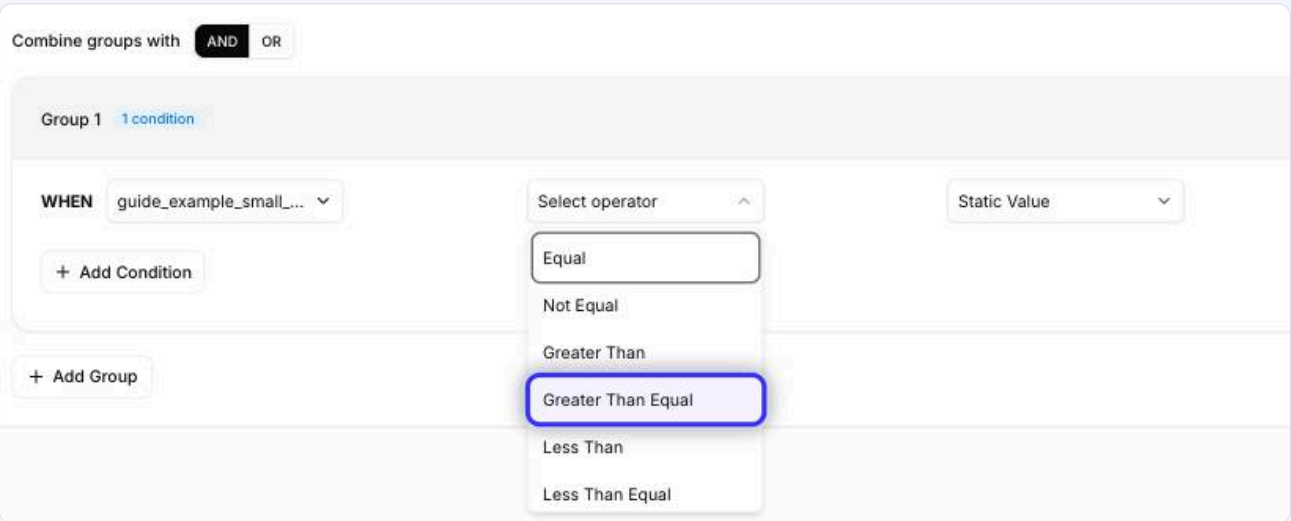


Figure 9.155 Rule 8 row 1: operator list

Step 13 **Enter 20 and go to the next step**

Type 20 in **Enter value**. Check the name (1), the type chip **Structuring (TP100)** (2), **1 Day** (3), the description (4), **Match** AND (5) and the row (6). Click **Next Step** (7).

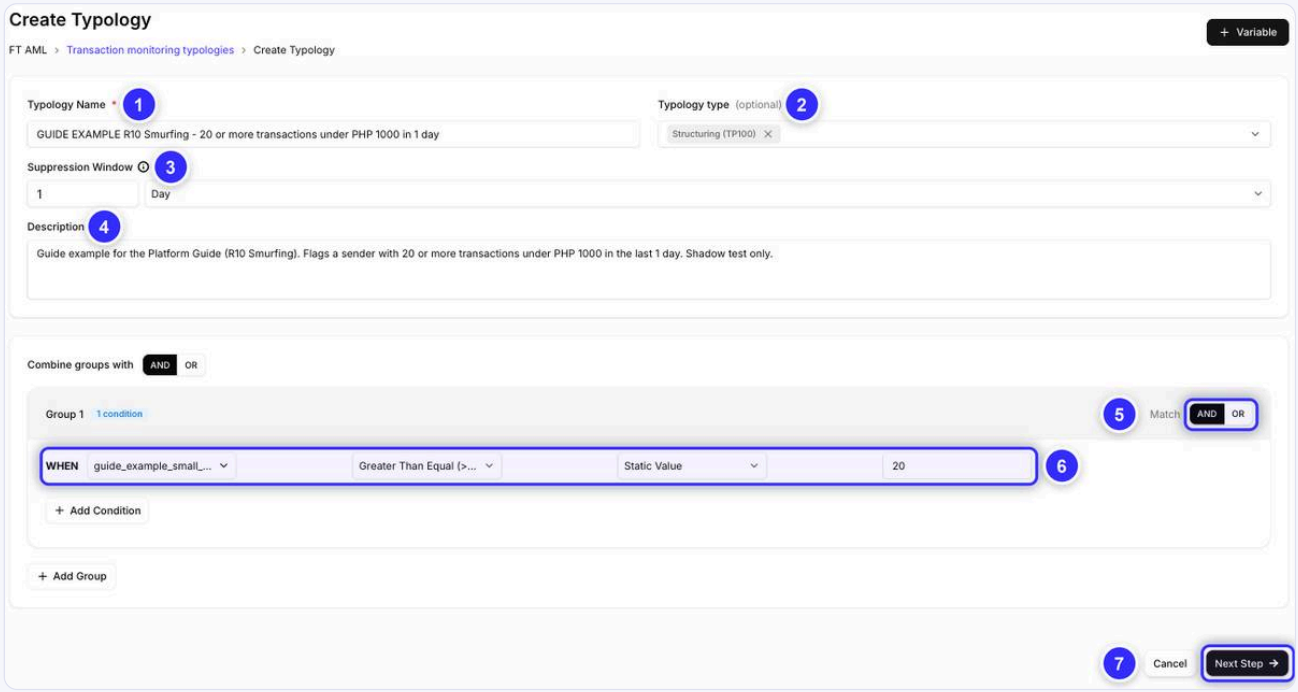


Figure 9.156 The completed Rule 8 page

Part C: Choose the schedule and save

Step 14 **Select the shared schedule and save the draft**

On **Review & schedule rule**, open **Select Schedule**, search for `schedule_2027`, click it and click **Save as Draft**, as in Rule 7.

Step 15 **Check the saved draft**

Wait a few seconds: the page becomes **Update Typology** (1) with the schedule (2), the run sentence (3), **Update** (4), **Dry Run** (5) and **Activate** (6). The screenshot shows the start in force when it was taken (01 Jan 2027).

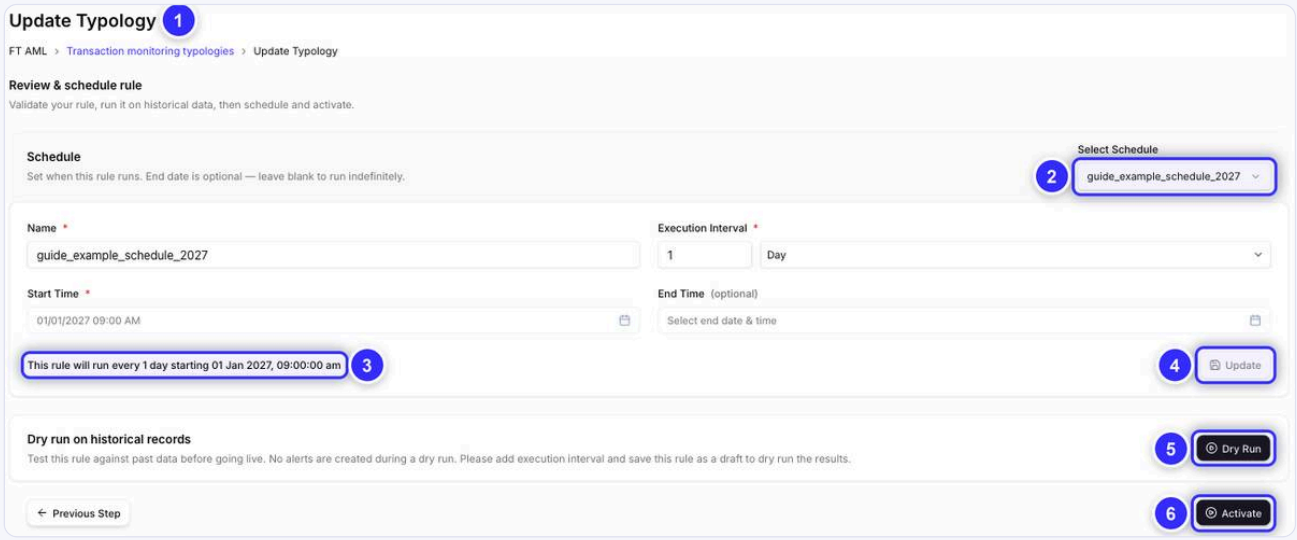


Figure 9.157 Rule 8 after Save as Draft

Step 16 **Check the rule page**

Open the rule from **Transaction Monitoring → Typology**. It shows **Draft** and the rule ID TMR-08102026-001132, created 08 Oct 2026, 05:17:54 pm (1); the summary with **INTERVAL** Every 1 day, **SUPPRESSION** 1Day and **TYPOLOGY** Structuring (2); the condition, with the operator shown as **Greater Than Equal (>=)** (3); and the variable card `small_txn_count_1d`, Str_agg_count, **WINDOW** in last 1 day, **GROUP** `sender_entity_id` (4). The card does not show the variable's filter; check it on **View Variable**.

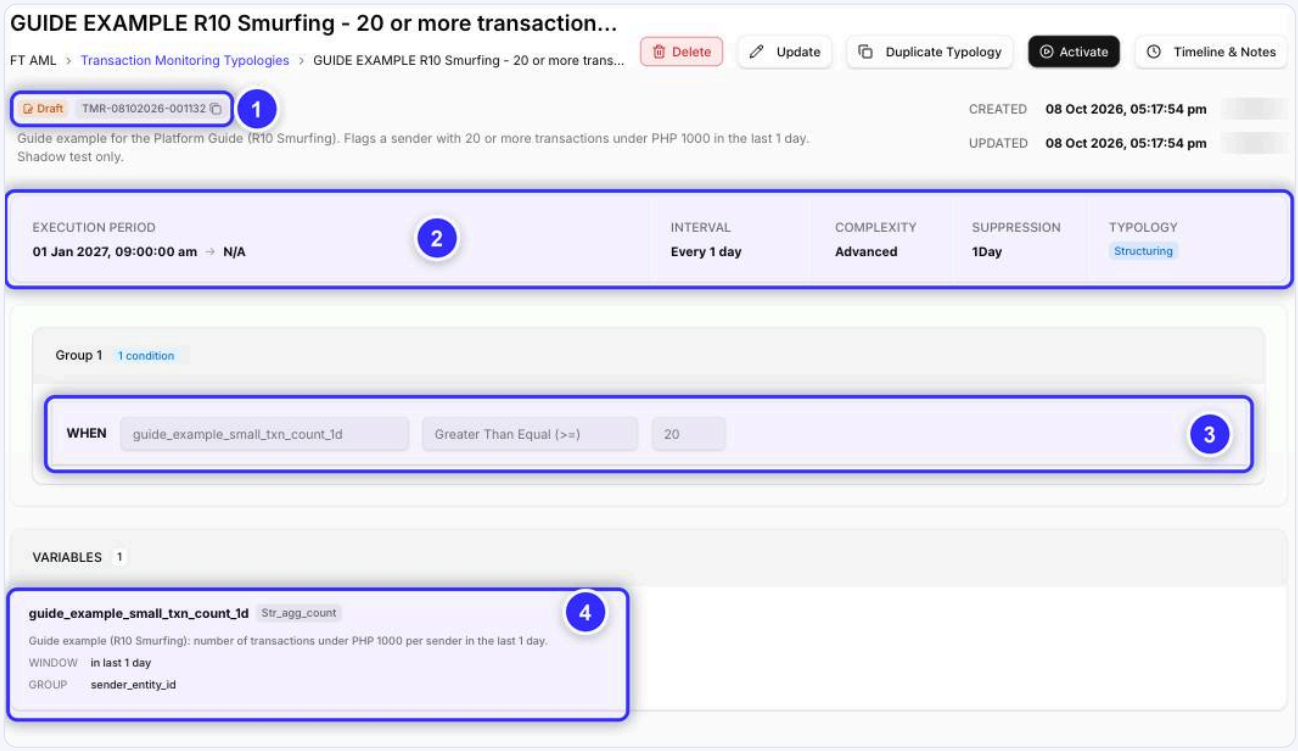


Figure 9.158 The saved Rule 8 as a Draft, TMR-08102026-001132

How it evaluates. At each run the variable counts, for each sender, the transactions under ₱1,000 in the last day. Sender A made 25 payments of ₱500: 25 >= 20, alert. Sender B made 30 payments, 15 of them under ₱1,000: the count is 15, no alert.

Dry-run result. In testing, the rule created 0 alerts at its real threshold (>= 20) in all four windows: the test data has transactions under ₱1,000, but no sender with 20 of them in a day. To prove the rule works, the threshold was lowered to >= 1 for one dry run. That created 339 alerts (0 / 0 / 194 / 145 by window, newest first), then the threshold was restored and a new dry run returned 0 again. See Test a typology with Dry Run for the method.

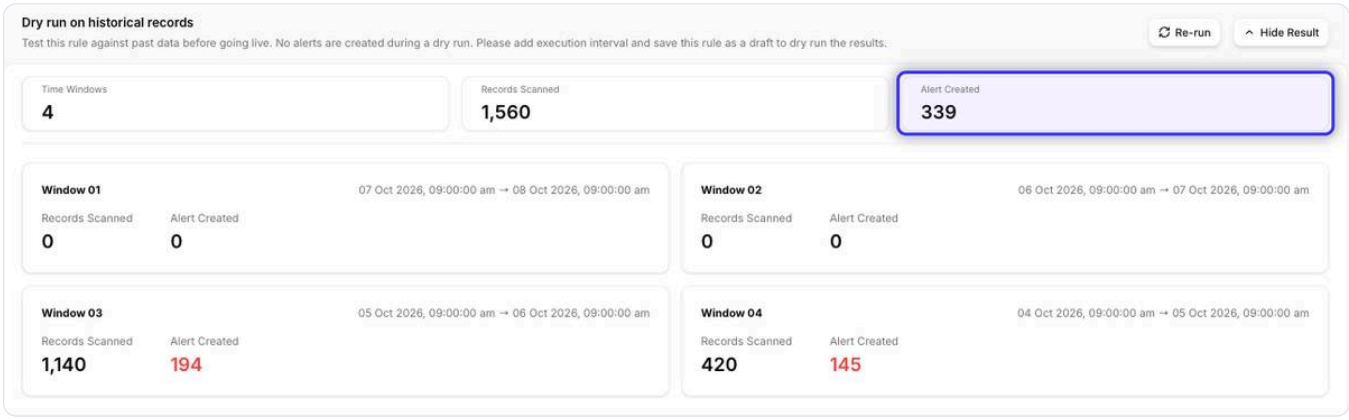


Figure 9.159 Rule 8 positive control (threshold temporarily >= 1): 339 alerts

Tuning. You can change the small-amount limit (the filter value 1000), the count (20) and the window. A higher limit or a lower count raises more alerts.

Rule 9 · Spike against own history

RED FLAG **A week that is large against the sender's 90 days**

LOGIC

Compares the sender's 7-day total with their 90-day total.

WINDOW
7 to 0 Days and 90 to 0 Days

THRESHOLD
7-day ≥ ₱100,000 AND ≥ 0.5 × 90-day

✓ Verified · 42 alerts

What it detects and why. This rule compares a sender with their own past. It flags a sender who sent ₱100,000 or more in the last 7 days when that is at least half of everything they sent in the last 90 days. A sudden jump against a customer's own baseline can matter even when the amount is ordinary for other customers.

Item	Setting
Variable A `sent_sum_7d_spike`	**Sum** of `amount`, grouped by `sender_entity_id`, **Days** from 7 to 0
Variable B `sent_sum_90d`	**Sum** of `amount`, grouped by `sender_entity_id`, **Days** from 90 to 0
Typology type	Anomaly (TP103)
Suppression Window	7 Day
Conditions	Group 1, Match AND: `sent_sum_7d_spike` **Greater Than Equal (>=)** Static Value 100000 AND `sent_sum_7d_spike` **Greater Than Equal (>=)** Variable `sent_sum_90d`, **THAN MULTIPLIER** 0.5
Schedule	Existing `schedule_2027` (created in Rule 1): every 1 Day, starting 09 Oct 2026, 09:00 AM, no end time

Part A: Create variable A, the recent total

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 1 **Open the form and name variable A**

Click **+ New** on **Variables**. Type `sent_sum_7d_spike` (1) and a description such as "Total amount sent per sender in the last 7 days." (2).

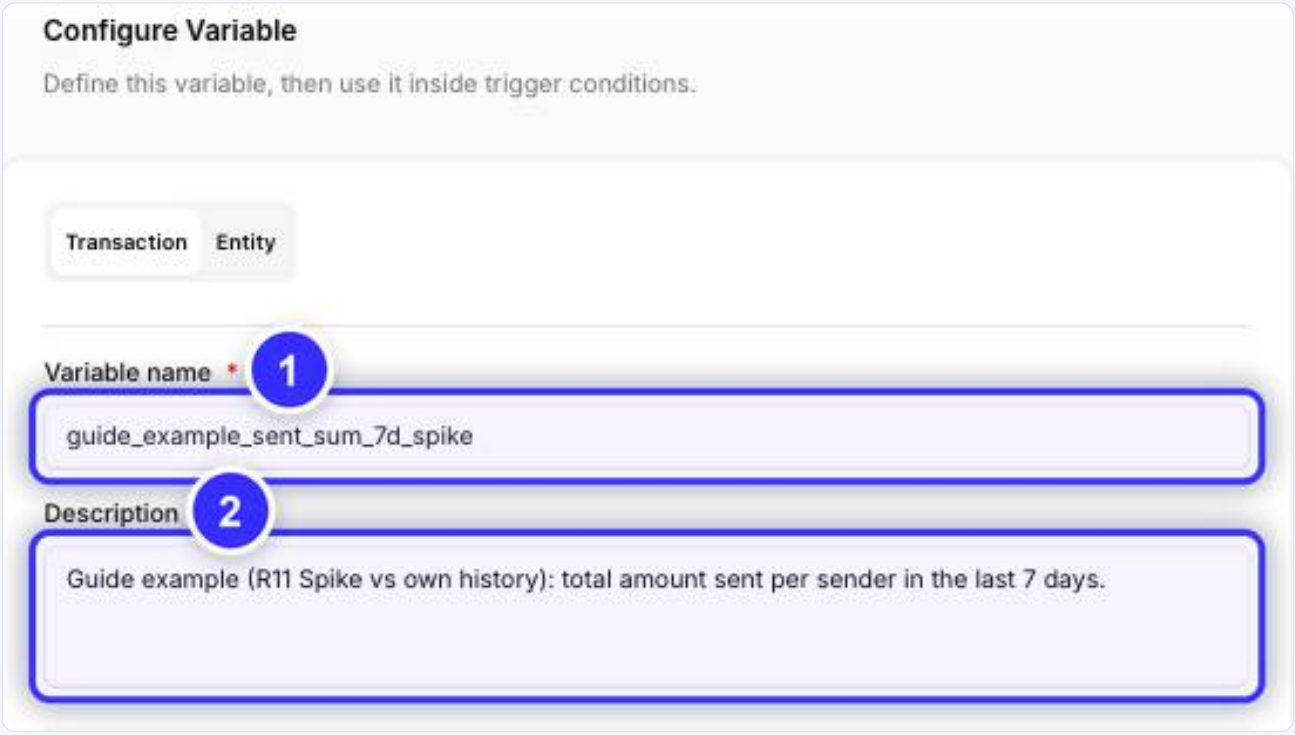


Figure 9.160 Variable A: name and description

Step 2 **Choose amount and Sum**

Open **Field** and choose `amount`. Open **Function** and choose **Sum**. Then open **Group by** and choose `sender_entity_id`, as in Rule 7.

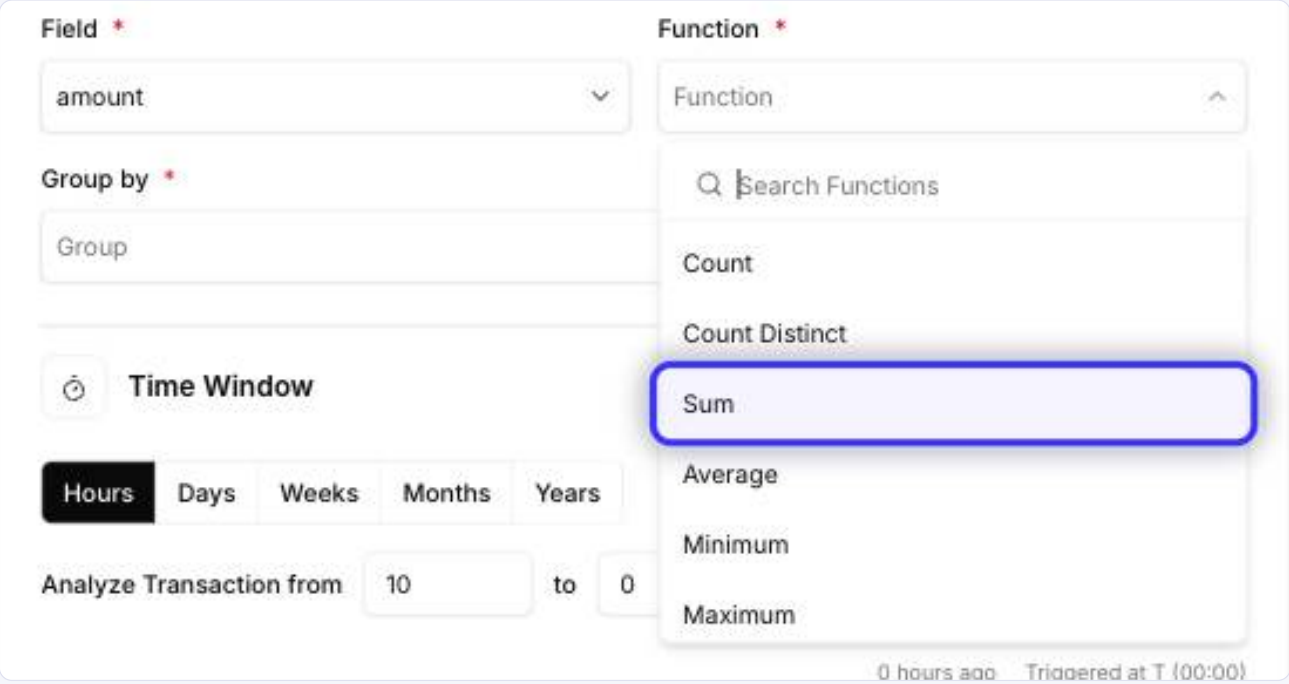


Figure 9.161 Variable A: Function Sum

Step 3 **Set the window: Days, 7 to 0, and save**

Scroll down. Click **Days** (1); the default is **Hours**. Enter 7 in **Analyze Transaction from** and 0 in **to** (2): the 7 days up to the trigger time T. Leave the blank row under **Filters (1)** (3) empty: a blank row is dropped when you save. Click **Save Variable** (4).

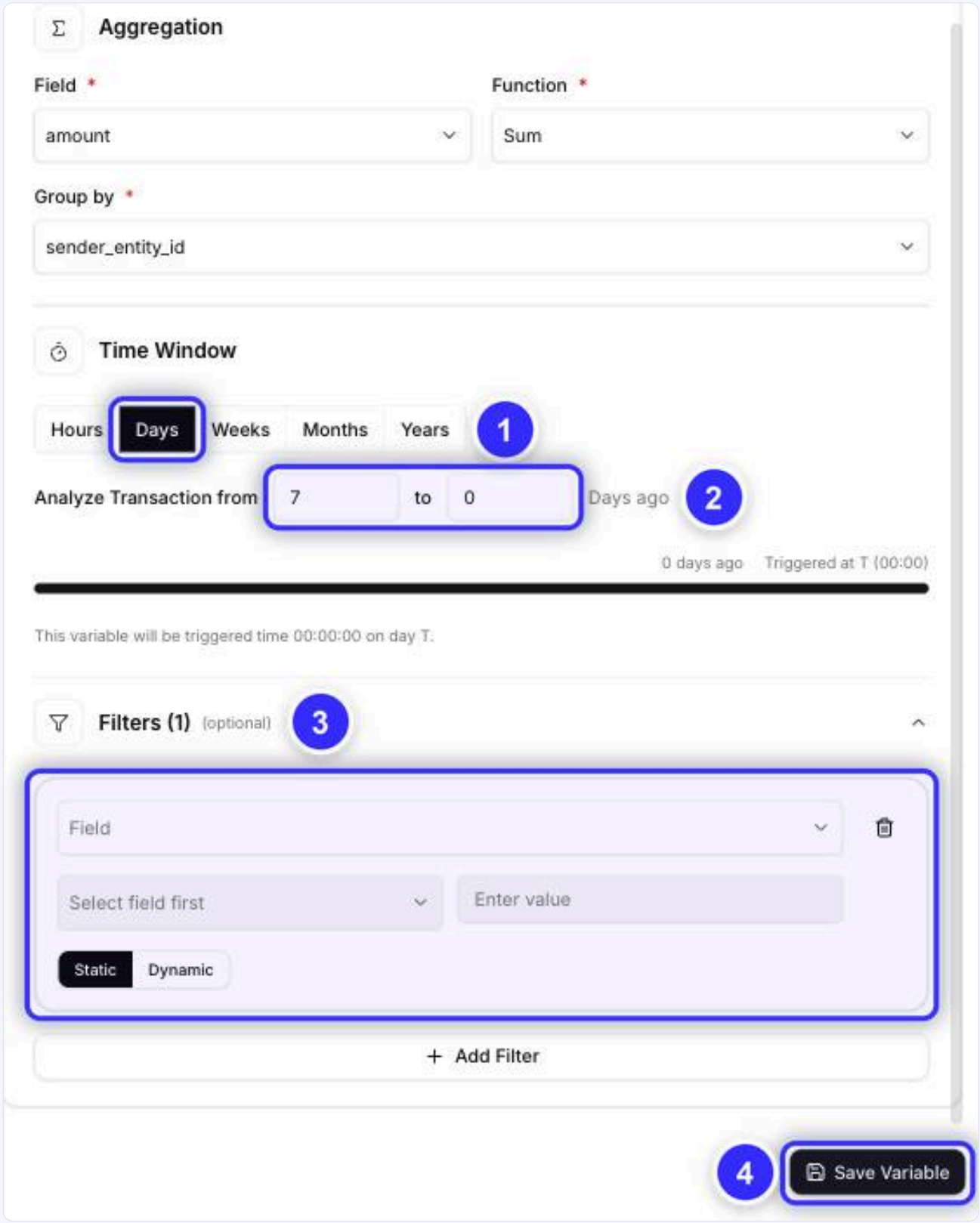


Figure 9.162 Variable A: window 7 to 0 Days ago and Save Variable

Step 4 **Check variable A**

The variable is listed as VAR-08102026-000798. Click the row. **View Variable** shows the type tag **NUM_AGG_SUM** (1), the **CREATED** and **UPDATED** times and user (2), `amount` / **Sum** / `sender_entity_id` (3), 7 to 0 **Days ago** (4) and **Filters (0)** (5).

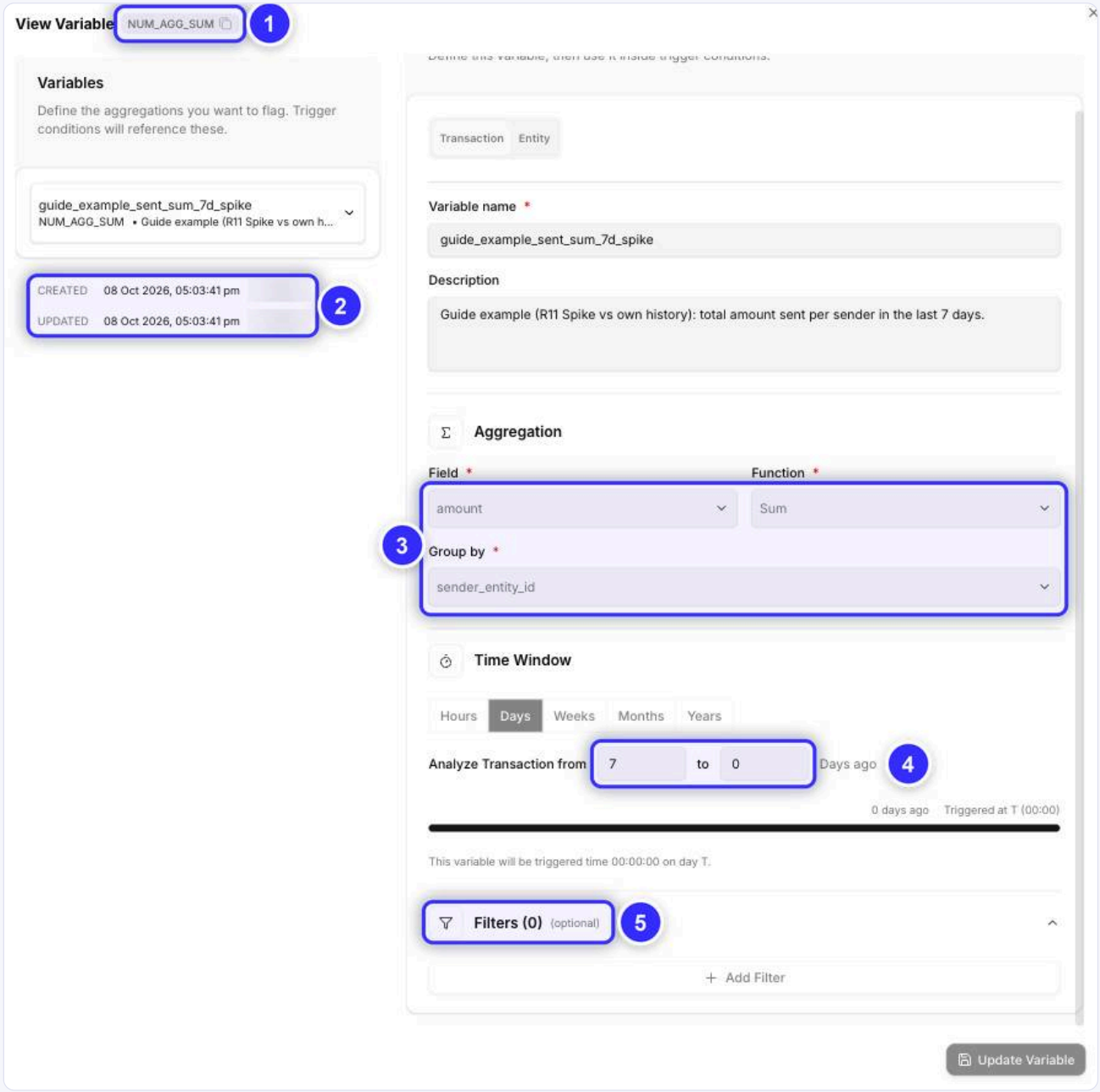


Figure 9.163 View Variable for variable A

Part B: Create variable B, the sender's own baseline

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 5 **Open the form and name variable B**

Click **+ New** again. Type `sent_sum_90d` (1) and a description such as “Total amount sent per sender in the last 90 days (the sender’s own baseline).” (2).

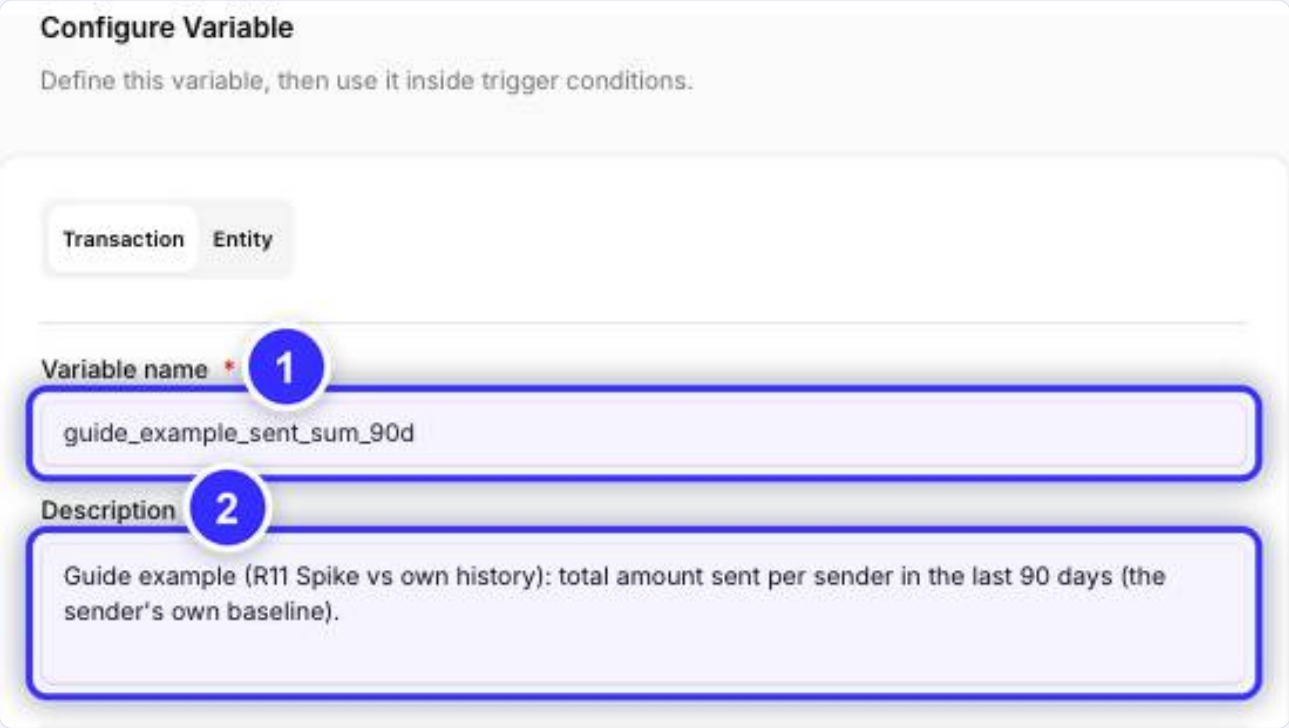


Figure 9.164 Variable B: name and description

Step 6 **Choose amount, Sum and sender_entity_id; set 90 to 0 and save**

Choose `amount`, **Sum** and `sender_entity_id`, as for variable A. Scroll down. Click **Days** (1); the default is **Hours**. Enter 90 in **Analyze Transaction from** and 0 in **to** (2): the 90 days up to the trigger time T. Leave the blank row under **Filters (1)** (3) empty: a blank row is dropped when you save. Click **Save Variable** (4).

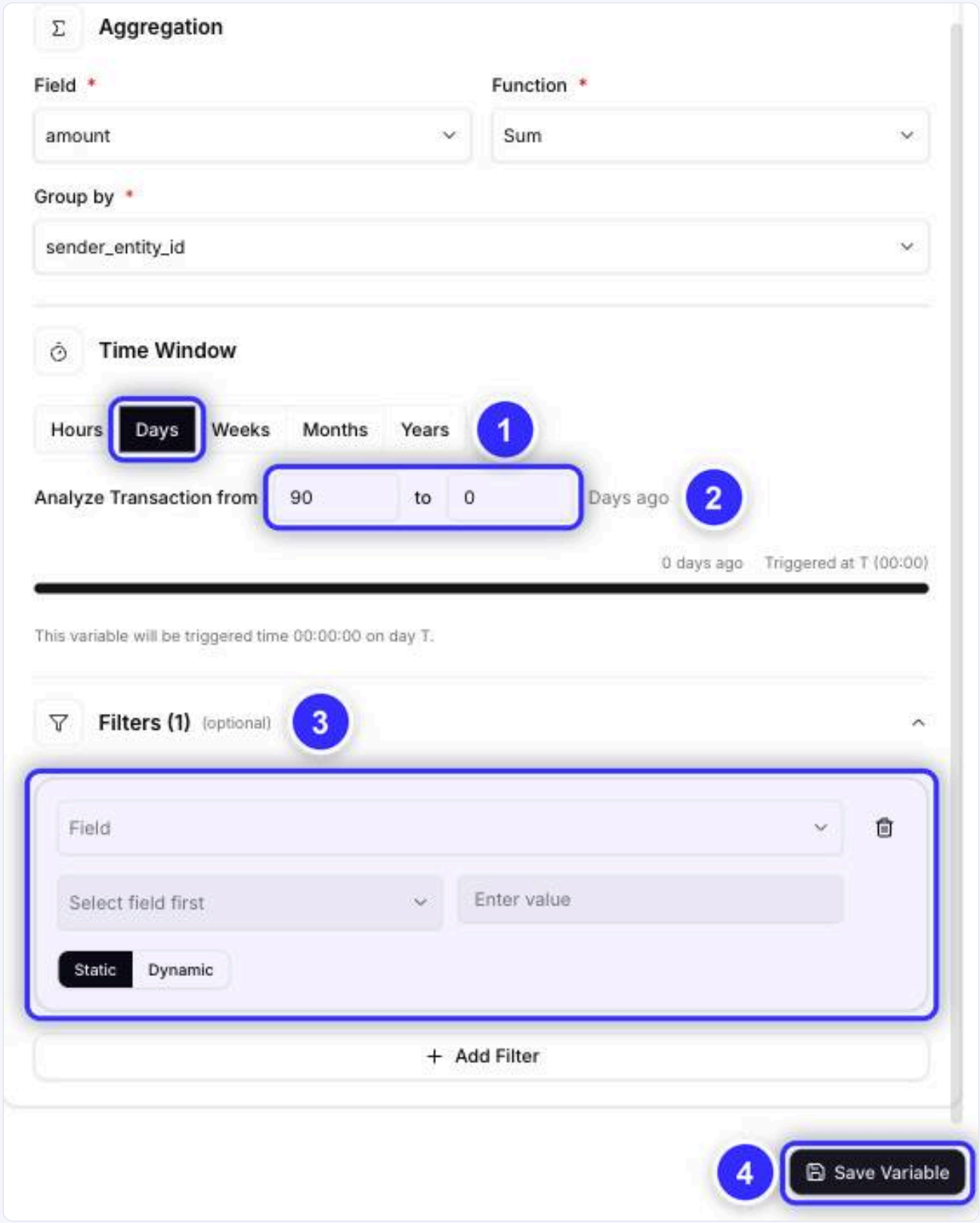


Figure 9.165 Variable B: window 90 to 0 Days ago and Save Variable

Step 7 **Find variable B in the list**

Variable B is the first row, here VAR-08102026-000799.

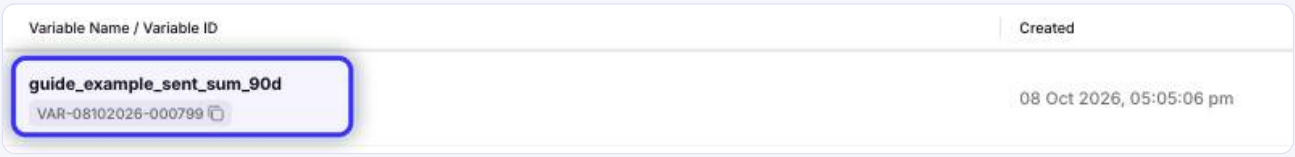


Figure 9.166 Variable B in the Variables list

Step 8 **Check variable B**

Click the row. **View Variable** shows the type tag **NUM_AGG_SUM** (1), the **CREATED** and **UPDATED** times and user (2), `amount` / **Sum** / `sender_entity_id` (3), 90 to 0 **Days ago** (4) and **Filters (0)** (5).

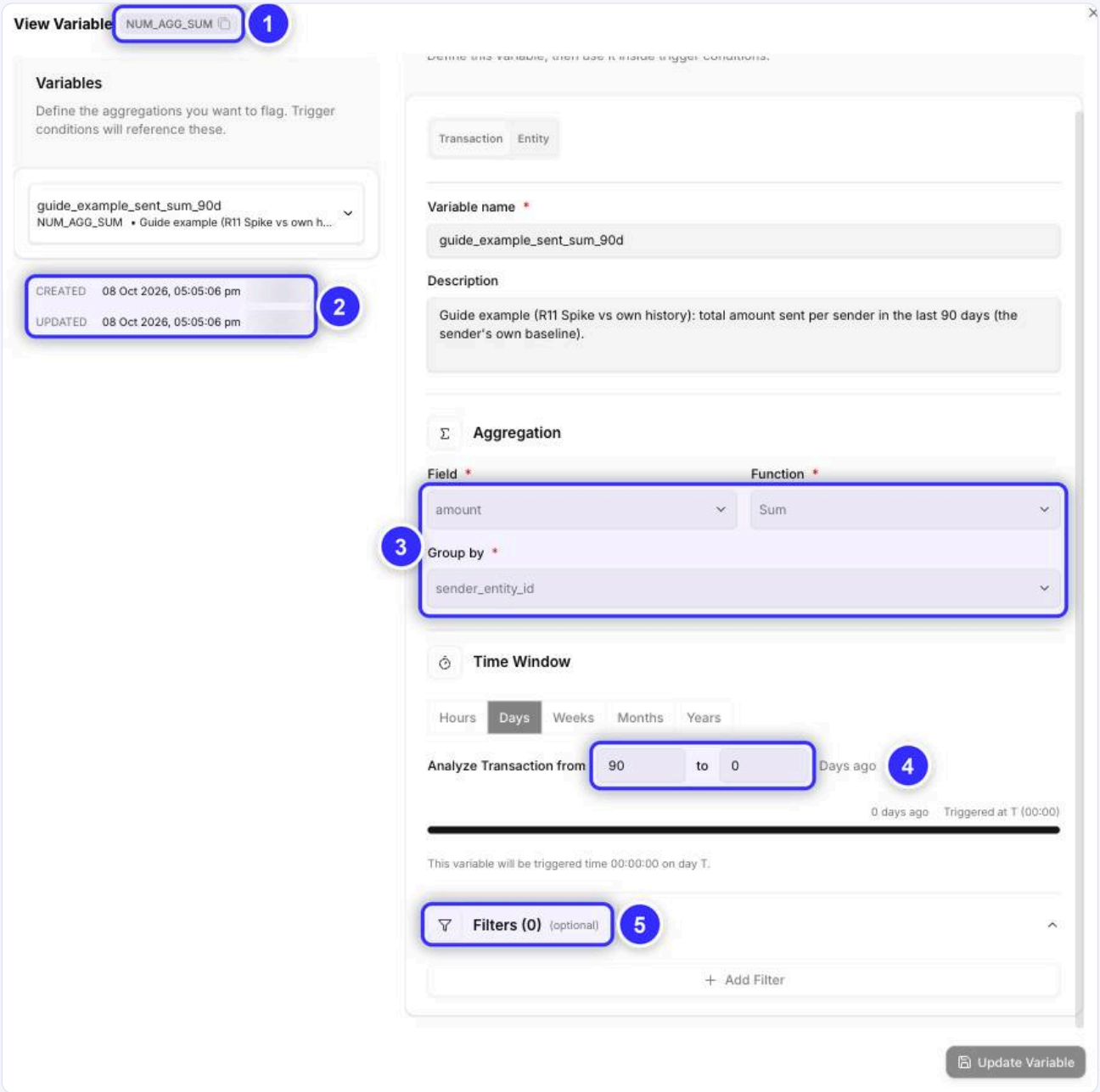


Figure 9.167 View Variable for variable B

Part C: Create the typology

Fyscal ARCX → Transaction Monitoring → Typology → + New

Step 9 **Fill in the details; keep the name to 100 characters**

Click **+ New** on **Typology**. Set **Suppression Window** to 7 **Day**, write a description, and in **Typology type** search `TP103` and click **Anomaly**. Names are limited to 100 characters: the first name tried for this example was longer, and **Next Step** stopped with "Rule name must be 3-100 characters" under **Typology Name**. The final name is `R11 Spike vs own history - PHP 100000 or more in 7 days and half of 90-day total`.

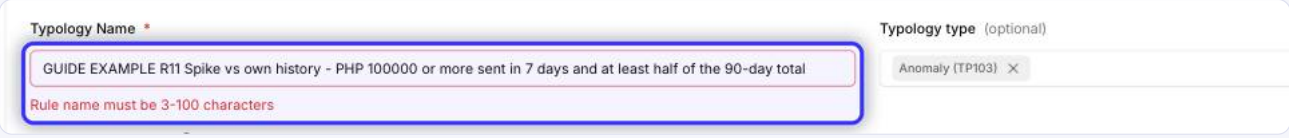


Figure 9.168 A name over 100 characters: Rule name must be 3-100 characters

Step 10 **Row 1: variable A Greater Than Equal 100000**

In **Group 1**, click **Select field**, type `sent_sum` and click `sent_sum_7d_spike`. Choose **Greater Than Equal**, keep **Static Value** and type 100000.

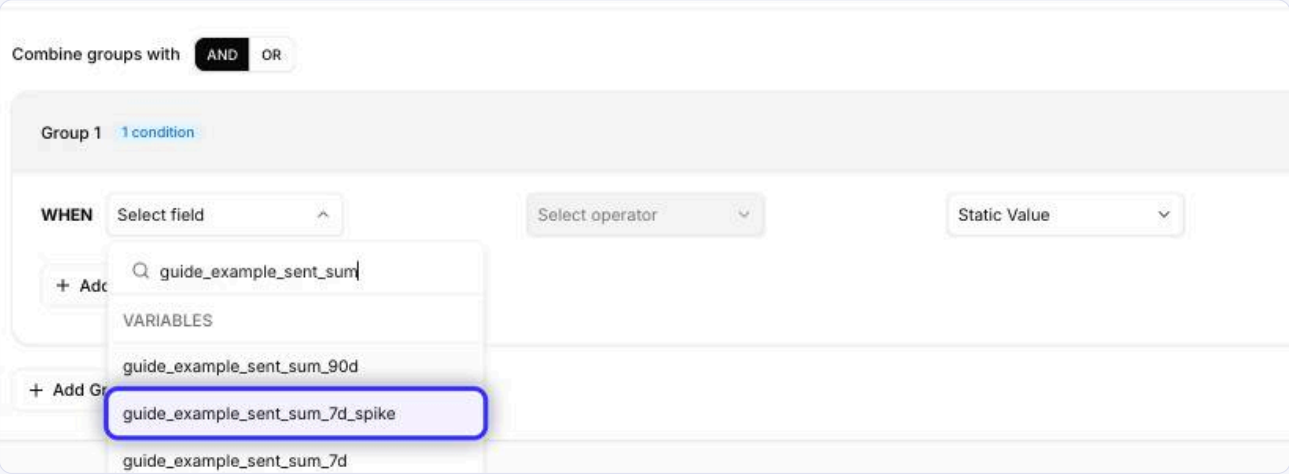


Figure 9.169 Row 1: choose variable A

Step 11 **Add row 2**

Click **Add Condition**. A second row appears, joined to the first by **AND — all must match** (1). In row 2 (2) choose `sent_sum_7d_spike` again and **Greater Than Equal**.

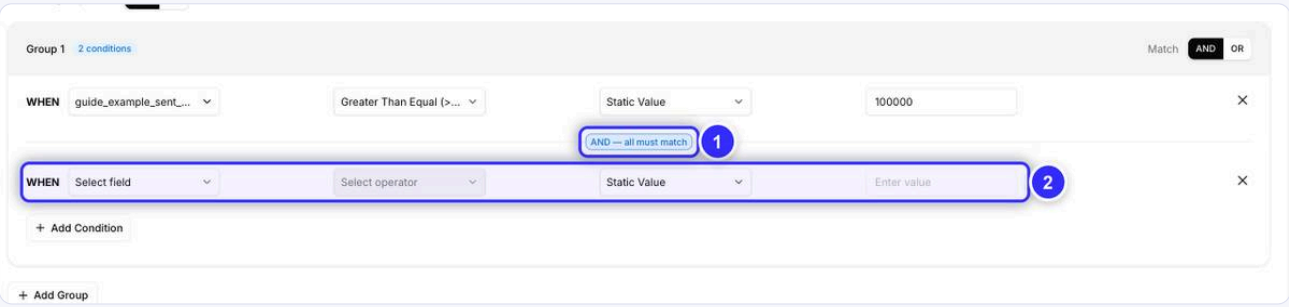


Figure 9.170 Row 2 added, joined by AND — all must match

Step 12 **Row 2: compare with variable B**

In row 2 open the compare-to list and choose **Variable** (1). **Select variable** (2) lists the variables, newest first, without a search box and without the row's own variable. Choose `sent_sum_90d`.



Figure 9.171 Row 2: compare with a Variable, the Select variable list

Step 13 **Enter the multiplier 0.5 and go to the next step**

Type 0.5 in **THAN MULTIPLIER**. Row 2 now means "the 7-day total is at least half of the 90-day total". Check the name (1), **Anomaly (TP103)** (2), **7 Day** (3), row 1 (4) and row 2 (5), then click **Next Step** (6).

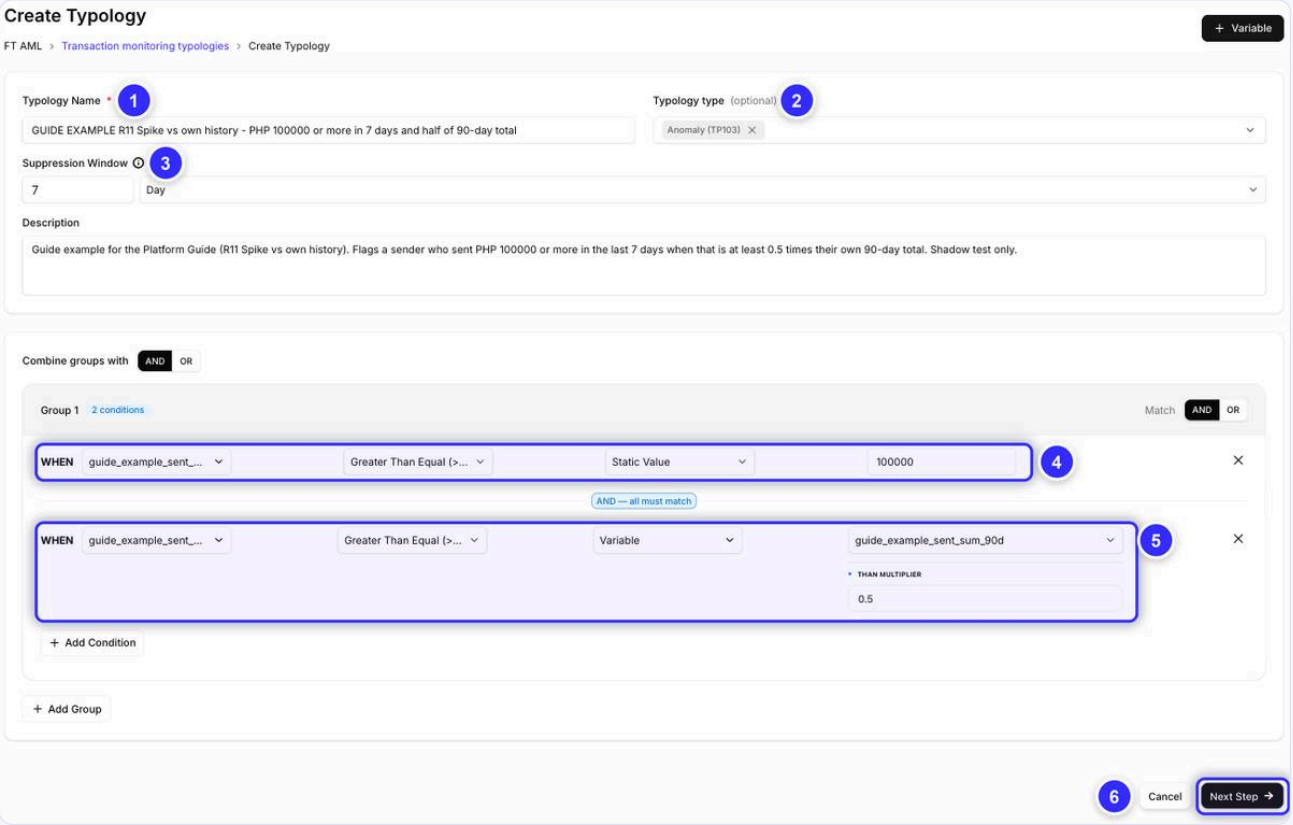


Figure 9.172 The completed Rule 9 page with two conditions

Part D: Choose the schedule and save

Step 14 **Select the shared schedule and save the draft**

Open **Select Schedule**, search for `schedule_2027`, click it and click **Save as Draft**, as in Rule 7.

Step 15 **Check the saved draft**

The page becomes **Update Typology** (1) with the schedule (2), the run sentence (3), **Update** (4), **Dry Run** (5) and **Activate** (6).

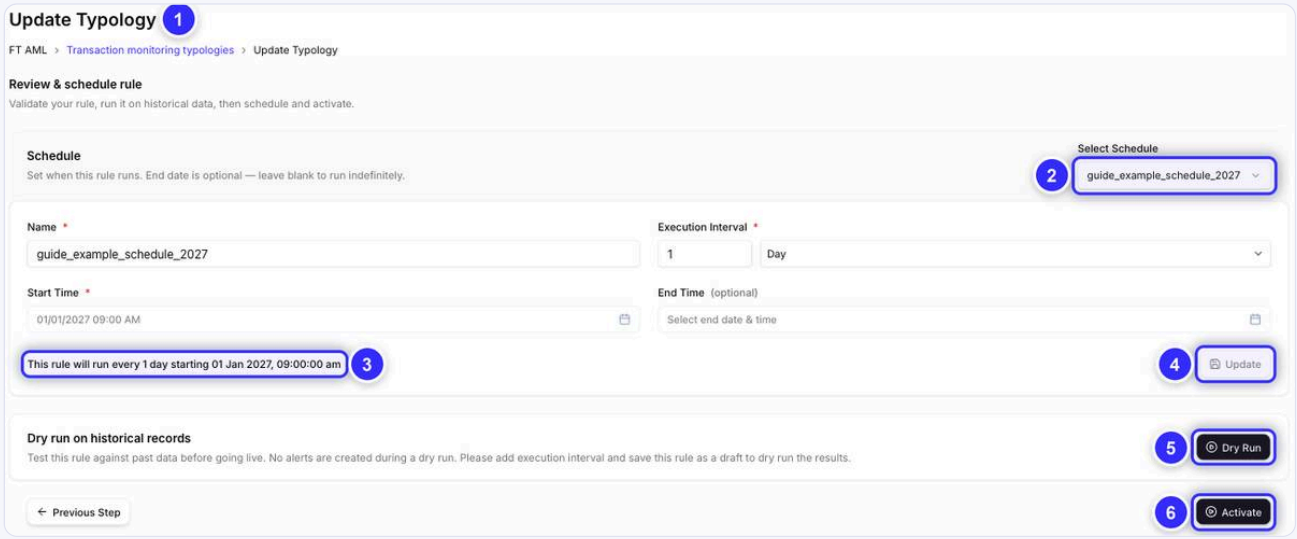


Figure 9.173 Rule 9 after Save as Draft

Step 16 **Check the rule page**

The rule page shows **Draft** TMR-08102026-001133 (1), **SUPPRESSION** 7Day and **TYPOLOGY** Anomaly (2), both conditions, the second reading "sent_sum_90d (multiplied by 0.5)" (3), and both variable cards, in last 90 day and in last 7 day (4).

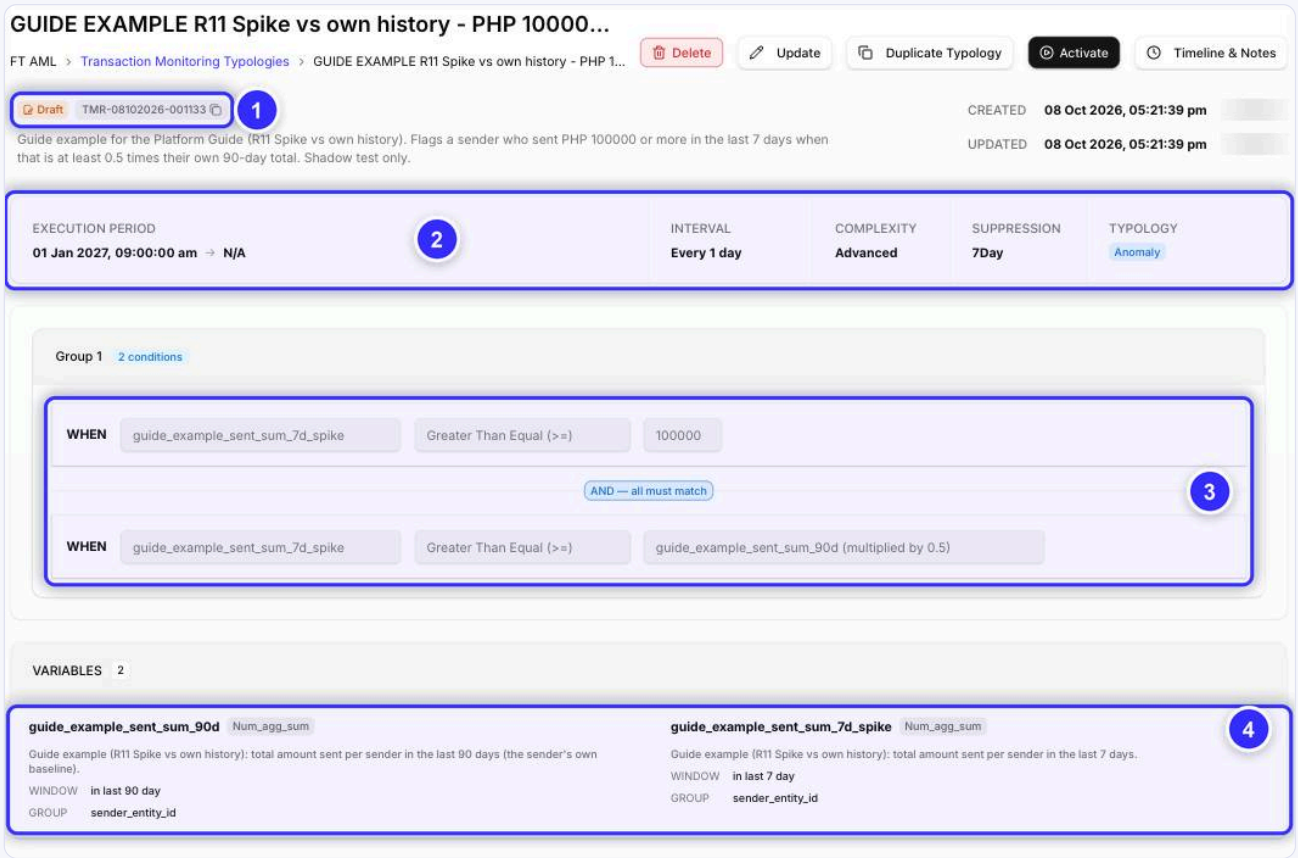


Figure 9.174 The saved Rule 9 as a Draft, TMR-08102026-001133

How it evaluates. The 90-day total includes the last 7 days. Sender A sent ₱150,000 in the last 7 days and ₱200,000 in 90 days: ₱150,000 >= 100000 and ₱150,000 >= 0.5 × ₱200,000, so the rule alerts. Sender B sent ₱150,000 in 7 days but ₱1,000,000 in 90 days: ₱150,000 is below ₱500,000, no alert. Sender C sent ₱40,000 in 7 days and ₱50,000 in 90 days: row 1 fails, no alert.

Dry-run result. In testing, the rule created 42 alerts at its real thresholds: 0, 6, 16 and 20 across the four windows, newest first.

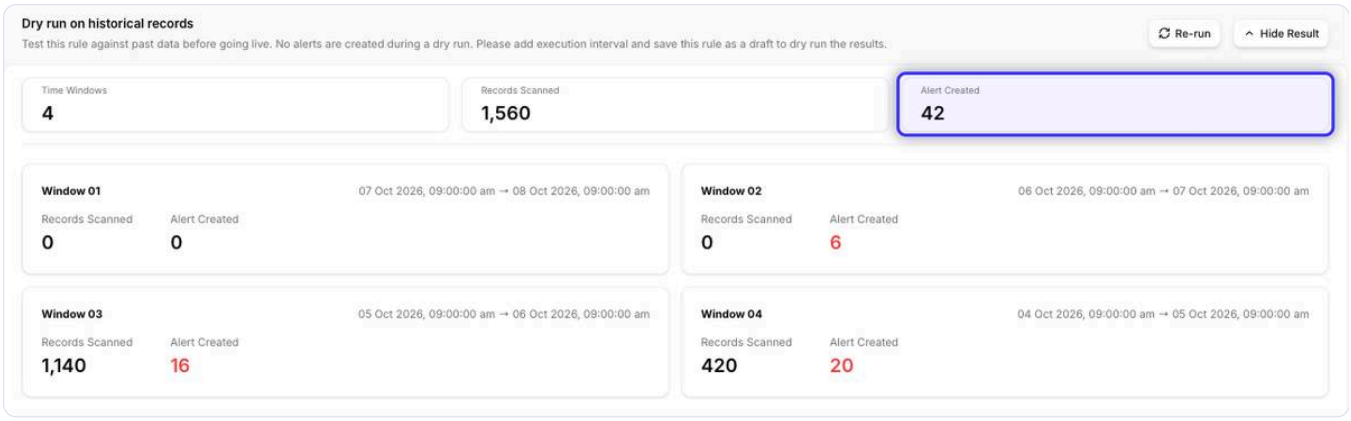


Figure 9.175 Rule 9 dry run: 42 alerts

Tuning. Raise the minimum (100000) to ignore small spikes, and change the multiplier: 0.5 means half of the 90-day total; 0.3 is broader. Keep both variables grouped by `sender_entity_id` so they describe the same sender.

Rule 10 · Many devices

RED FLAG **One account used from many devices**

LOGIC

Counts the different devices (sender_device_id) the sender used in the last 7 days.

WINDOW

7 to 0 Days

THRESHOLD

≥ 3 devices

✓ Verified by positive control

What it detects and why. This rule flags a sender who used 3 or more different devices in 7 days. A customer account operated from many devices can mean that others are using it, as with a shared or rented mule account.

Item	Setting
Variable **`distinct_devices_7d`**	**Count Distinct** of `sender_device_id`, grouped by `sender_entity_id`, **Days** from 7 to 0, no filters
Typology type	Anomaly (TP103)
Suppression Window	7 Day
Condition	Group 1, Match AND: `distinct_devices_7d` **Greater Than Equal (>=)** Static Value 3
Schedule	Existing `schedule_2027` (created in Rule 1): every 1 Day, starting 09 Oct 2026, 09:00 AM, no end time

Part A: Create the variable

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 1 **Open the form and name the variable**

Click **+ New** on **Variables** and leave **Transaction** selected. Type `distinct_devices_7d` in **Variable name** (1) and a description such as “Number of distinct sender devices per sender in the last 7 days.” (2).

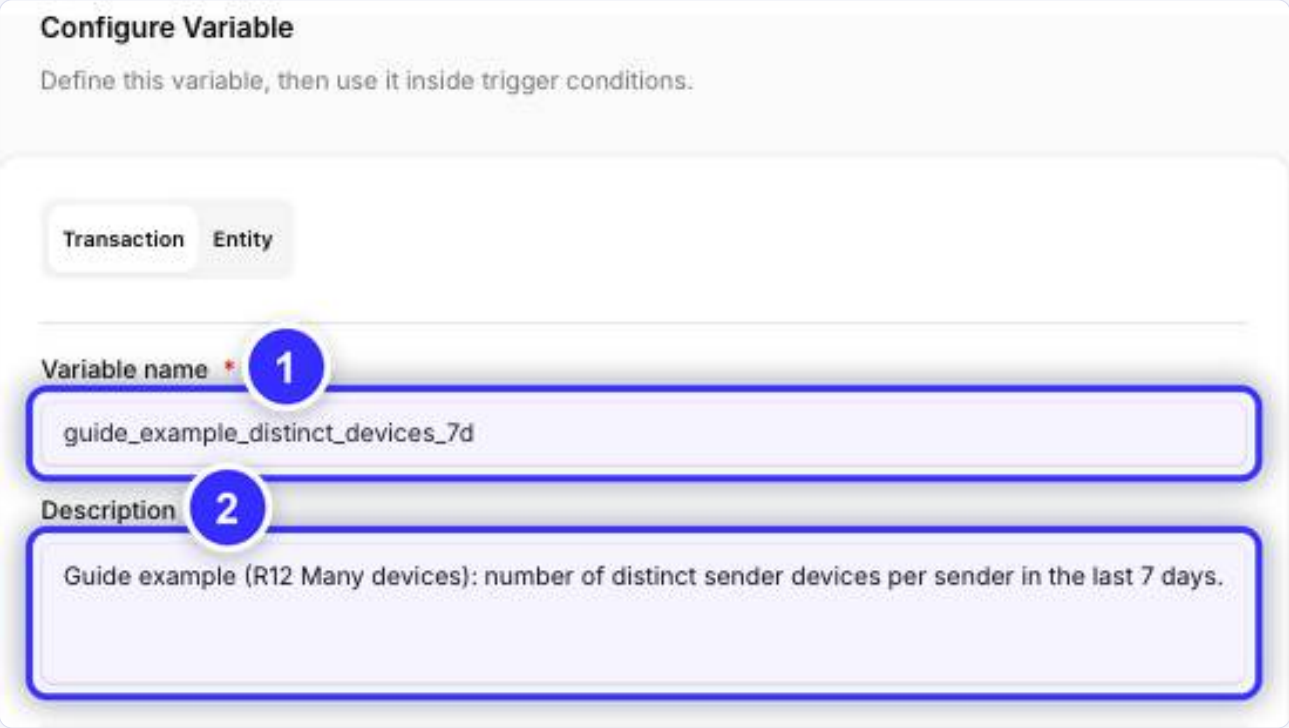


Figure 9.176 Rule 10 variable: name and description

Step 2 **Choose the Field: sender_device_id**

Open **Field** and type `device`. Two fields match, `receiver_device_id` and `sender_device_id`. Choose `sender_device_id`.

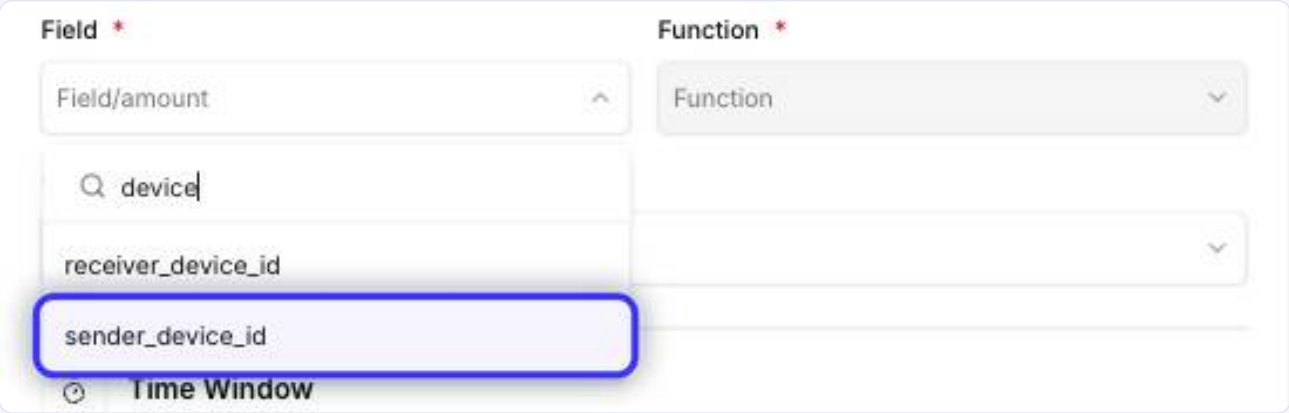


Figure 9.177 Field search for device: choose sender_device_id

Step 3 **Choose the Function: Count Distinct**

Open **Function**. For an ID or text field the list offers **Count**, **Count Distinct**, **Minimum** and **Maximum**. Choose **Count Distinct**: each different value is counted once.

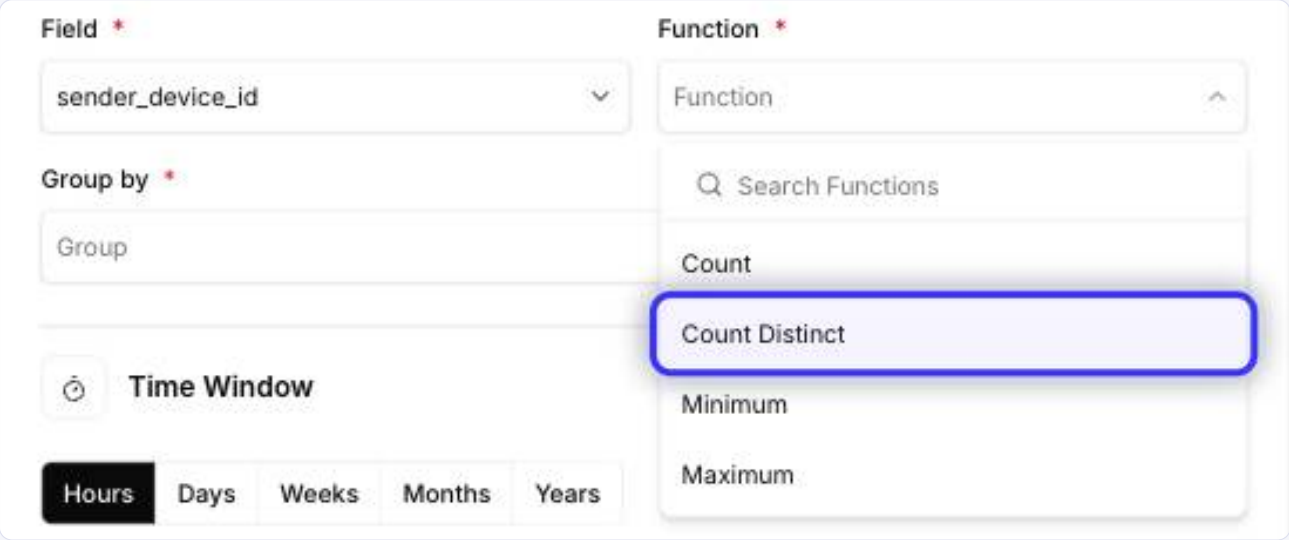


Figure 9.178 Function: Count Distinct

Step 4 **Choose Group by: sender_entity_id**

Open **Group by**, type `sender_entity` in **Search Fields** and choose `sender_entity_id`, so the count is calculated separately for each sender.



Figure 9.179 Group by search: sender_entity_id

Step 5 **Set the time window: Days, 7 to 0, and save**

Scroll down. Click **Days** (1); the default is **Hours**. Enter 7 in **Analyze Transaction from** and 0 in **to** (2): the 7 days up to the trigger time T. Leave the blank row under **Filters (1)** (3) empty: a blank row is dropped when you save. Click **Save Variable** (4).

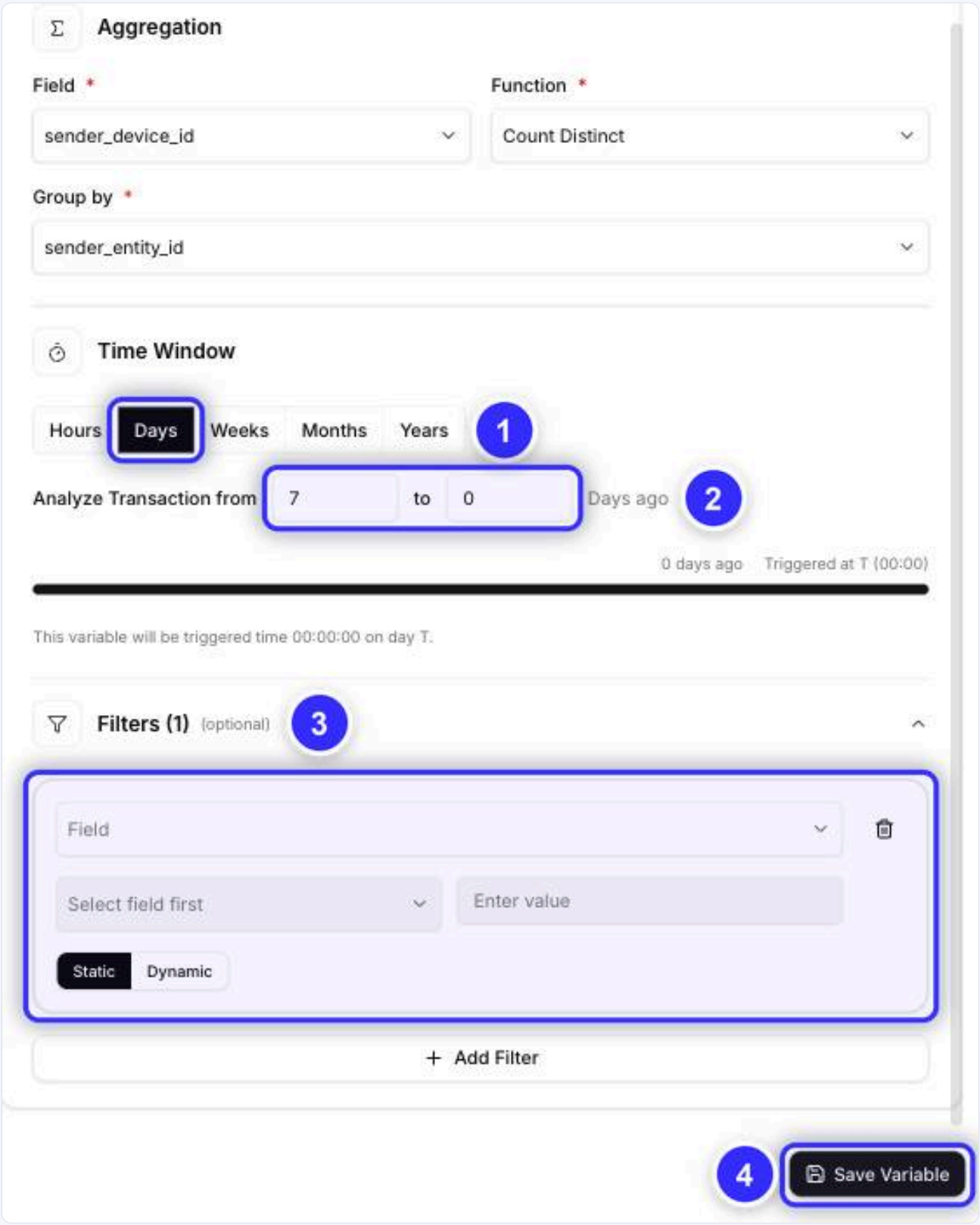


Figure 9.180 Time window 7 to 0 Days ago, blank filter row and Save Variable

Step 6 **Find the variable in the list**

The dialog closes and the variable is the first row of the **Variables** list, here VAR-08102026-000800.

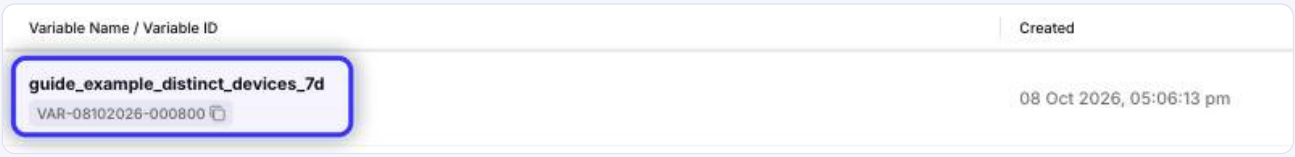


Figure 9.181 Rule 10 variable in the Variables list

Step 7 **Check the saved variable**

Click the row. **View Variable** shows the type tag **STR_AGG_COUNT_DISTINCT** (1), the **CREATED** and **UPDATED** times and user (2), `sender_device_id` / **Count Distinct** / `sender_entity_id` (3), 7 to 0 **Days ago** (4) and **Filters (0)** (5).

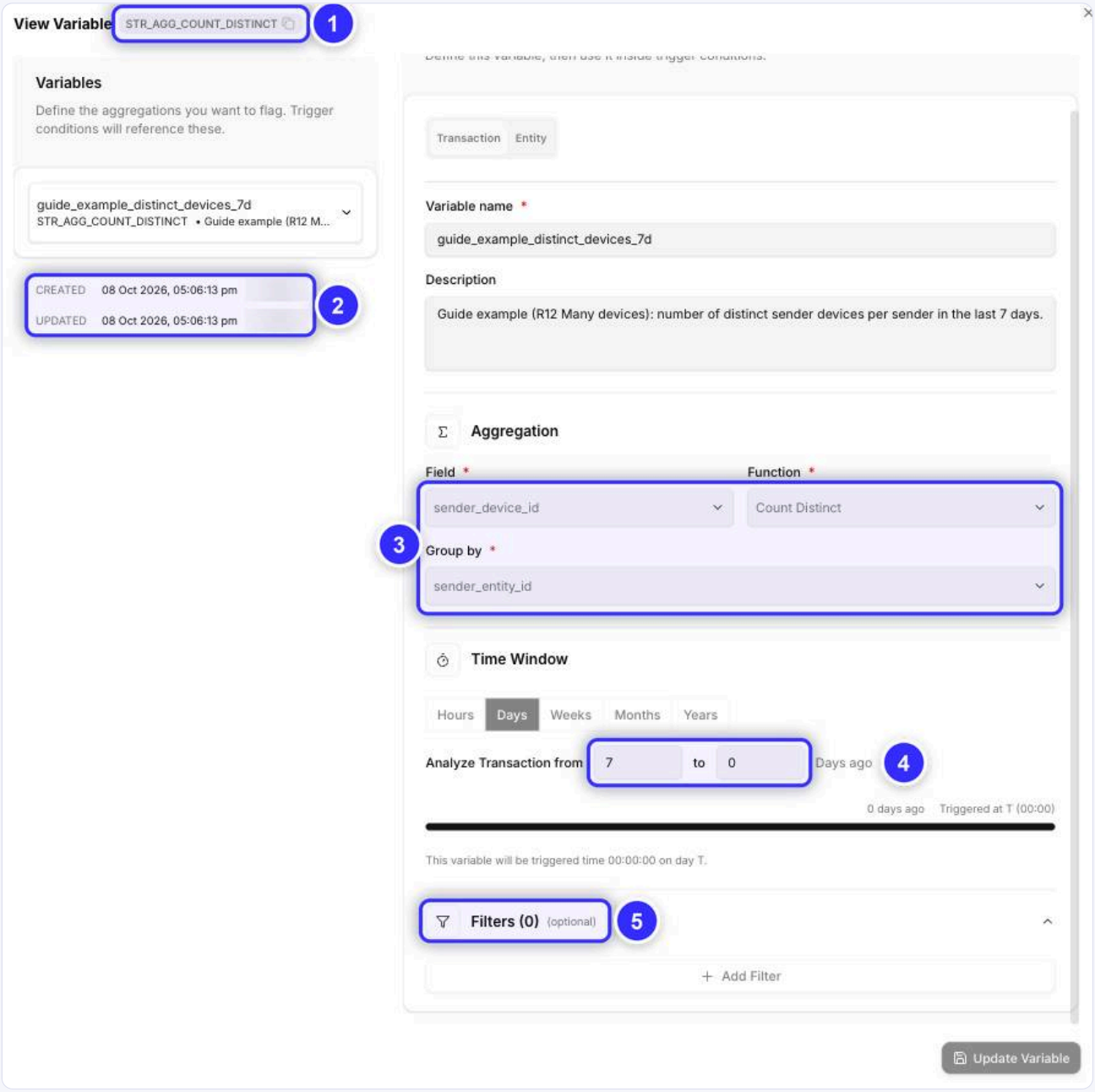


Figure 9.182 View Variable for distinct_devices_7d

Part B: Create the typology

Fyscal ARCX → Transaction Monitoring → Typology → + New

Step 8 **Fill in the details and choose Anomaly**

Click **+ New** on **Typology**. Type the name `R12 Many devices - 3 or more sender devices in 7 days` (1). Set **Suppression Window** to 7 and choose **Day** (2): it matches the 7-day window. Write a description (3). Open **Typology type** (4), type `TP103` and click **Anomaly TP103**.

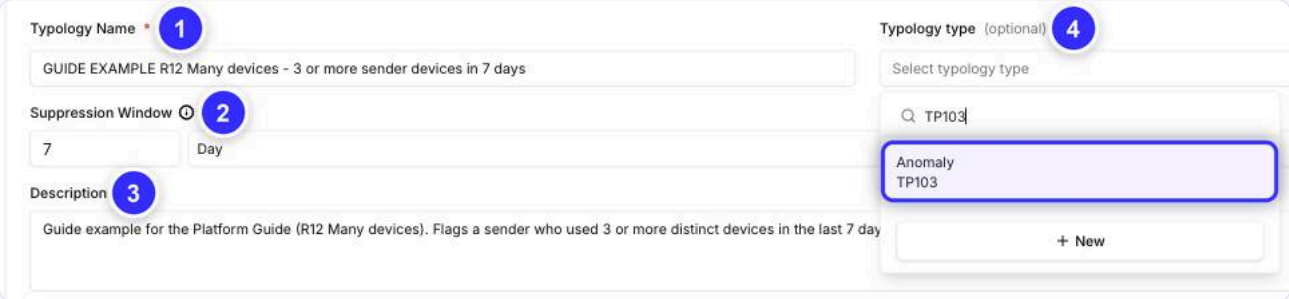


Figure 9.183 Rule 10 details and the Typology type search

Step 9 **Choose the variable in row 1**

In **Group 1**, click **Select field** next to **WHEN**, type part of the name and click `distinct_devices_7d` .

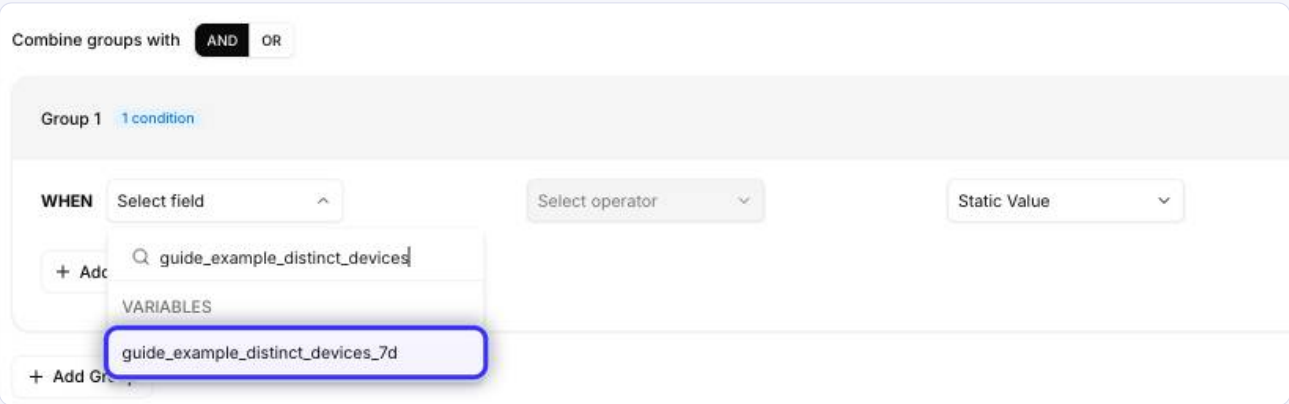


Figure 9.184 Rule 10 row 1: variable search

Step 10 **Choose Greater Than Equal and keep Static Value**

Open **Select operator** and choose **Greater Than Equal**. Keep **Static Value** in the compare-to list: the threshold is a fixed number.

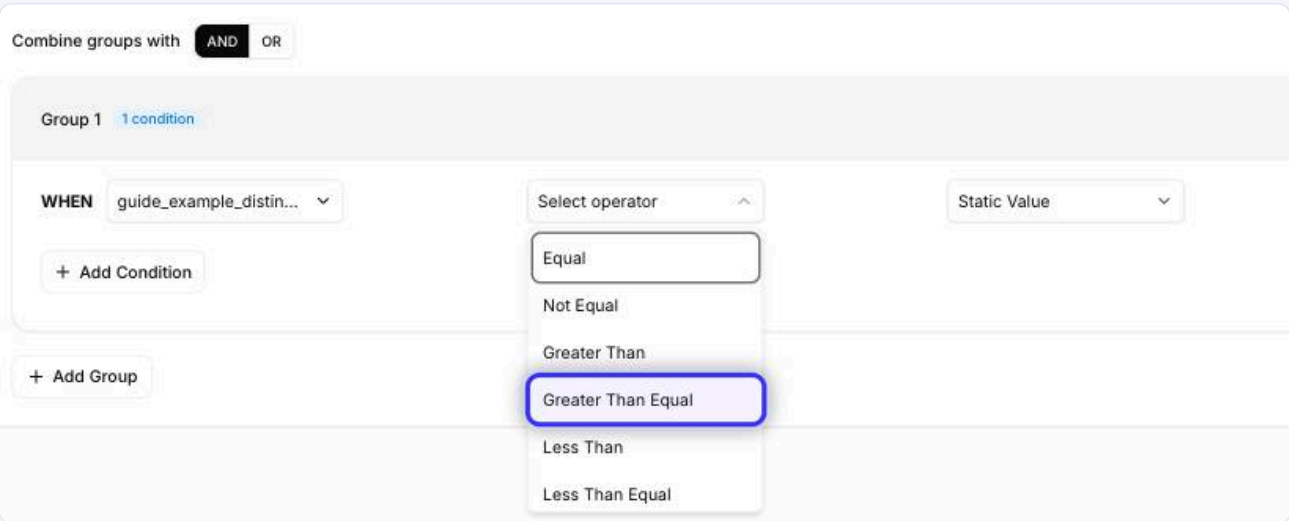


Figure 9.185 Rule 10 row 1: operator list

Step 11 **Enter 3 and go to the next step**

Type 3 in **Enter value**. Check the name (1), the type chip **Anomaly (TP103)** (2), **7 Day** (3), the description (4), **Match** AND (5) and the row (6). Click **Next Step** (7).

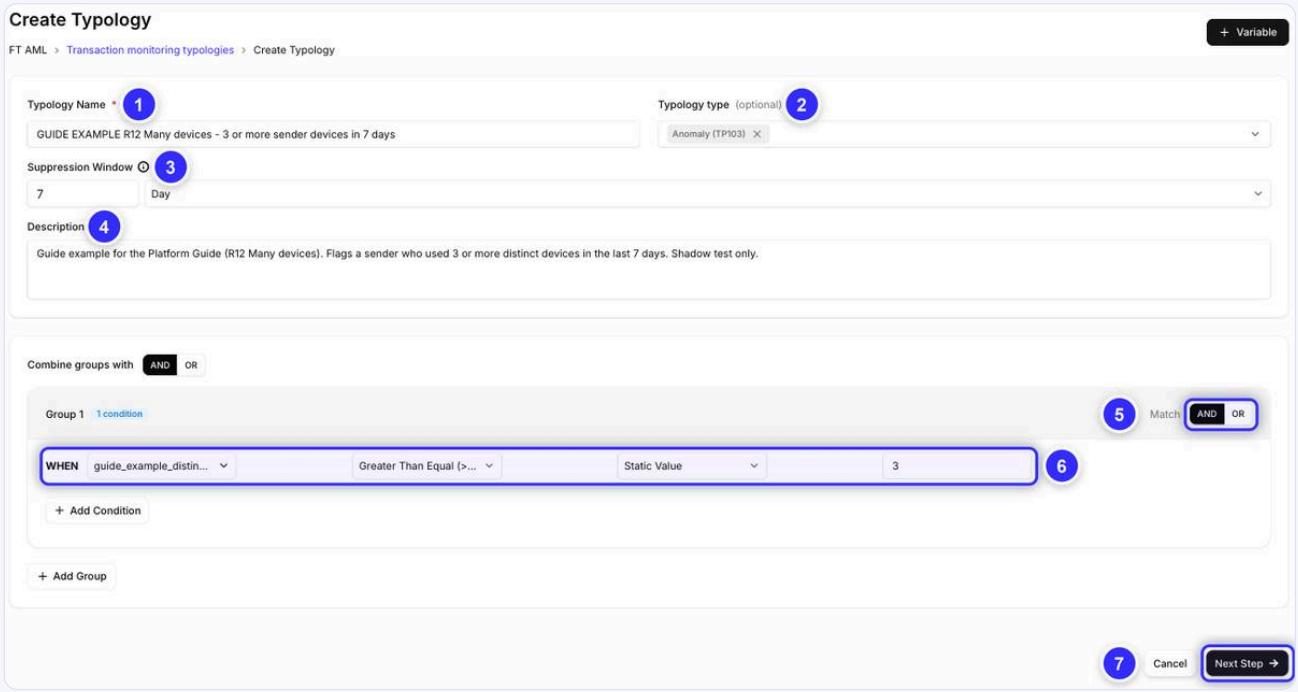


Figure 9.186 The completed Rule 10 page

Part C: Choose the schedule and save

Step 12 **Select the shared schedule and save the draft**

On **Review & schedule rule**, open **Select Schedule**, search for `schedule_2027`, click it and click **Save as Draft**, as in Rule 7.

Step 13 **Check the saved draft**

Wait a few seconds: the page becomes **Update Typology** (1) with the schedule (2), the run sentence (3), **Update** (4), **Dry Run** (5) and **Activate** (6). The screenshot shows the start in force when it was taken (01 Jan 2027).

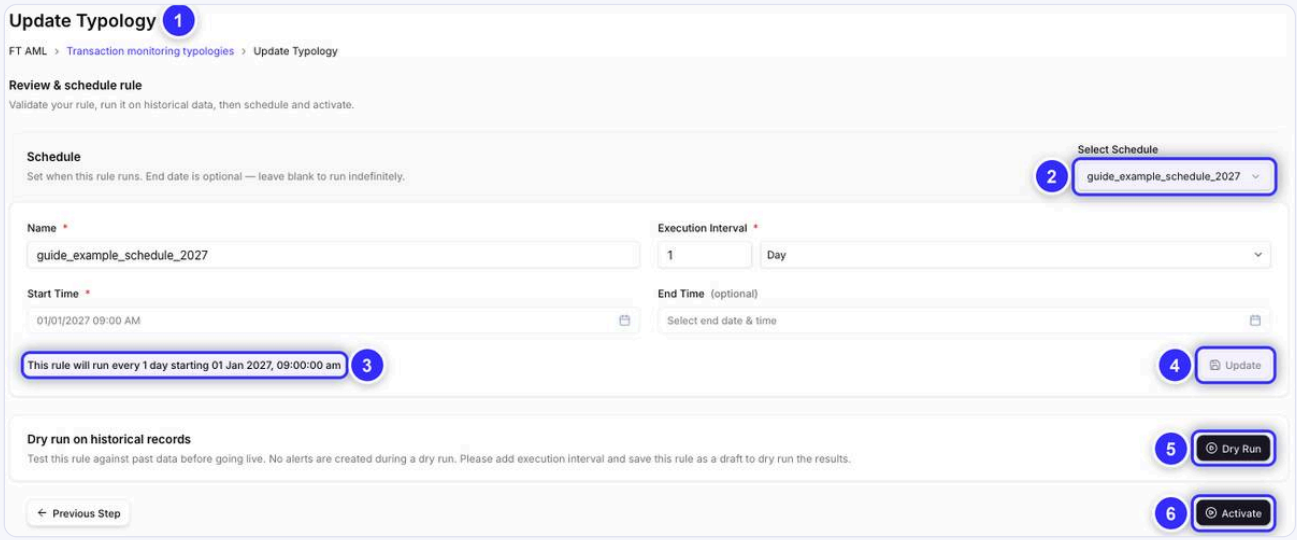


Figure 9.187 Rule 10 after Save as Draft

Step 14 **Check the rule page**

Open the rule from **Transaction Monitoring → Typology**. It shows **Draft** and the rule ID TMR-08102026-001134, created 08 Oct 2026, 05:24:06 pm (1); the summary with **INTERVAL** Every 1 day, **SUPPRESSION** 7Day and **TYPOLOGY** Anomaly (2); the condition, with the operator shown as **NUM_GTE (>=)** (3); and the variable card `distinct_devices_7d`, Str_agg_count_distinct, **WINDOW** in last 7 day, **GROUP** `sender_entity_id` (4).

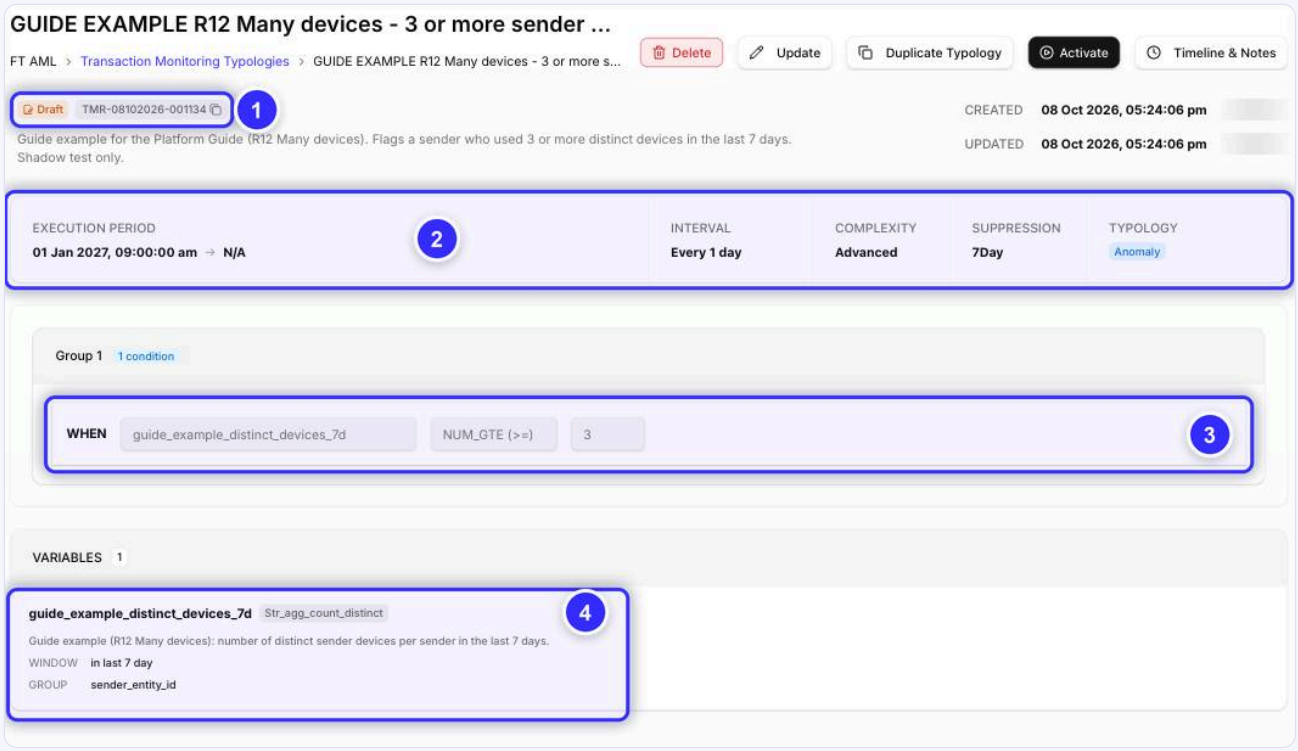


Figure 9.188 The saved Rule 10 as a Draft, TMR-08102026-001134

How it evaluates. Sender A sent 6 payments in 7 days from 4 different devices: 4 >= 3, alert. Sender B sent 40 payments from the same 2 devices: 2, no alert.

Dry-run result. In testing, the rule created 0 alerts at its real threshold (>= 3) in all four windows: in the test data each sender used 1 or 2 devices. To prove the rule works, the threshold was lowered to >= 1 for one dry run. That created 4,043 alerts (1,046 / 1,059 / 1,061 / 877 by window, newest first), then the threshold was restored and a new dry run returned 0 again. See Test a typology with Dry Run for the method.

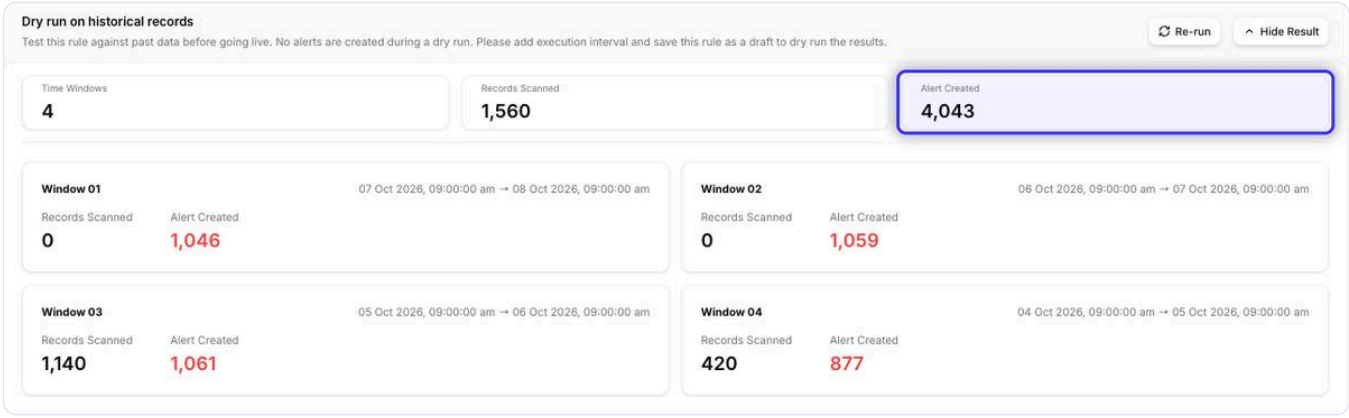


Figure 9.189 Rule 10 positive control (threshold temporarily >= 1): 4,043 alerts

Tuning. Set the number of devices from what is normal for your customers; a household or a business may use several. Keep the **Suppression Window** at least as long as the window.

Rule 11 · Many IP addresses

RED FLAG **One account used from many network locations**

LOGIC

Counts the different IP addresses (sender_ip) the sender used in the last 7 days.

WINDOW THRESHOLD

7 to 0 Days ≥ 15 IP addresses

✓ Verified · 120 alerts

What it detects and why. This rule flags a sender who used 15 or more different IP addresses in 7 days. Logging in from many network locations in a short time can mean the account is being operated by several people or through changing connections.

Item	Setting
Variable `distinct_ips_7d`	**Count Distinct** of `sender_ip`, grouped by `sender_entity_id`, **Days** from 7 to 0, no filters
Typology type	Anomaly (TP103)
Suppression Window	7 Day
Condition	Group 1, Match AND: `distinct_ips_7d` **Greater Than Equal (>=)** Static Value 15
Schedule	Existing `schedule_2027` (created in Rule 1): every 1 Day, starting 09 Oct 2026, 09:00 AM, no end time

Part A: Create the variable

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 1 **Open the form and name the variable**

Click **+ New** on **Variables** and leave **Transaction** selected. Type `distinct_ips_7d` in **Variable name** (1) and a description such as “Number of distinct sender IP addresses per sender in the last 7 days.” (2).

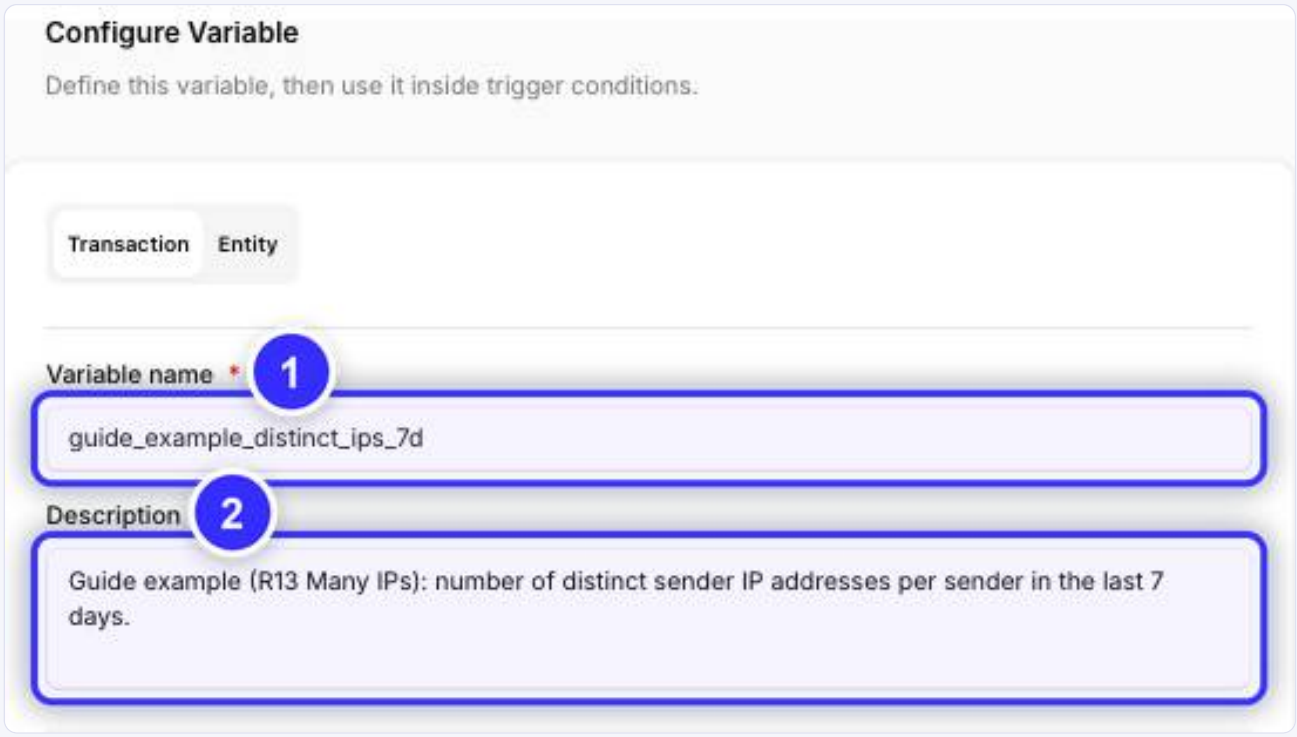


Figure 9.190 Rule 11 variable: name and description

Step 2 **Choose the Field: sender_ip**

Open **Field** and type `_ip`. Two fields match, `receiver_ip` and `sender_ip`. Choose `sender_ip`.

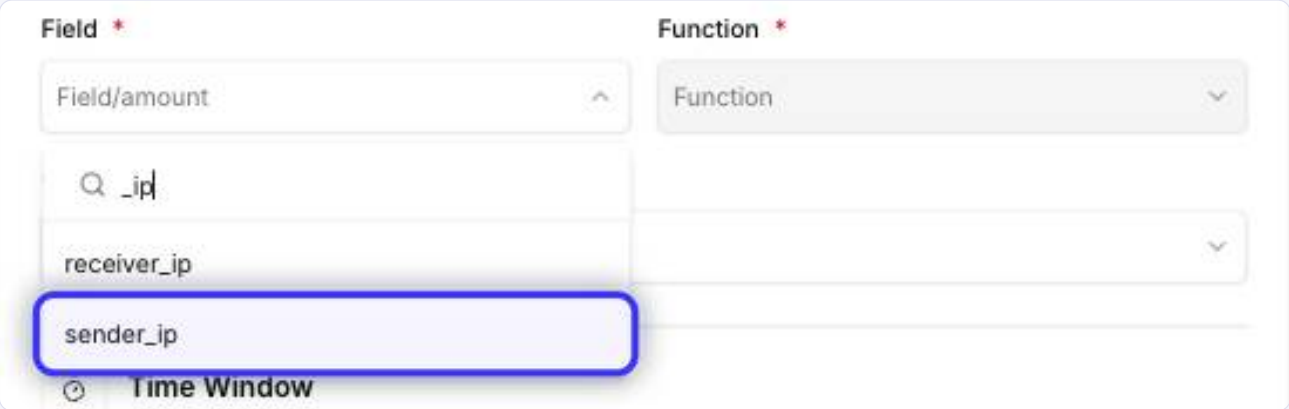


Figure 9.191 Field search for _ip: choose sender_ip

Step 3 **Choose the Function: Count Distinct**

Open **Function**. For an ID or text field the list offers **Count**, **Count Distinct**, **Minimum** and **Maximum**. Choose **Count Distinct**: each different value is counted once.

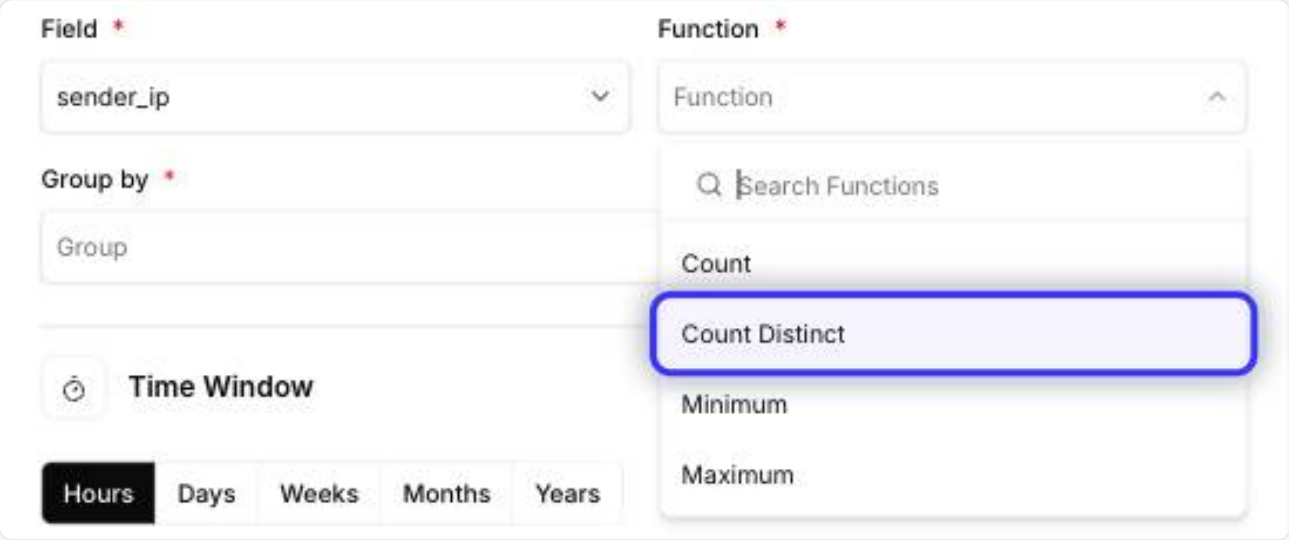


Figure 9.192 Function: Count Distinct

Step 4 **Choose Group by: sender_entity_id**

Open **Group by**, type `sender_entity` in **Search Fields** and choose `sender_entity_id`, so the count is calculated separately for each sender.



Figure 9.193 Group by search: sender_entity_id

Step 5 **Set the time window: Days, 7 to 0, and save**

Scroll down. Click **Days** (1); the default is **Hours**. Enter 7 in **Analyze Transaction from** and 0 in **to** (2): the 7 days up to the trigger time T. Leave the blank row under **Filters (1)** (3) empty: a blank row is dropped when you save. Click **Save Variable** (4).

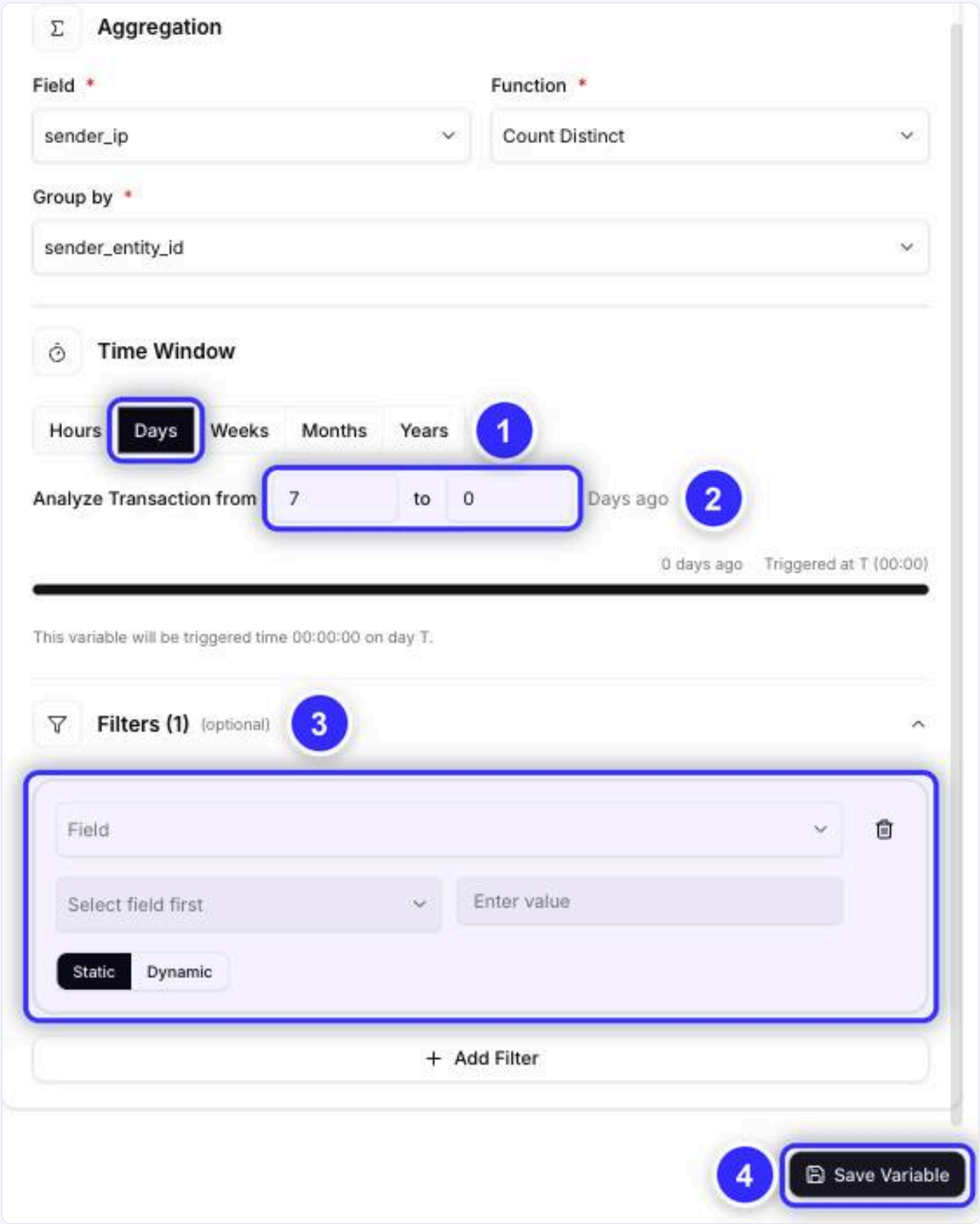


Figure 9.194 Time window 7 to 0 Days ago, blank filter row and Save Variable

Step 6 **Find the variable in the list**

The dialog closes and the variable is the first row of the **Variables** list, here VAR-08102026-000801.

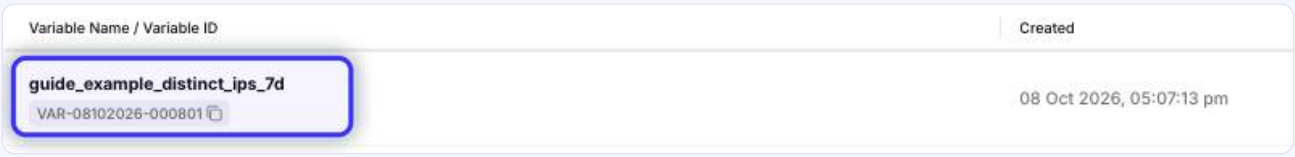


Figure 9.195 Rule 11 variable in the Variables list

Step 7 **Check the saved variable**

Click the row. **View Variable** shows the type tag **STR_AGG_COUNT_DISTINCT** (1), the **CREATED** and **UPDATED** times and user (2), `sender_ip` / **Count Distinct** / `sender_entity_id` (3), 7 to 0 **Days ago** (4) and **Filters (0)** (5).

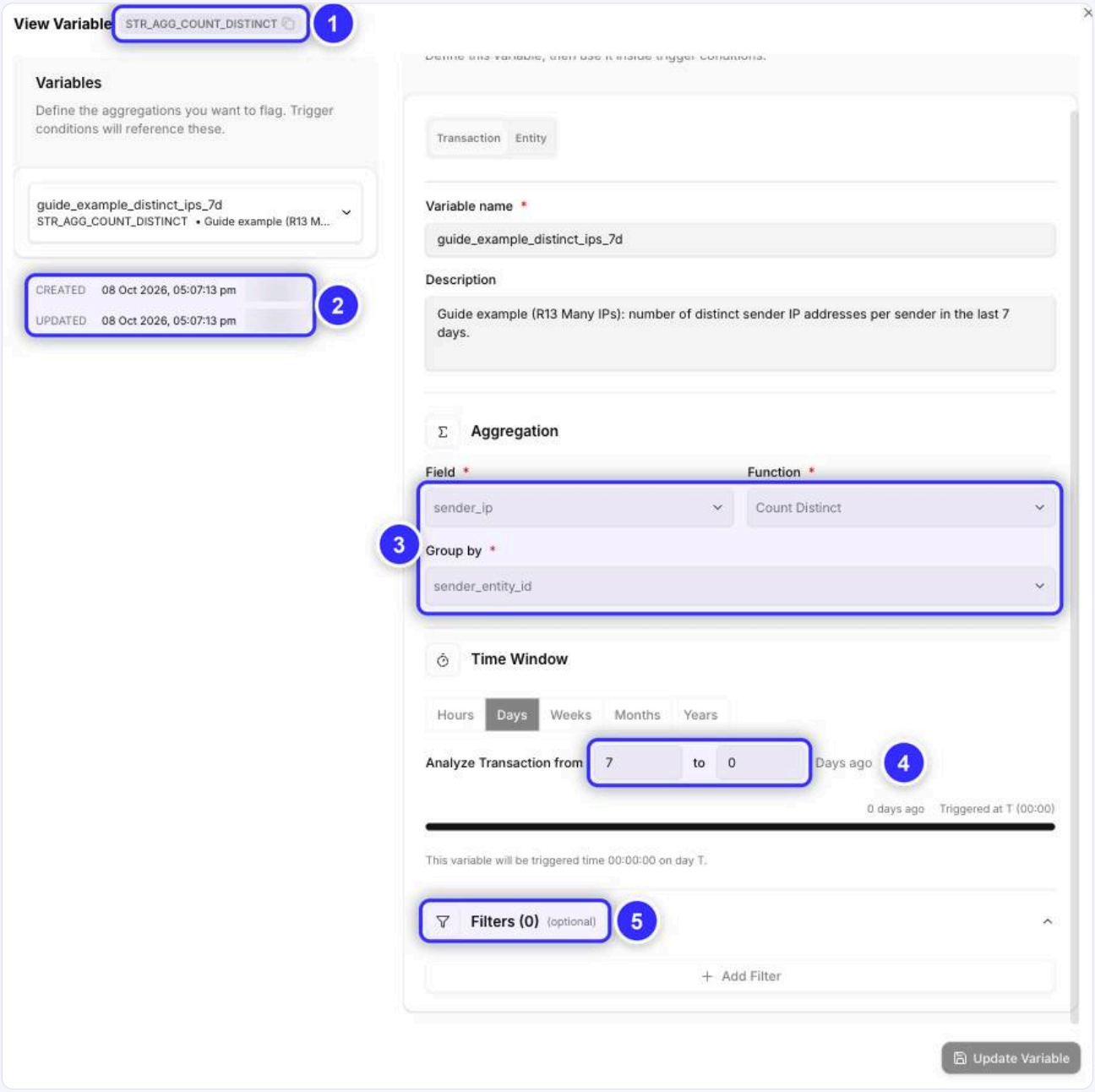


Figure 9.196 View Variable for distinct_ips_7d

Part B: Create the typology

Fyscal ARCX → Transaction Monitoring → Typology → + New

Step 8 **Fill in the details and choose Anomaly**

Click **+ New** on **Typology**. Type the name `R13 Many IPs - 15 or more sender IP addresses in 7 days`, set **Suppression Window** to 7 and choose **Day**, and write a description. Open **Typology type**, type `TP103` and click **Anomaly TP103**. The screens are the same as in Rule 10; the example was first saved with the name and threshold for 5 IP addresses, then changed to 15 after the dry run (see Test a typology with Dry Run).

Step 9 **Choose the variable in row 1**

In **Group 1**, click **Select field** next to **WHEN**, type part of the name and click `distinct_ips_7d`.

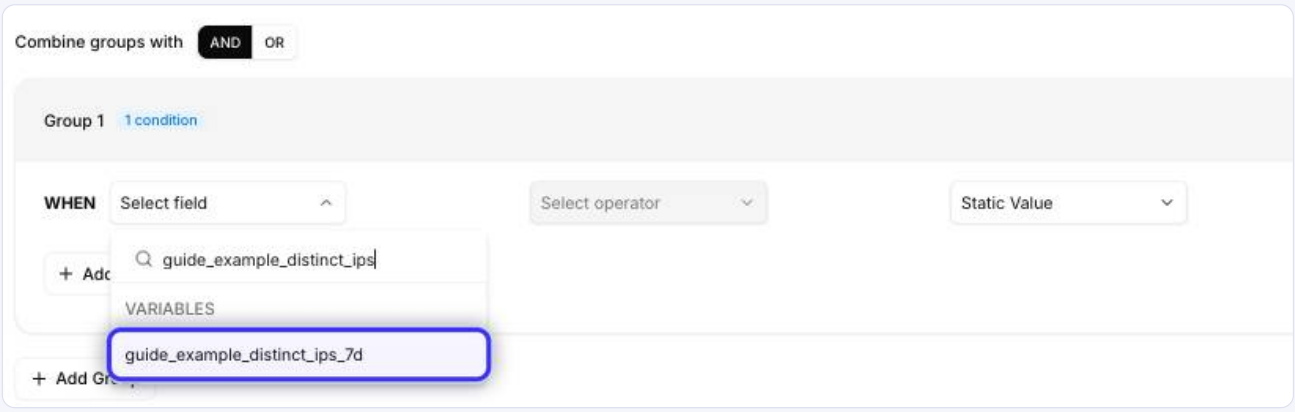


Figure 9.197 Rule 11 row 1: variable search

Step 10 **Choose Greater Than Equal and keep Static Value**

Open **Select operator** and choose **Greater Than Equal**. Keep **Static Value** in the compare-to list: the threshold is a fixed number.

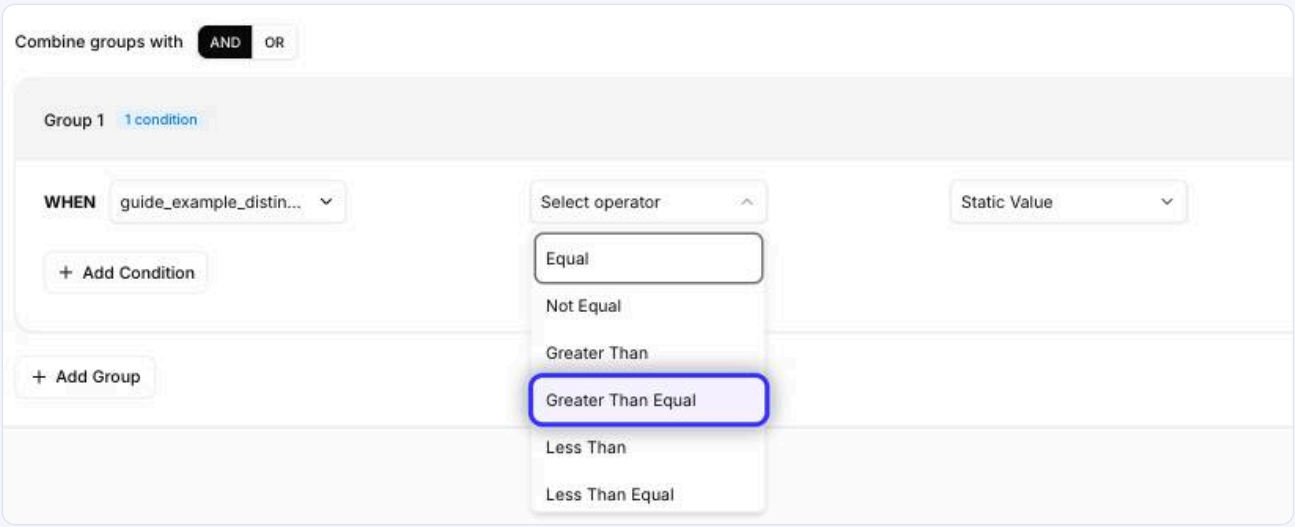


Figure 9.198 Rule 11 row 1: operator list

Step 11 **Enter 15 and go to the next step**

Type 15 in **Enter value** and click **Next Step**. In the list of typologies the rule then shows its name, `R13 Many IPs - 15 or more sender IP addresses in 7 days`, with **Draft** and its rule ID, TMR-08102026-001135.

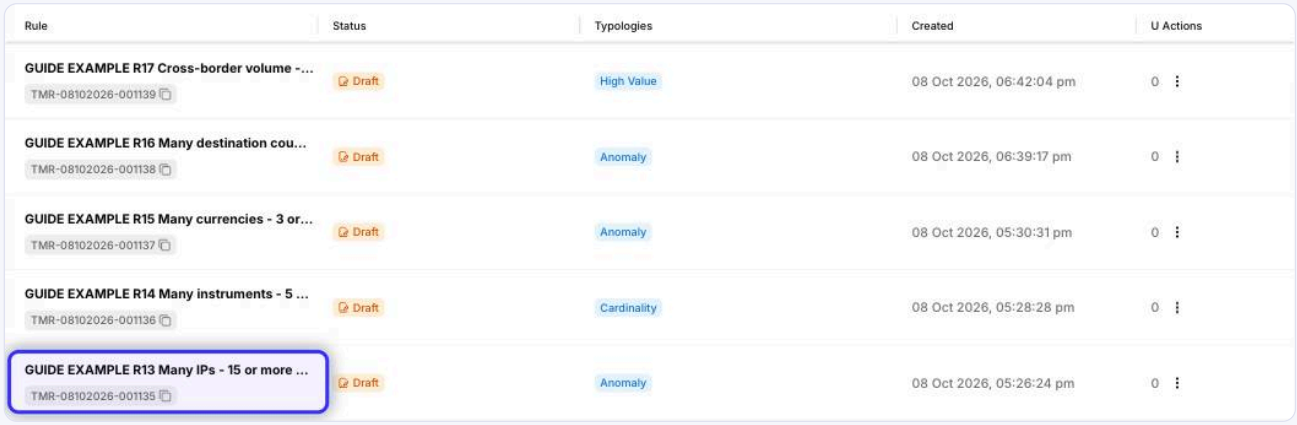


Figure 9.199 The Rule 11 example in the typology list, with its final name

Part C: Choose the schedule and save

Step 12 **Select the shared schedule and save the draft**

On **Review & schedule rule**, open **Select Schedule**, search for `schedule_2027`, click it and click **Save as Draft**, as in Rule 7.

Step 13 **Check the saved draft**

Wait a few seconds: the page becomes **Update Typology** (1) with the schedule (2), the run sentence (3), **Update** (4), **Dry Run** (5) and **Activate** (6). The screenshot shows the start in force when it was taken (01 Jan 2027).

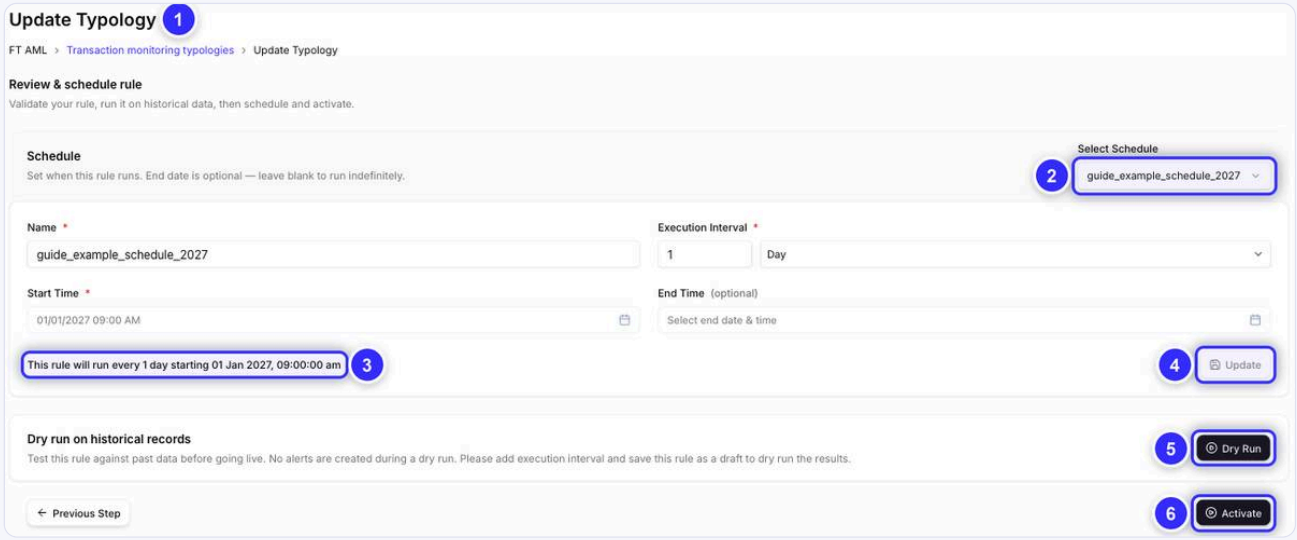


Figure 9.200 Rule 11 after Save as Draft

Step 14 **Check the rule page**

Open the rule from **Transaction Monitoring → Typology** to check it, as in Rule 10. It is listed as **Draft**, TMR-08102026-001135, with the typology type Anomaly.

How it evaluates. Sender A used 18 IP addresses in 7 days: 18 >= 15, alert. Sender B used 6: no alert.

Dry-run result. The threshold was set from the dry run. At 5 IP addresses the rule created 758 alerts across the four windows, far too many to review; at 10 it created 240, at 20 none, and at 15 it created 120 (30 in each window). The rule was saved at 15 and renamed to match. The tuning steps are in Test a typology with Dry Run.

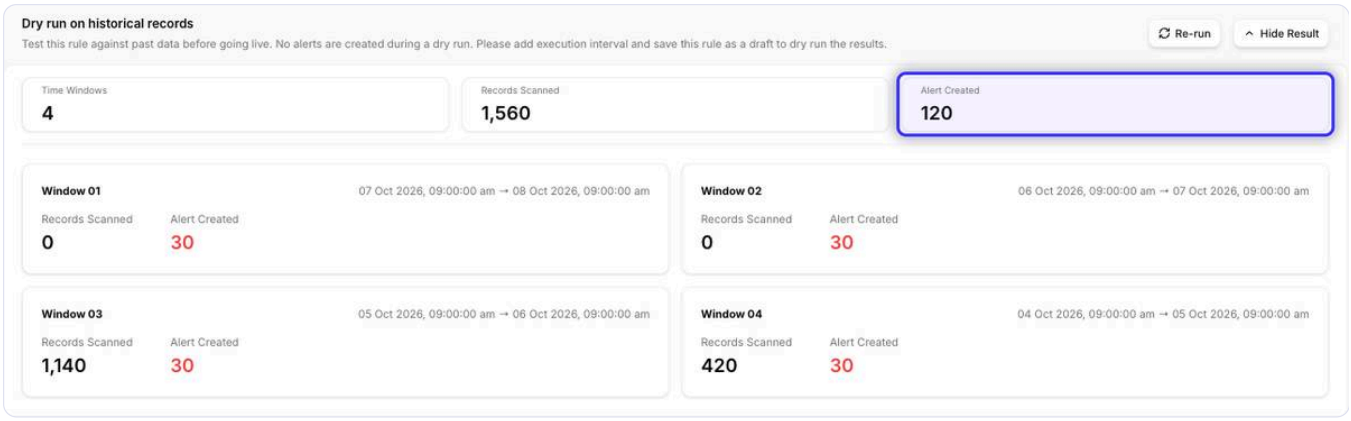


Figure 9.201 Rule 11 at the final threshold, >= 15: 120 alerts

Tuning. Mobile customers can change IP address often, so set the threshold from a dry run on your own data, as shown for this rule, rather than from a fixed number.

Rule 12 · Many instruments

RED FLAG **Payments funded from many cards or accounts**

LOGIC

Counts the different instruments (sender_instrument_id) the sender paid from in the last 7 days.

WINDOW

7 to 0 Days

THRESHOLD

≥ 5 instruments

✓ Verified by positive control

What it detects and why. This rule flags a sender who paid from 5 or more different instruments (for example cards or accounts) in 7 days. Funding payments from many instruments can hide where the money comes from.

Item	Setting
Variable `distinct_instruments_7d`	**Count Distinct** of `sender_instrument_id`, grouped by `sender_entity_id`, **Days** from 7 to 0, no filters
Typology type	Cardinality (C-01)
Suppression Window	7 Day
Condition	Group 1, Match AND: `distinct_instruments_7d` **Greater Than Equal (>=)** Static Value 5
Schedule	Existing `schedule_2027` (created in Rule 1): every 1 Day, starting 09 Oct 2026, 09:00 AM, no end time

Part A: Create the variable

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 1 **Open the form and name the variable**

Click **+ New** on **Variables** and leave **Transaction** selected. Type `distinct_instruments_7d` in **Variable name** (1) and a description such as “Number of distinct sender instruments (cards or accounts) per sender in the last 7 days.” (2).

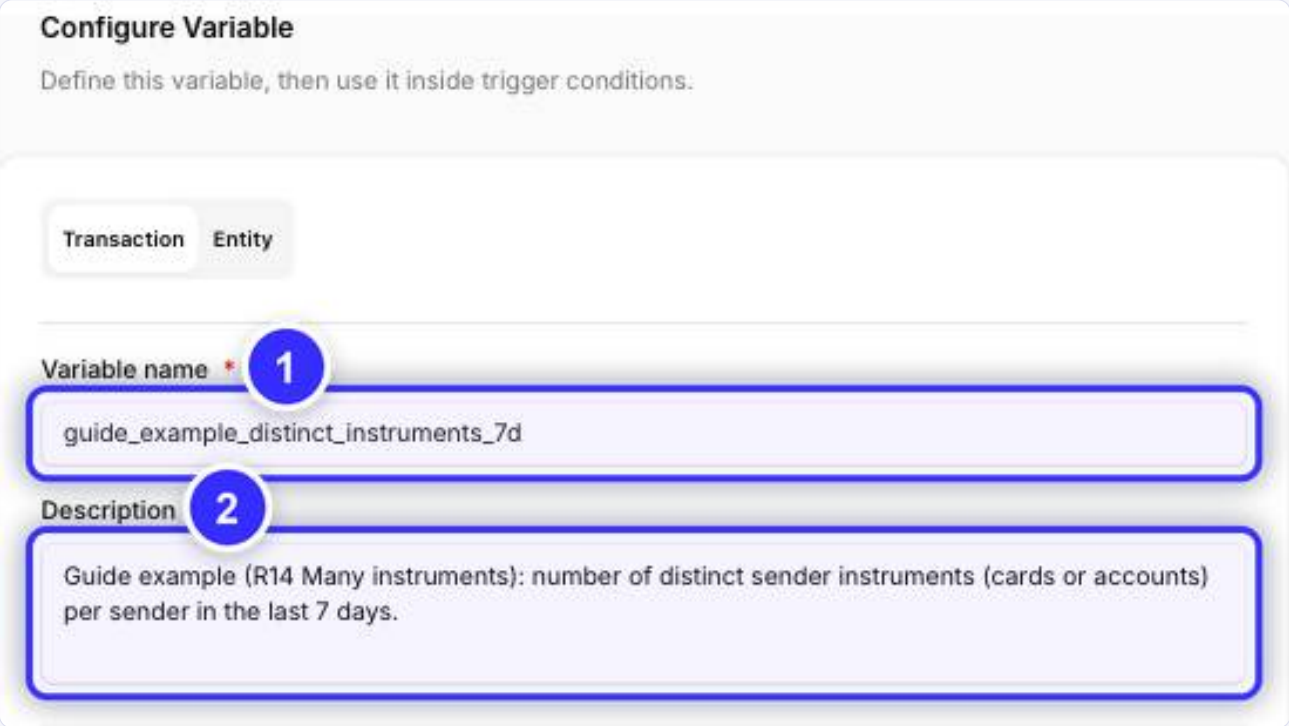


Figure 9.202 Rule 12 variable: name and description

Step 2 **Choose the Field: sender_instrument_id**

Open **Field** and type `instrument`. The matches include `receiver_instrument_id`, `receiver_instrument_subtype`, `receiver_instrument_type` and `sender_instrument_id`. Choose `sender_instrument_id`.

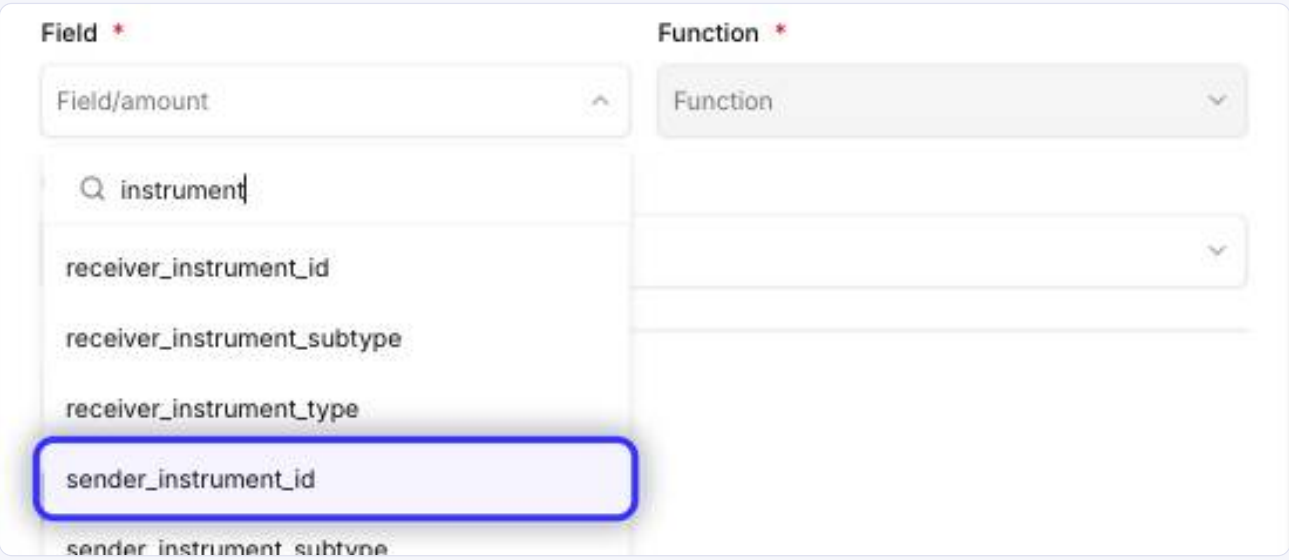


Figure 9.203 Field search for instrument: choose sender_instrument_id

Step 3 **Choose the Function: Count Distinct**

Open **Function**. For an ID or text field the list offers **Count**, **Count Distinct**, **Minimum** and **Maximum**. Choose **Count Distinct**: each different value is counted once.

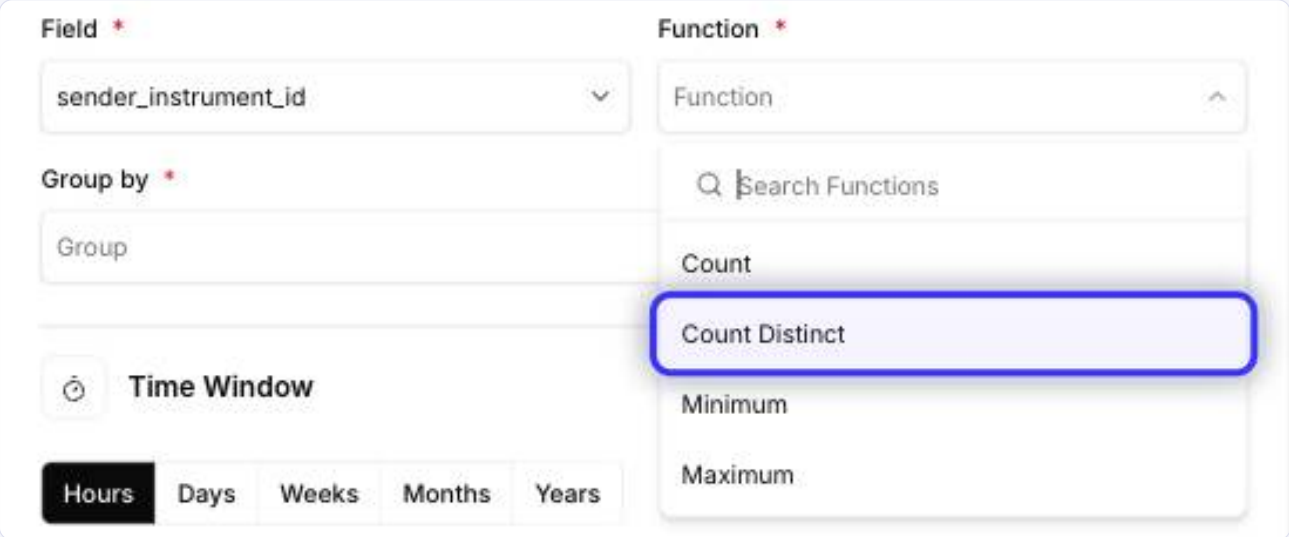


Figure 9.204 Function: Count Distinct

Step 4 **Choose Group by: sender_entity_id**

Open **Group by**, type `sender_entity` in **Search Fields** and choose `sender_entity_id`, so the count is calculated separately for each sender.



Figure 9.205 Group by search: sender_entity_id

Step 5 **Set the time window: Days, 7 to 0, and save**

Scroll down. Click **Days** (1); the default is **Hours**. Enter 7 in **Analyze Transaction from** and 0 in **to** (2): the 7 days up to the trigger time T. Leave the blank row under **Filters (1)** (3) empty: a blank row is dropped when you save. Click **Save Variable** (4).

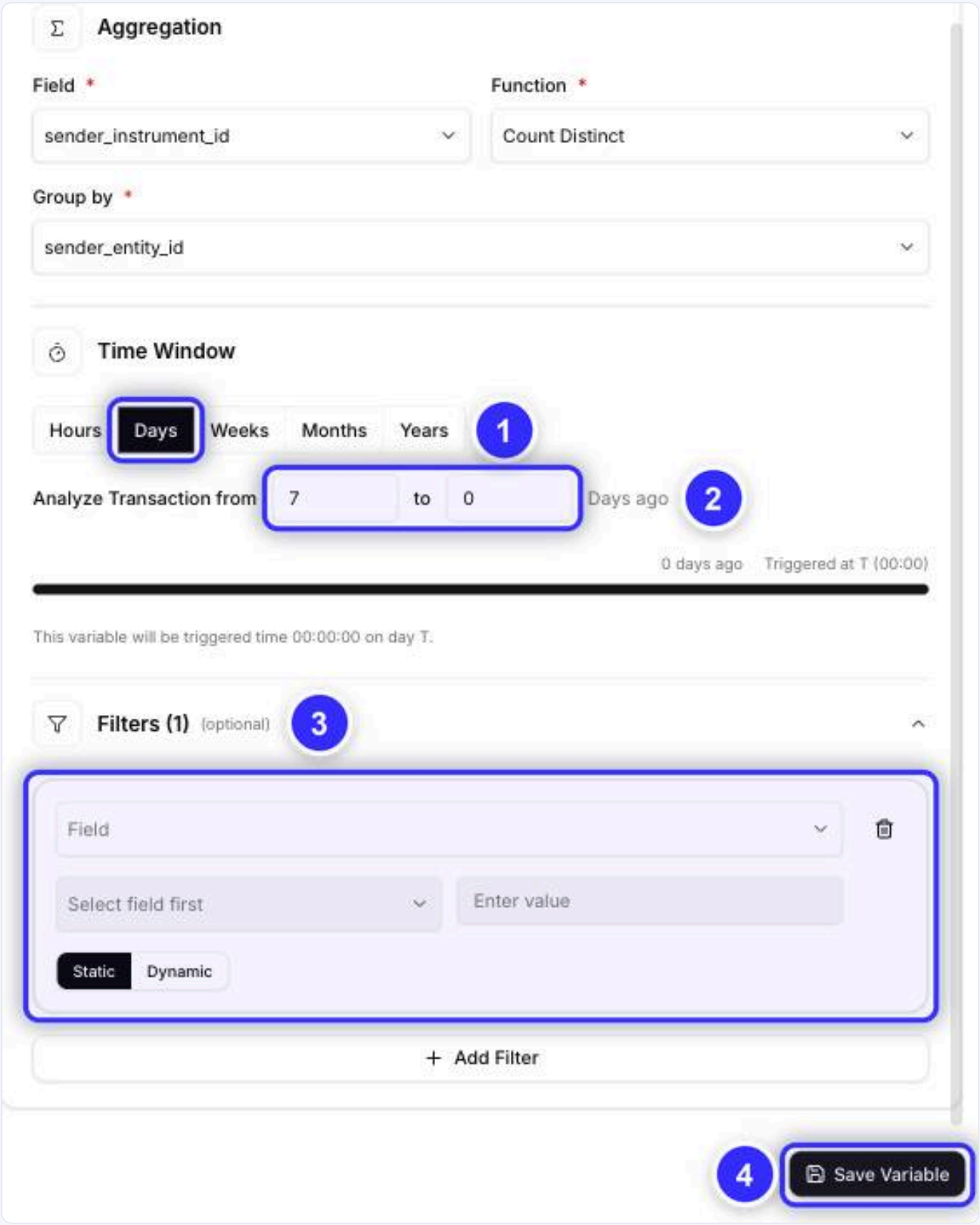


Figure 9.206 Time window 7 to 0 Days ago, blank filter row and Save Variable

Step 6 **Find the variable in the list**

The dialog closes and the variable is the first row of the **Variables** list, here VAR-08102026-000802.

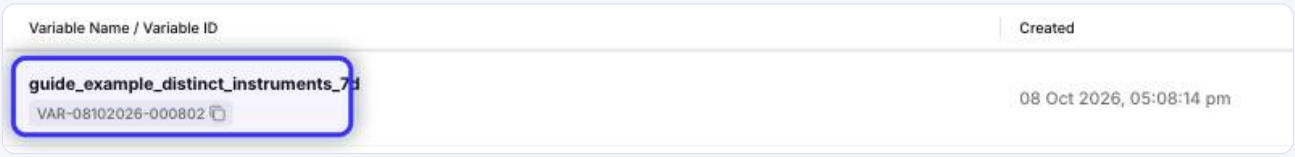


Figure 9.207 Rule 12 variable in the Variables list

Step 7 **Check the saved variable**

Click the row. **View Variable** shows the type tag **STR_AGG_COUNT_DISTINCT** (1), the **CREATED** and **UPDATED** times and user (2), `sender_instrument_id` / **Count Distinct** / `sender_entity_id` (3), 7 to 0 **Days ago** (4) and **Filters (0)** (5).

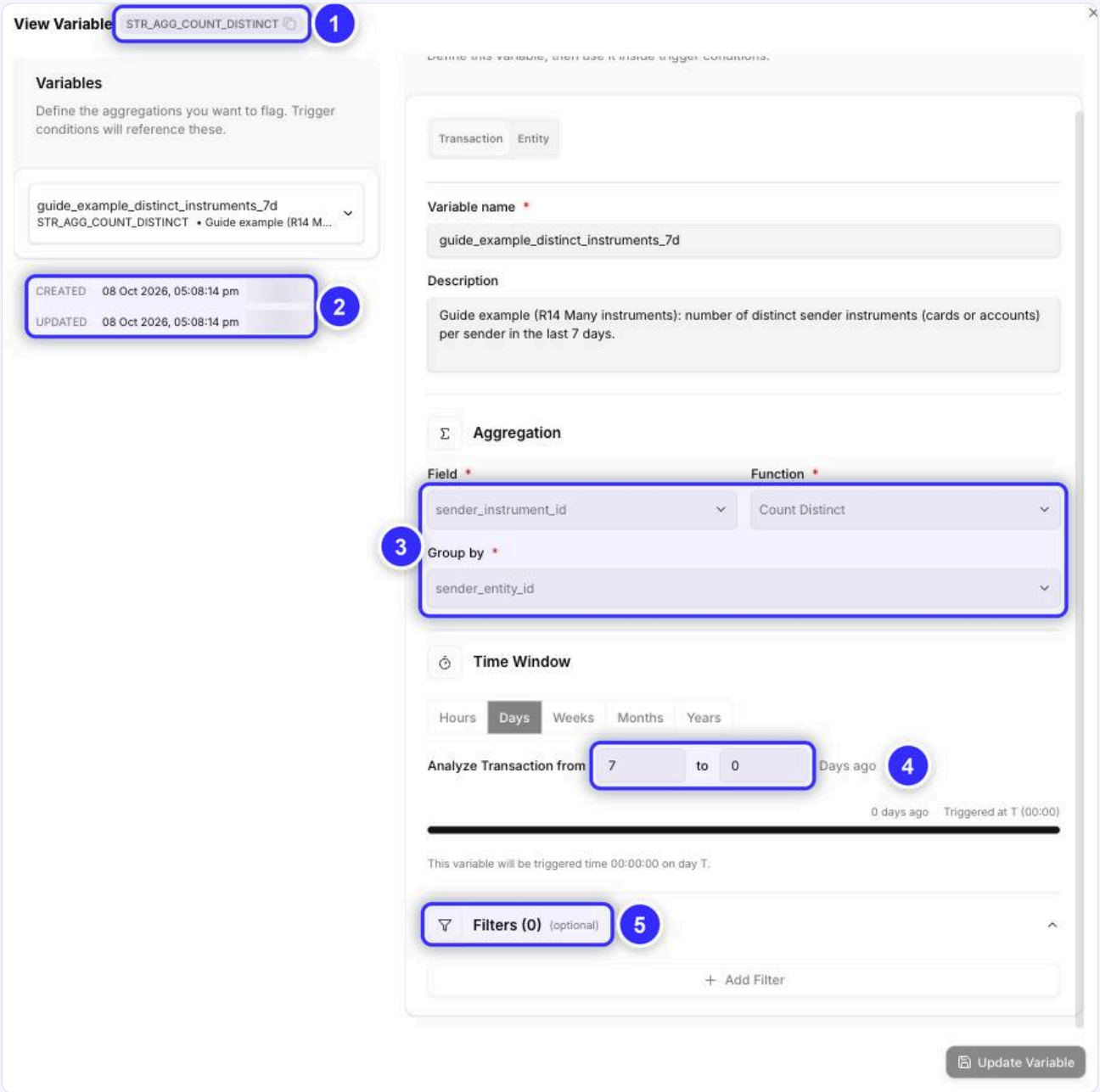


Figure 9.208 View Variable for distinct_instruments_7d

Part B: Create the typology

Fyscal ARCX → Transaction Monitoring → Typology → + New

Step 8 **Fill in the details and choose Cardinality**

Click **+ New** on **Typology**. Type the name `R14 Many instruments - 5 or more sender instruments in 7 days` (1). Set **Suppression Window** to 7 and choose **Day** (2): it matches the 7-day window. Write a description (3). Open **Typology type** (4), type `Cardin` and click **Cardinality C-01**.

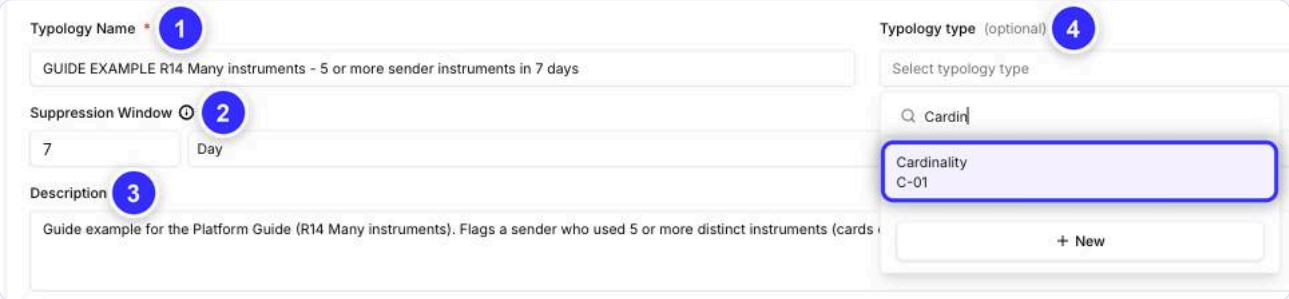


Figure 9.209 Rule 12 details and the Typology type search

Step 9 **Choose the variable in row 1**

In **Group 1**, click **Select field** next to **WHEN**, type part of the name and click `distinct_instruments_7d`.

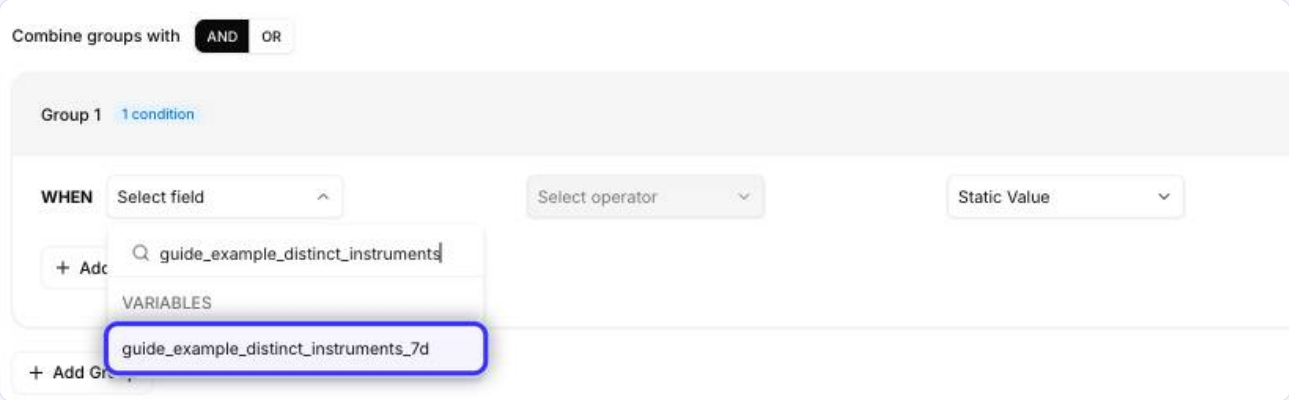


Figure 9.210 Rule 12 row 1: variable search

Step 10 **Choose Greater Than Equal and keep Static Value**

Open **Select operator** and choose **Greater Than Equal**. Keep **Static Value** in the compare-to list: the threshold is a fixed number.

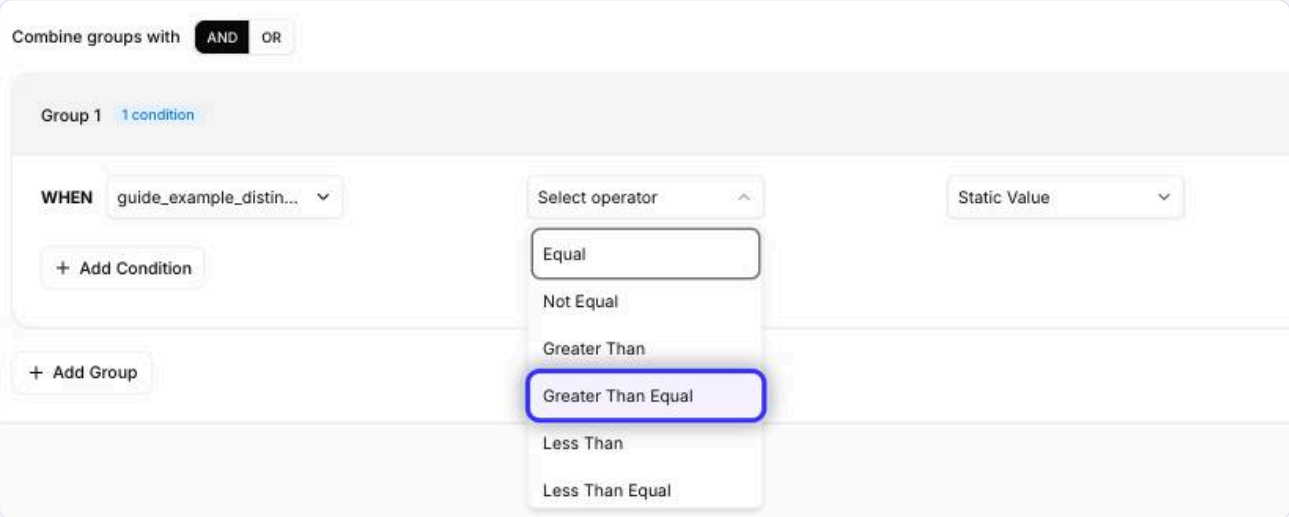


Figure 9.211 Rule 12 row 1: operator list

Step 11 **Enter 5 and go to the next step**

Type 5 in **Enter value**. Check the name (1), the type chip **Cardinality (C-01)** (2), **7 Day** (3), the description (4), **Match** AND (5) and the row (6). Click **Next Step** (7).

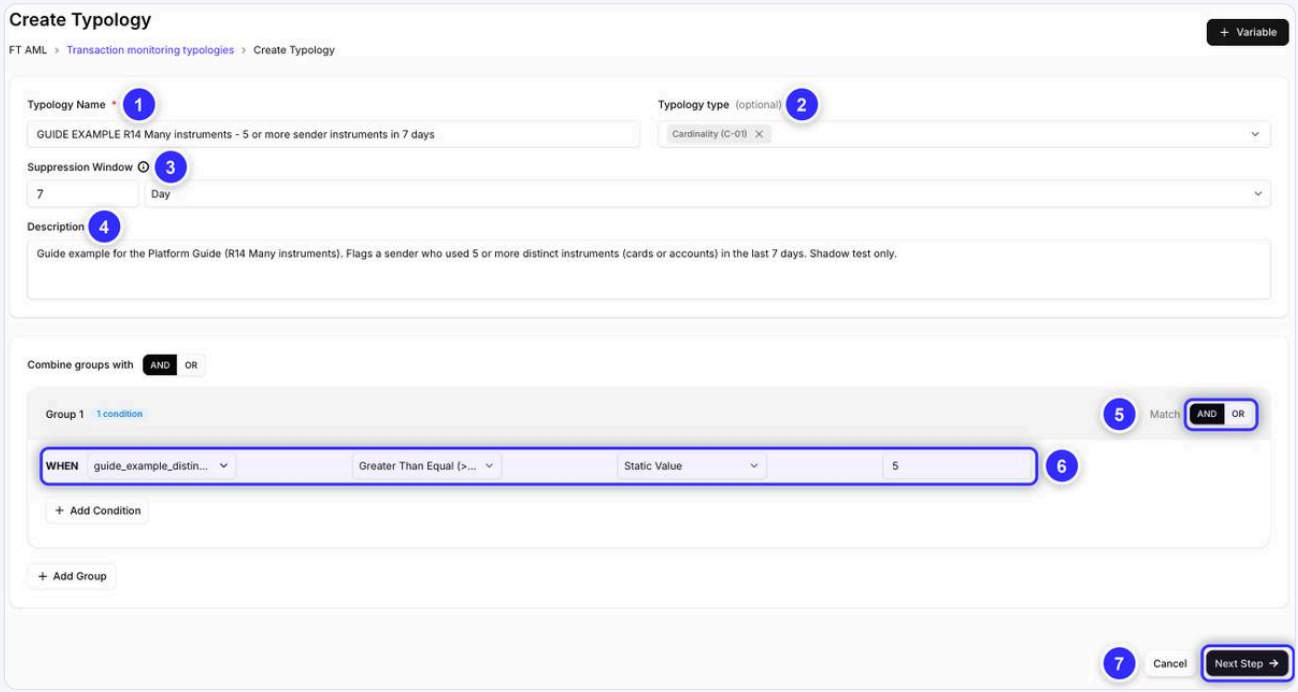


Figure 9.212 The completed Rule 12 page

Part C: Choose the schedule and save

Step 12 **Select the shared schedule and save the draft**

On **Review & schedule rule**, open **Select Schedule**, search for `schedule_2027`, click it and click **Save as Draft**, as in Rule 7.

Step 13 **Check the saved draft**

Wait a few seconds: the page becomes **Update Typology** (1) with the schedule (2), the run sentence (3), **Update** (4), **Dry Run** (5) and **Activate** (6). The screenshot shows the start in force when it was taken (01 Jan 2027).

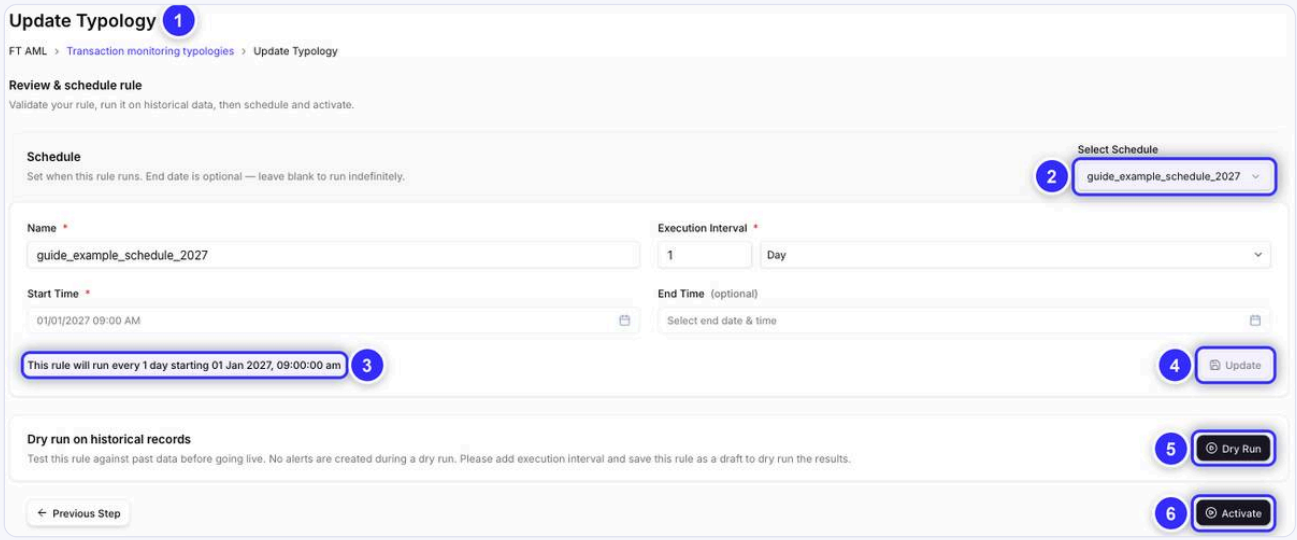


Figure 9.213 Rule 12 after Save as Draft

Step 14 **Check the rule page**

Open the rule from **Transaction Monitoring → Typology**. It shows **Draft** and the rule ID TMR-08102026-001136, created 08 Oct 2026, 05:28:28 pm (1); the summary with **INTERVAL** Every 1 day, **SUPPRESSION** 7Day and **TYPOLOGY** Cardinality (2); the condition, with the operator shown as **Greater Than Equal (>=)** (3); and the variable card `distinct_instruments_7d`, Str_agg_count_distinct, **WINDOW** in last 7 day, **GROUP** `sender_entity_id` (4).

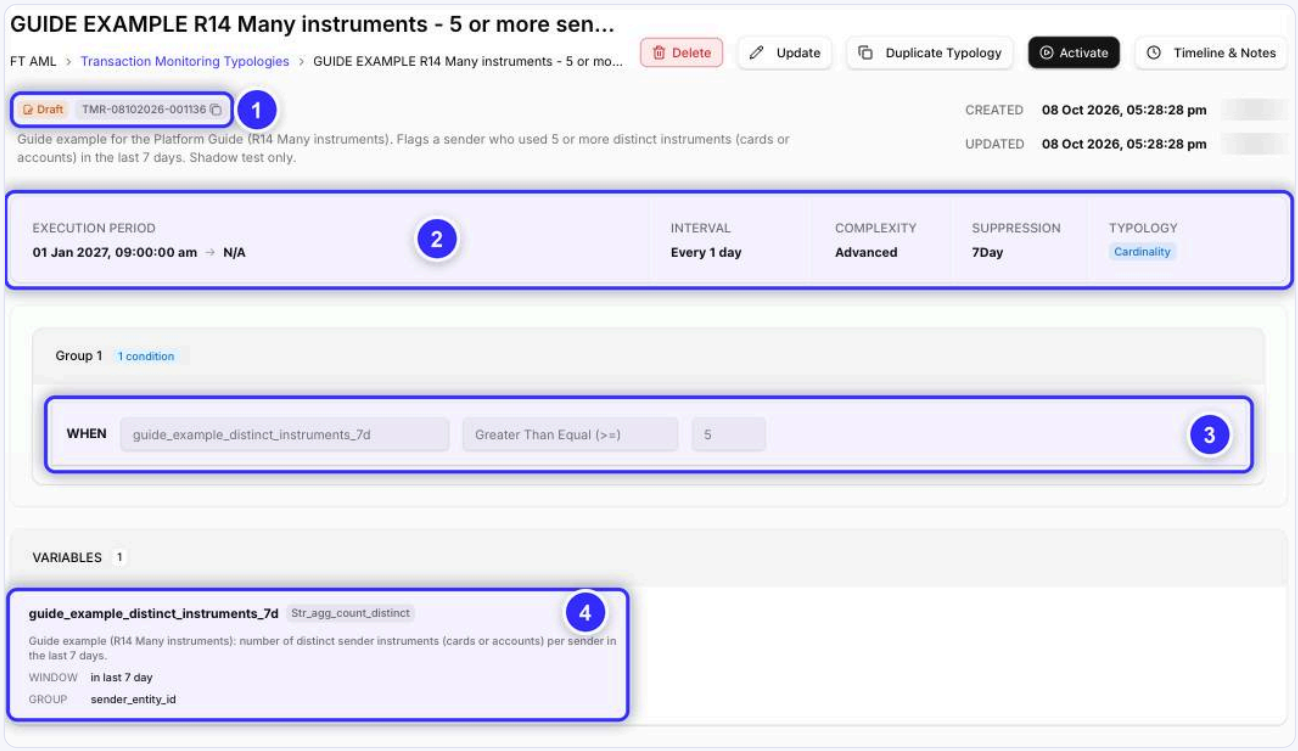


Figure 9.214 The saved Rule 12 as a Draft, TMR-08102026-001136

How it evaluates. Sender A paid from 6 different cards in a week: 6 >= 5, alert. Sender B paid 30 times from 1 account: no alert.

Dry-run result. In testing, the rule created 0 alerts at its real threshold (>= 5) in all four windows: no sender in the test data used 5 instruments in 7 days. To prove the rule works, the threshold was lowered to >= 1 for one dry run. That created 4,615 alerts (1,164 / 1,187 / 1,222 / 1,042 by window, newest first), then the threshold was restored and a new dry run returned 0 again. See Test a typology with Dry Run for the method.

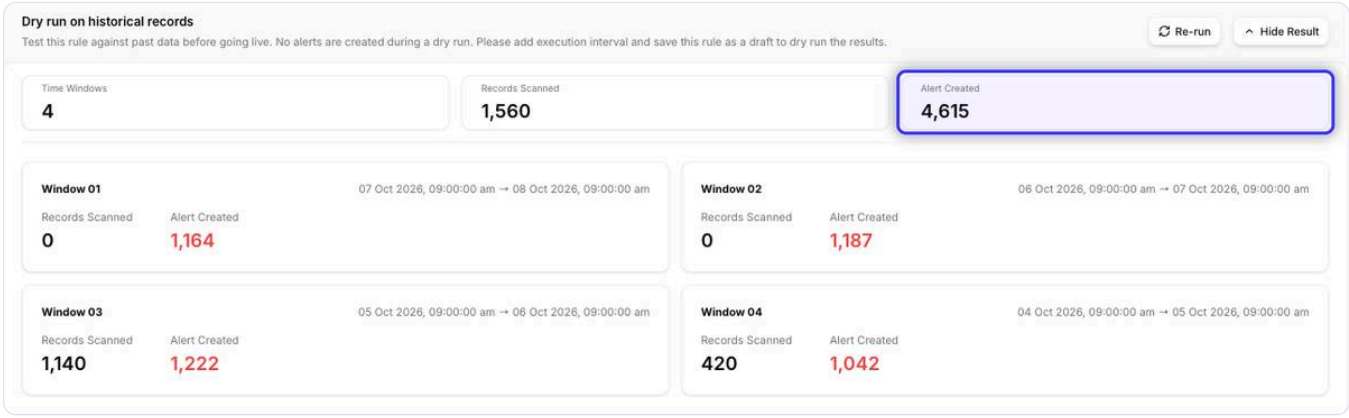


Figure 9.215 Rule 12 positive control (threshold temporarily >= 1): 4,615 alerts

Tuning. Set the number of instruments from what your customers normally hold. To count only one kind of instrument, add a filter on `sender_instrument_type`.

Rule 13 · Many currencies

RED FLAG **Switching between currencies**

LOGIC

Counts the different currencies (currency_code) the sender used in the last 30 days.

WINDOW	THRESHOLD
30 to 0 Days	≥ 3 currencies

✓ Verified by positive control

What it detects and why. This rule flags a sender who transacted in 3 or more different currencies in 30 days. Frequent switching between currencies is unusual for most retail customers and can be part of moving value across borders.

Item	Setting
Variable `distinct_currencies_30d`	**Count Distinct** of `currency_code`, grouped by `sender_entity_id`, **Days** from 30 to 0, no filters
Typology type	Anomaly (TP103)
Suppression Window	30 Day
Condition	Group 1, Match AND: `distinct_currencies_30d` **Greater Than Equal (>=)** Static Value 3
Schedule	Existing `schedule_2027` (created in Rule 1): every 1 Day, starting 09 Oct 2026, 09:00 AM, no end time

Part A: Create the variable

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 1 **Open the form and name the variable**

Click **+ New** on **Variables** and leave **Transaction** selected. Type `distinct_currencies_30d` in **Variable name** (1) and a description such as "Number of distinct transaction currencies per sender in the last 30 days." (2).

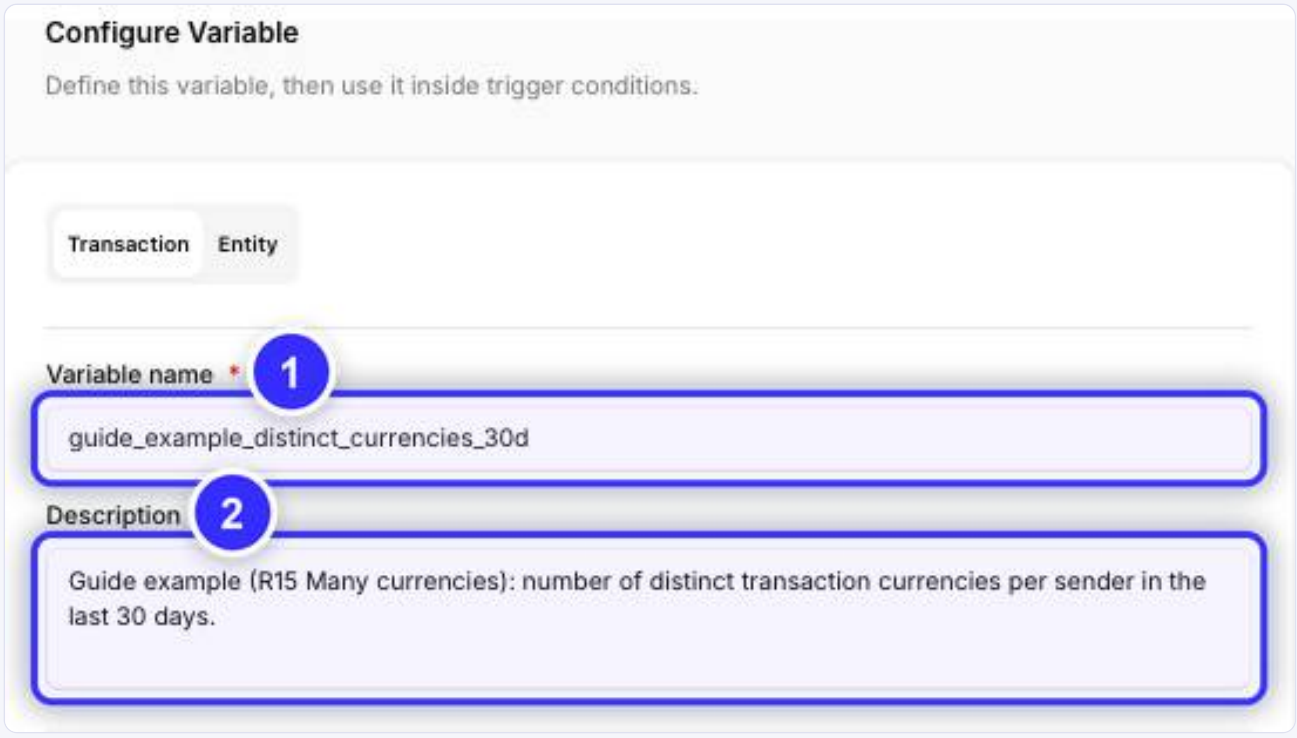


Figure 9.216 Rule 13 variable: name and description

Step 2 **Choose the Field: currency_code**

Open **Field** and type `currency`. The matches are `currency_code`, `orig_currency_amount`, `orig_currency_code`, `receiver_currency_code` and `sender_currency_code`. Choose `currency_code`.

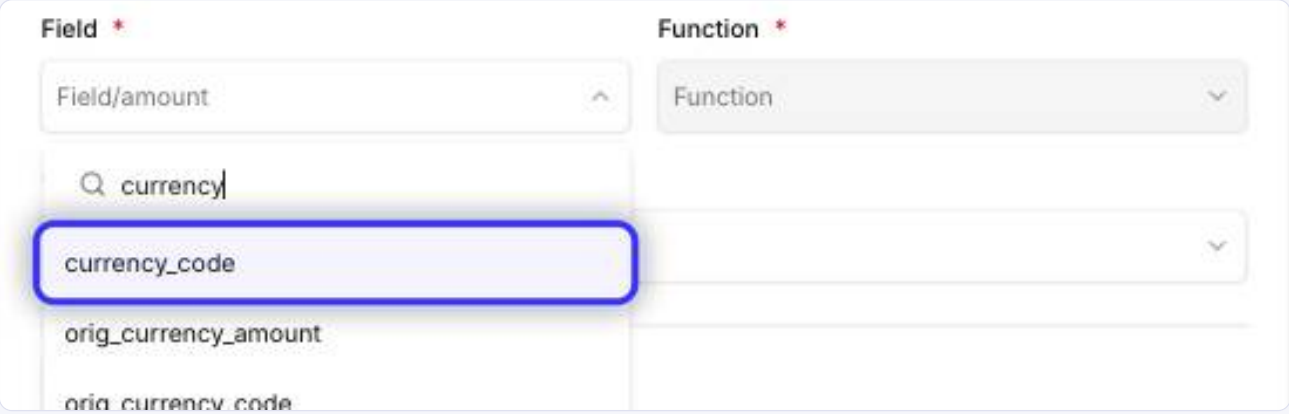


Figure 9.217 Field search for currency: choose currency_code

Step 3 **Choose the Function: Count Distinct**

Open **Function**. For an ID or text field the list offers **Count**, **Count Distinct**, **Minimum** and **Maximum**. Choose **Count Distinct**: each different value is counted once.

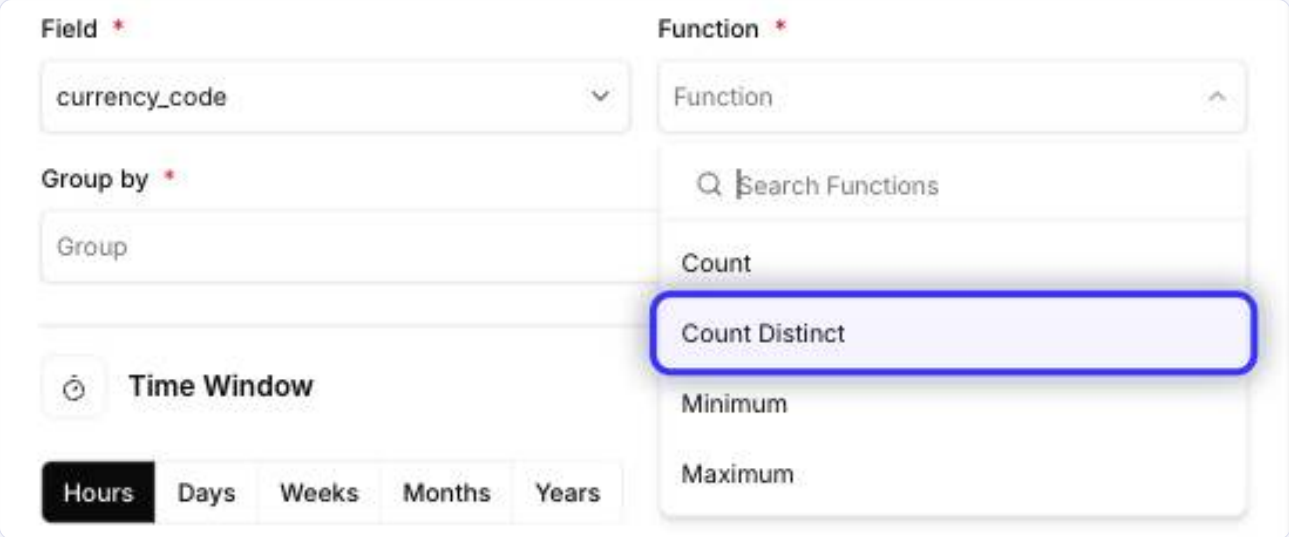


Figure 9.218 Function: Count Distinct

Step 4 **Choose Group by: sender_entity_id**

Open **Group by**, type `sender_entity` in **Search Fields** and choose `sender_entity_id`, so the count is calculated separately for each sender.



Figure 9.219 Group by search: sender_entity_id

Step 5 **Set the time window: Days, 30 to 0, and save**

Scroll down. Click **Days** (1); the default is **Hours**. Enter 30 in **Analyze Transaction from** and 0 in **to** (2): the 30 days up to the trigger time T. Leave the blank row under **Filters (1)** (3) empty: a blank row is dropped when you save. Click **Save Variable** (4).

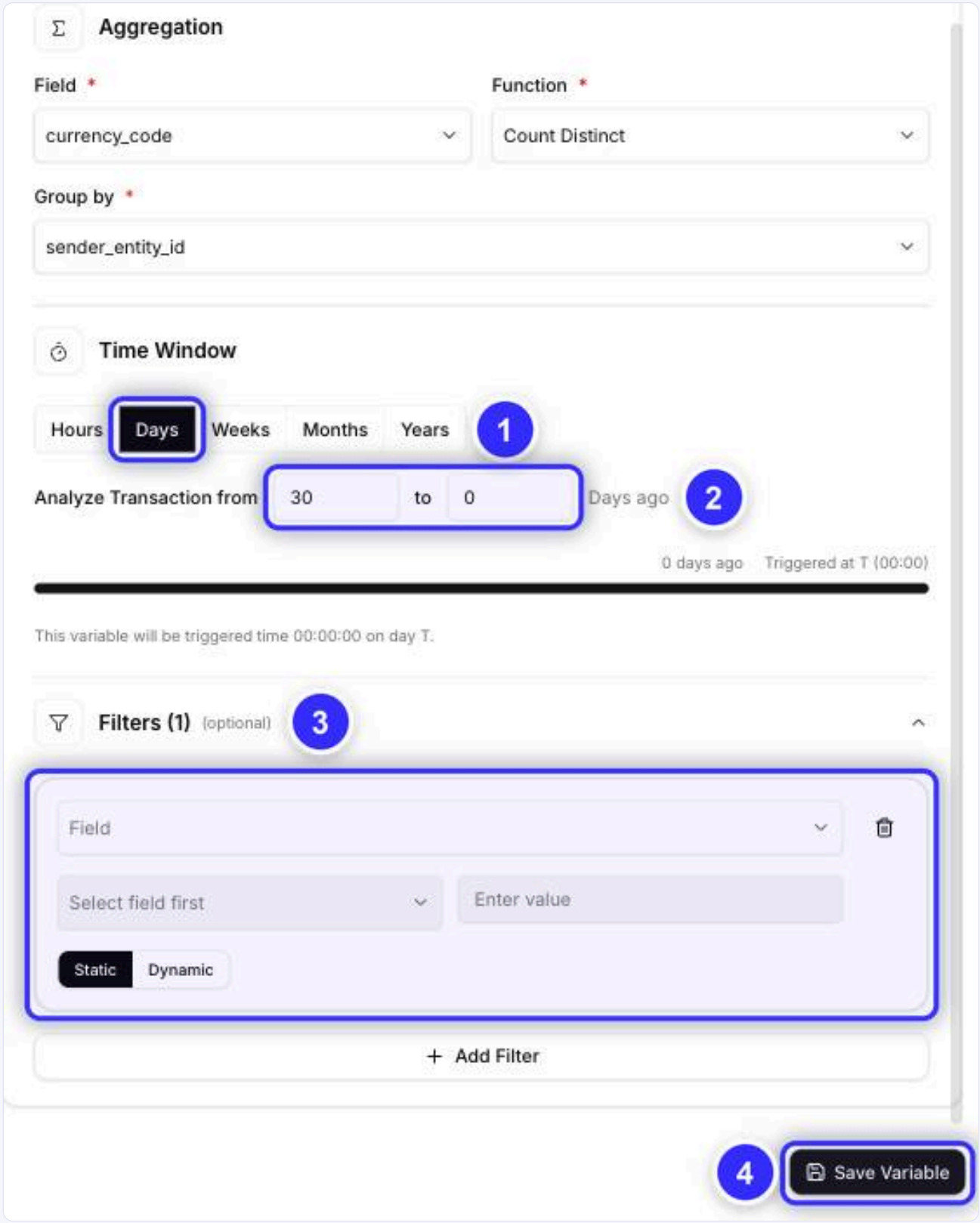


Figure 9.220 Time window 30 to 0 Days ago, blank filter row and Save Variable

Step 6 **Find the variable in the list**

The dialog closes and the variable is the first row of the **Variables** list, here VAR-08102026-000803.

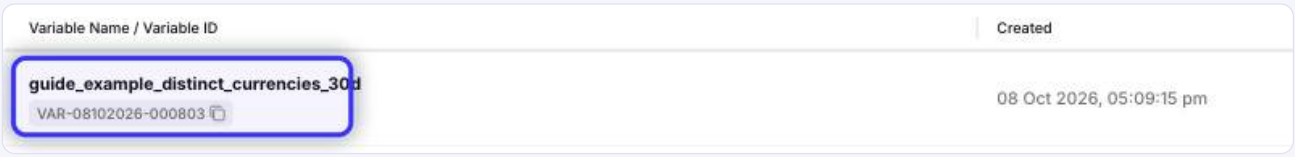


Figure 9.221 Rule 13 variable in the Variables list

Step 7 **Check the saved variable**

Click the row. **View Variable** shows the type tag **STR_AGG_COUNT_DISTINCT** (1), the **CREATED** and **UPDATED** times and user (2), `currency_code` / **Count Distinct** / `sender_entity_id` (3), 30 to 0 **Days ago** (4) and **Filters (0)** (5).

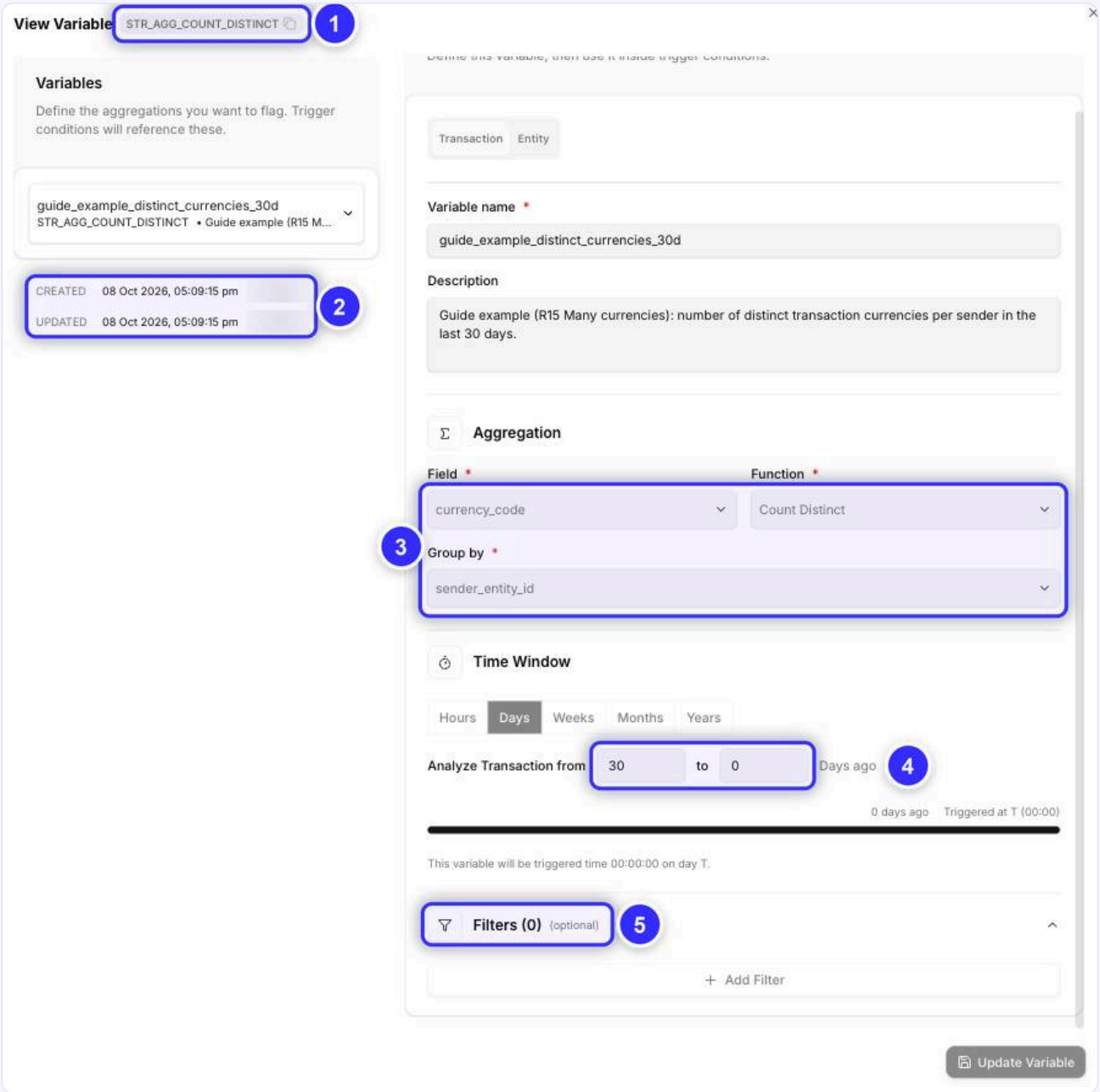


Figure 9.222 View Variable for distinct_currencies_30d

Part B: Create the typology

Fyscal ARCX → Transaction Monitoring → Typology → + New

Step 8 **Fill in the details and choose Anomaly**

Click **+ New** on **Typology**. Type the name `R15 Many currencies - 3 or more currencies in 30 days` (1). Set **Suppression Window** to 30 and choose **Day** (2): it matches the 30-day window. Write a description (3). Open **Typology type** (4), type `TP103` and click **Anomaly TP103**.



Figure 9.223 Rule 13 details and the Typology type search

Step 9 **Choose the variable in row 1**

In **Group 1**, click **Select field** next to **WHEN**, type part of the name and click `distinct_currencies_30d`.

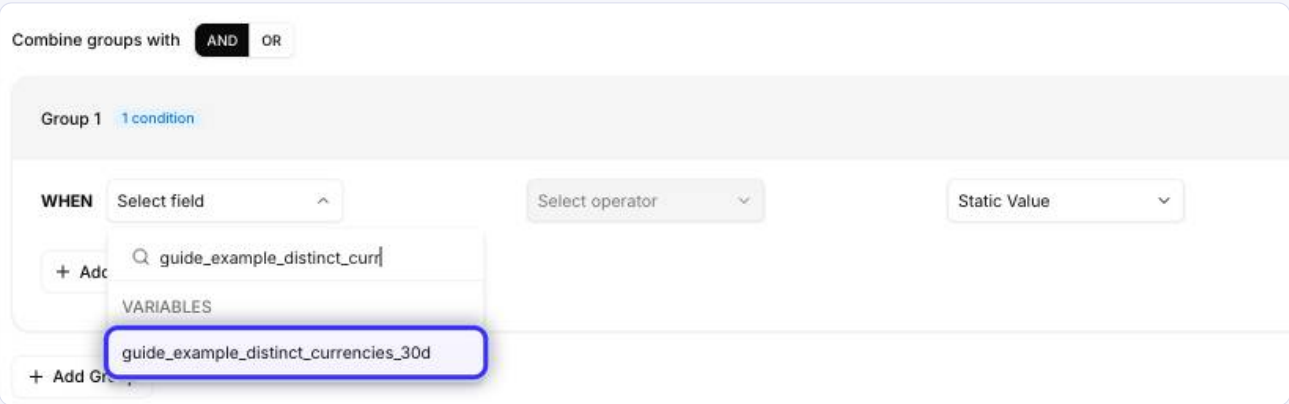


Figure 9.224 Rule 13 row 1: variable search

Step 10 **Choose Greater Than Equal and keep Static Value**

Open **Select operator** and choose **Greater Than Equal**. Keep **Static Value** in the compare-to list: the threshold is a fixed number.

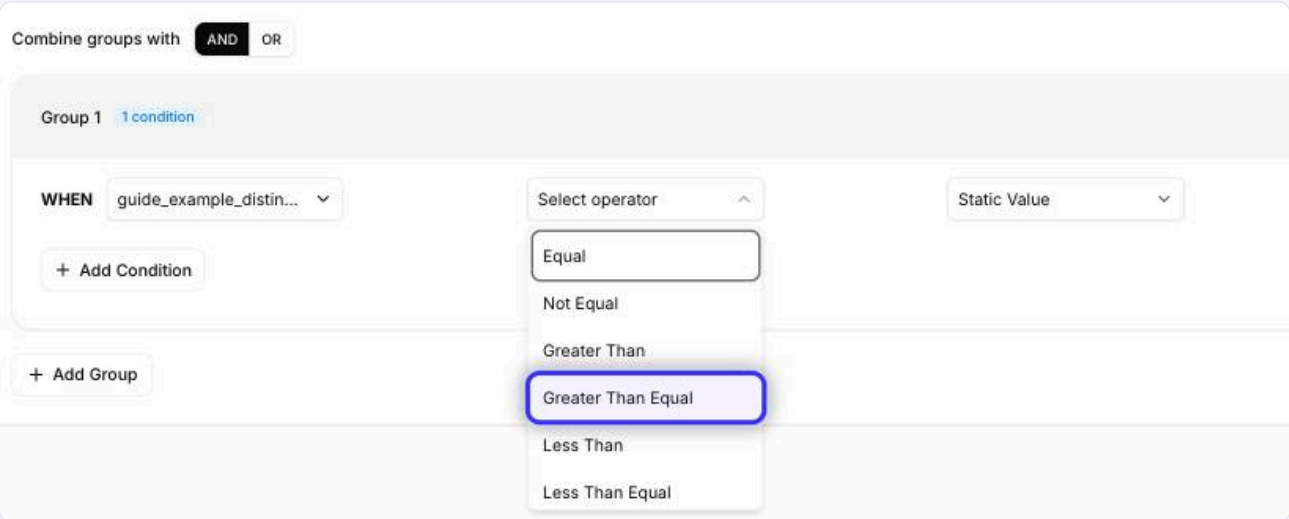


Figure 9.225 Rule 13 row 1: operator list

Step 11 **Enter 3 and go to the next step**

Type 3 in **Enter value**. Check the name (1), the type chip **Anomaly (TP103)** (2), **30 Day** (3), the description (4), **Match** AND (5) and the row (6). Click **Next Step** (7).

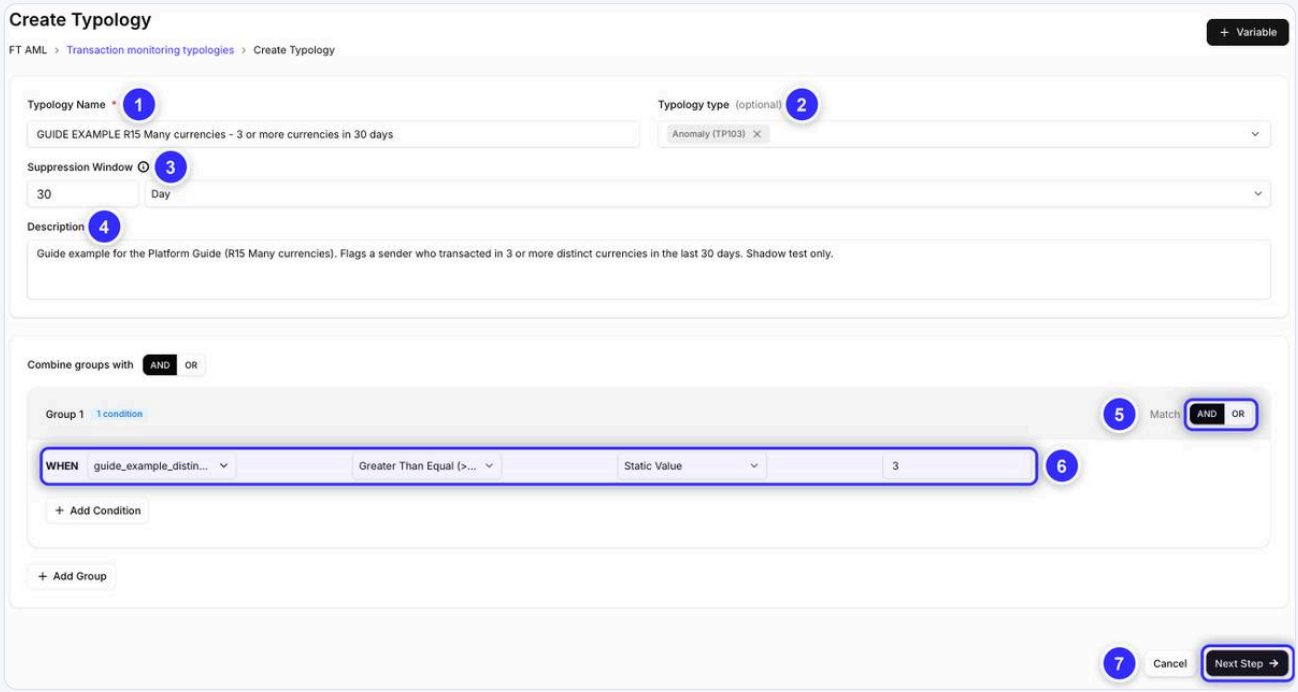


Figure 9.226 The completed Rule 13 page

Part C: Choose the schedule and save

Step 12 **Select the shared schedule and save the draft**

On **Review & schedule rule**, open **Select Schedule**, search for `schedule_2027`, click it and click **Save as Draft**, as in Rule 7.

Step 13 **Check the saved draft**

Wait a few seconds: the page becomes **Update Typology** (1) with the schedule (2), the run sentence (3), **Update** (4), **Dry Run** (5) and **Activate** (6). The screenshot shows the start in force when it was taken (01 Jan 2027).

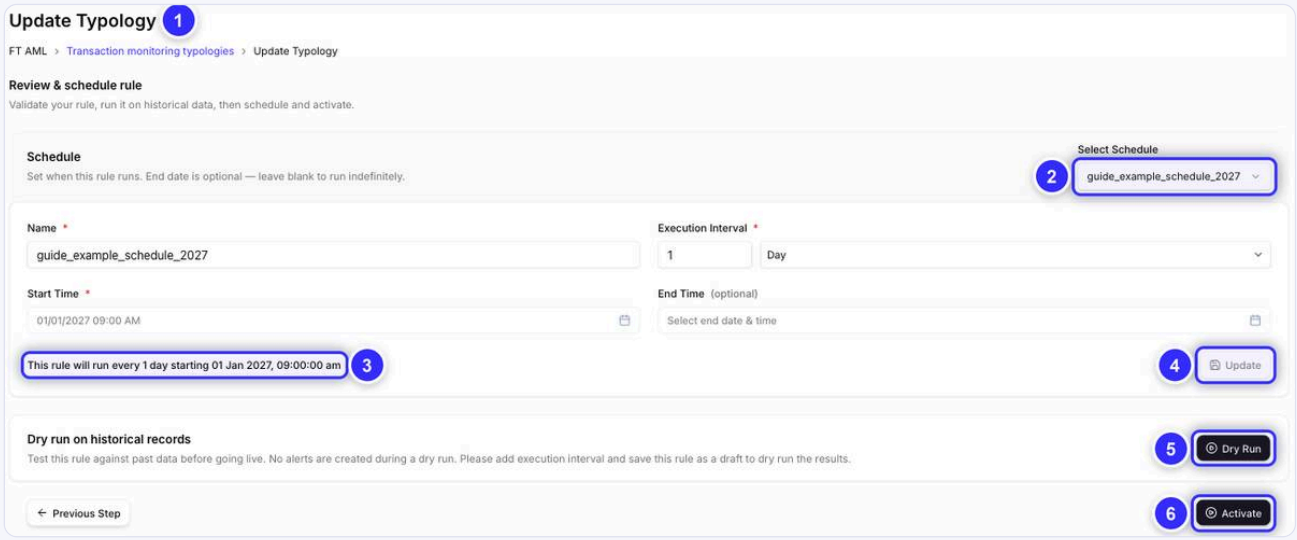


Figure 9.227 Rule 13 after Save as Draft

Step 14 **Check the rule page**

Open the rule from **Transaction Monitoring → Typology**. The page has the same layout as in Rule 12: **Draft** with the rule ID TMR-08102026-001137, **SUPPRESSION** 30Day, **TYPOLOGY** Anomaly, the condition and the variable card.

How it evaluates. Sender A sent payments in PHP, USD and EUR within 30 days: 3 >= 3, alert. Sender B paid only in PHP: 1, no alert.

Dry-run result. In testing, the rule created 0 alerts at its real threshold (>= 3) in all four windows: no sender in the test data used 3 currencies in 30 days. To prove the rule works, the threshold was lowered to >= 1 for one dry run. That created 6,512 alerts (1,671 / 1,680 / 1,685 / 1,476 by window, newest first), then the threshold was restored and a new dry run returned 0 again. See Test a typology with Dry Run for the method. This control shows that `currency_code` is filled in for every sender; with only one currency per sender in the test data, it cannot show a sender with several currencies.

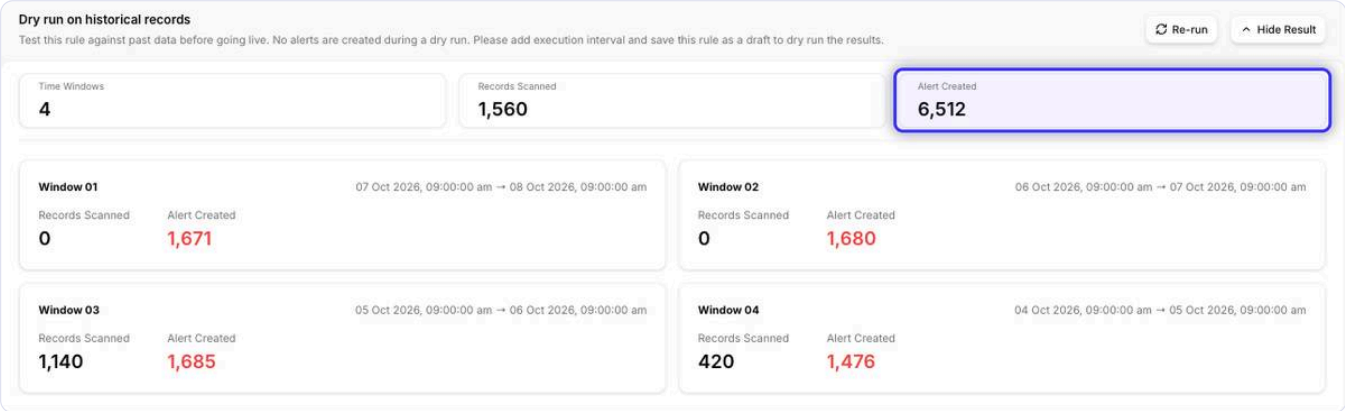


Figure 9.228 Rule 13 positive control (threshold temporarily >= 1): 6,512 alerts

Tuning. Set the number of currencies from your product range: a foreign-exchange or remittance customer may normally use several.

Rule 14 · Many destination countries

RED FLAG **Payments spread across countries**

LOGIC

Counts the different destination countries (receiver_provider_country) the sender paid into in the last 30 days.

WINDOW	THRESHOLD
30 to 0 Days	≥ 3 countries

✓ Verified · 94 alerts

What it detects and why. This rule flags a sender who paid receivers in 3 or more different provider countries in 30 days. Spreading payments across many countries is a common way to move funds out of reach.

Item	Setting
Variable `distinct_dest_countries_30d`	**Count Distinct** of `receiver_provider_country`, grouped by `sender_entity_id`, **Days** from 30 to 0, no filters
Typology type	Anomaly (TP103)
Suppression Window	30 Day
Condition	Group 1, Match AND: `distinct_dest_countries_30d` **Greater Than Equal (>=)** Static Value 3
Schedule	Existing `schedule_2027` (created in Rule 1): every 1 Day, starting 09 Oct 2026, 09:00 AM, no end time

Part A: Create the variable

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 1 **Open the form and name the variable**

Click **+ New** on **Variables** and leave **Transaction** selected. Type `distinct_dest_countries_30d` in **Variable name** (1) and a description such as “Number of distinct receiver provider countries per sender in the last 30 days.” (2).

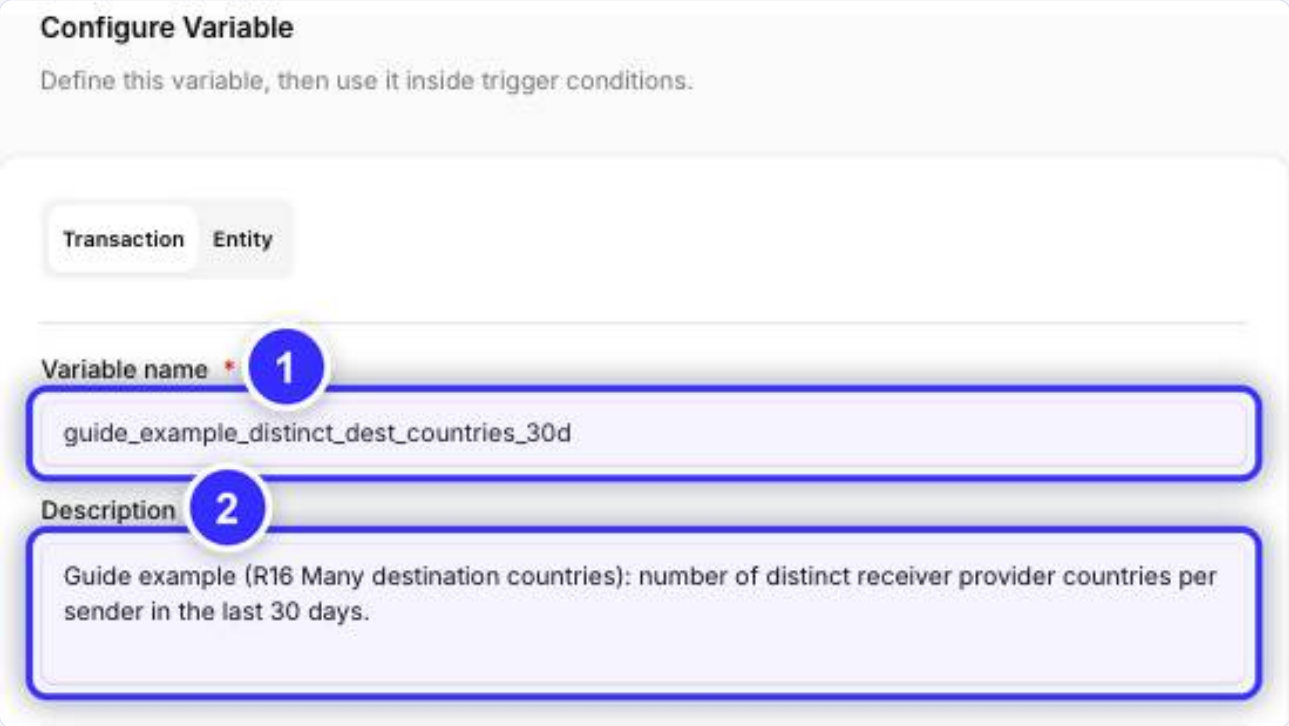


Figure 9.229 Rule 14 variable: name and description

Step 2 **Choose the Field: receiver_provider_country**

Open **Field** and type `country`. Two fields match, `receiver_provider_country` and `sender_provider_country`. Choose `receiver_provider_country`.

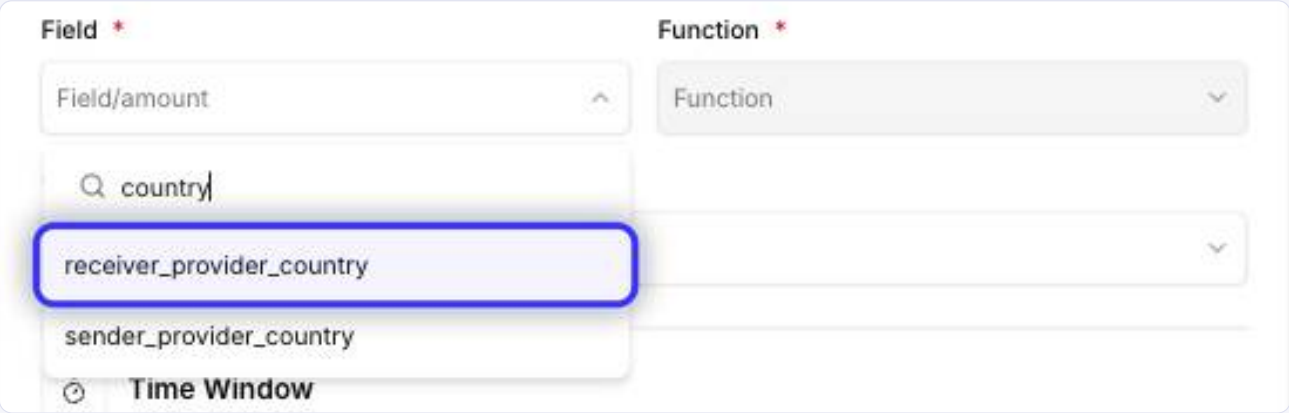


Figure 9.230 Field search for country: choose receiver_provider_country

Step 3 **Choose the Function: Count Distinct**

Open **Function**. For an ID or text field the list offers **Count**, **Count Distinct**, **Minimum** and **Maximum**. Choose **Count Distinct**: each different value is counted once.

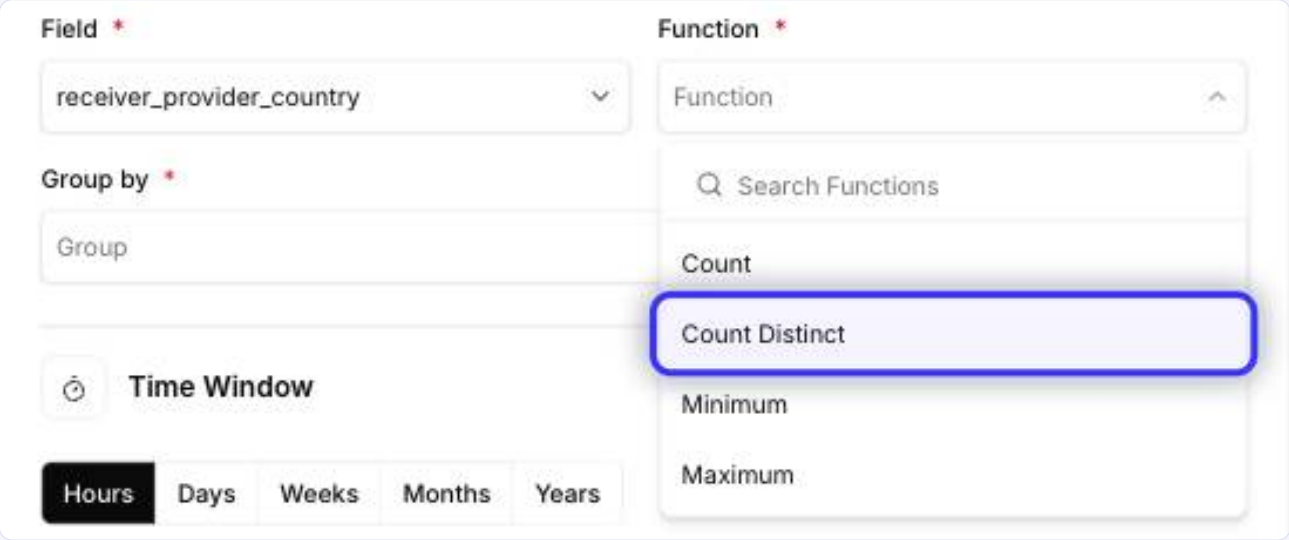


Figure 9.231 Function: Count Distinct

Step 4 **Choose Group by: sender_entity_id**

Open **Group by**, type `sender_entity` in **Search Fields** and choose `sender_entity_id`, so the count is calculated separately for each sender.



Figure 9.232 Group by search: sender_entity_id

Step 5 **Set the time window: Days, 30 to 0, and save**

Scroll down. Click **Days** (1); the default is **Hours**. Enter 30 in **Analyze Transaction from** and 0 in **to** (2): the 30 days up to the trigger time T. Leave the blank row under **Filters (1)** (3) empty: a blank row is dropped when you save. Click **Save Variable** (4).

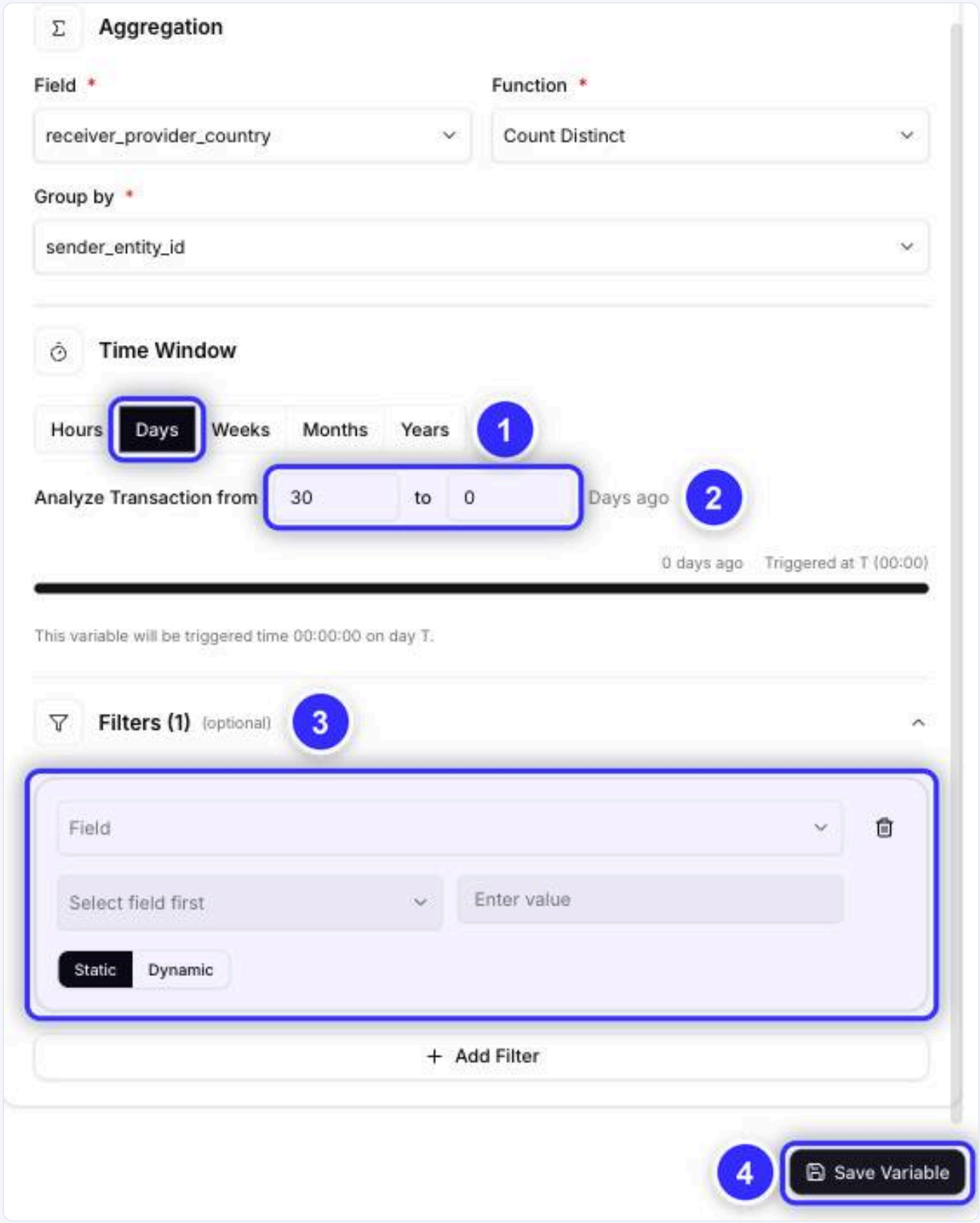


Figure 9.233 Time window 30 to 0 Days ago, blank filter row and Save Variable

Step 6 **Find the variable in the list**

The dialog closes and the variable is the first row of the **Variables** list, here VAR-08102026-000804.

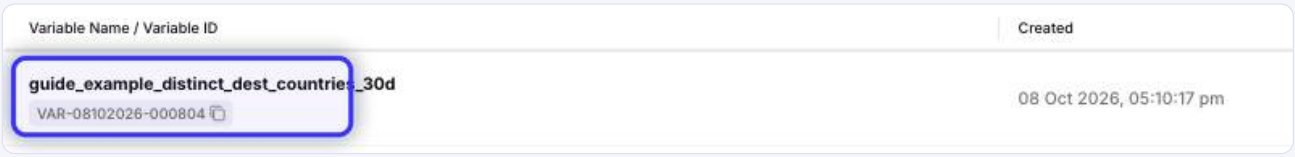


Figure 9.234 Rule 14 variable in the Variables list

Step 7 **Check the saved variable**

Click the row. **View Variable** shows the type tag **STR_AGG_COUNT_DISTINCT** (1), the **CREATED** and **UPDATED** times and user (2), `receiver_provider_country` / **Count Distinct** / `sender_entity_id` (3), 30 to 0 **Days ago** (4) and **Filters (0)** (5).

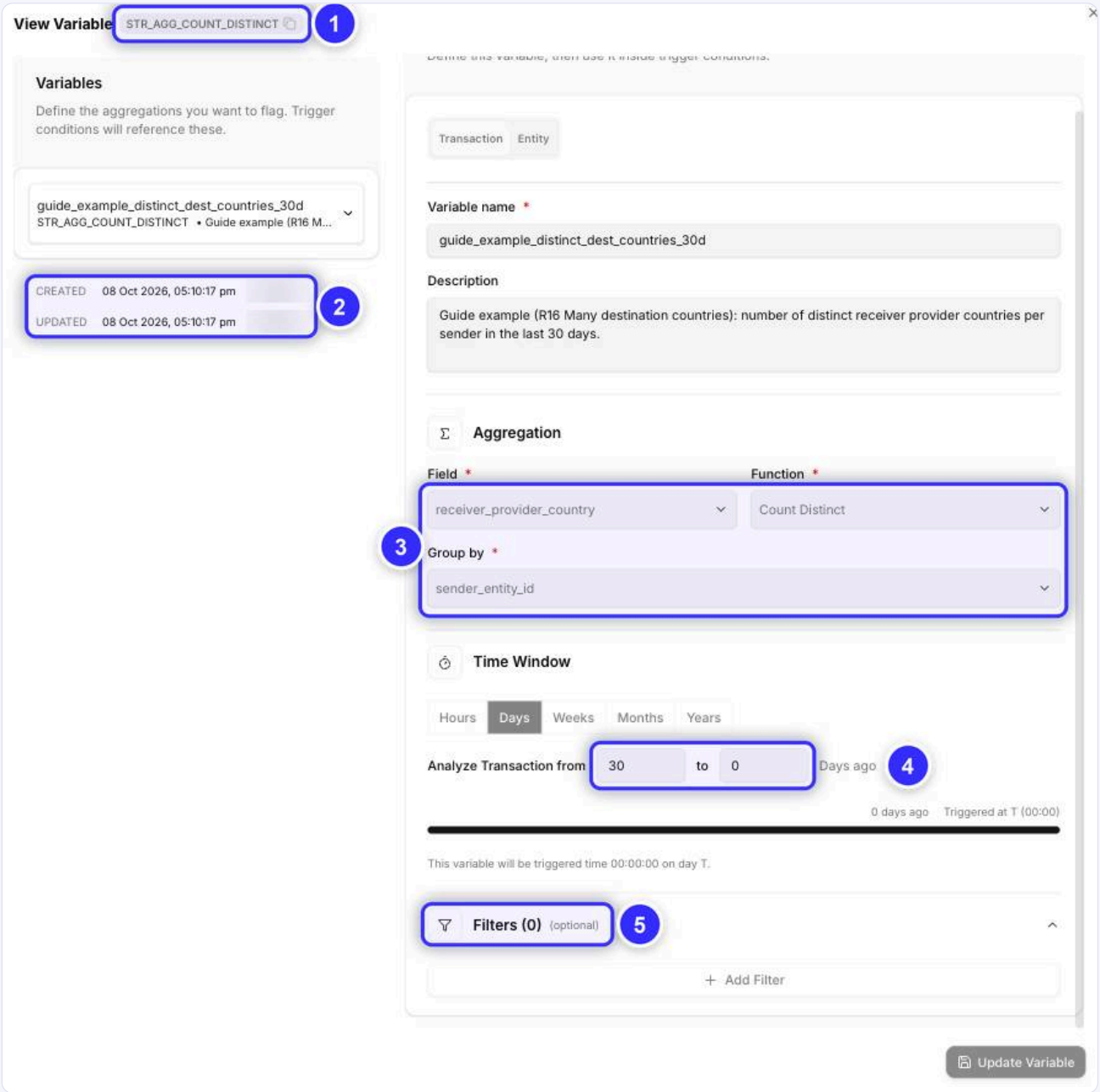


Figure 9.235 View Variable for distinct_dest_countries_30d

Part B: Create the typology

Fyscal ARCX → Transaction Monitoring → Typology → + New

Step 8 **Fill in the details and choose Anomaly**

Click **+ New** on **Typology**. Type the name `R16 Many destination countries - 3 or more receiver countries in 30 days` (1). Set **Suppression Window** to 30 and choose **Day** (2): it matches the 30-day window. Write a description (3). Open **Typology type** (4), type `TP103` and click **Anomaly TP103**.



Figure 9.236 Rule 14 details and the Typology type search

Step 9 **Choose the variable in row 1**

In **Group 1**, click **Select field** next to **WHEN**, type part of the name and click `distinct_dest_countries_30d`.

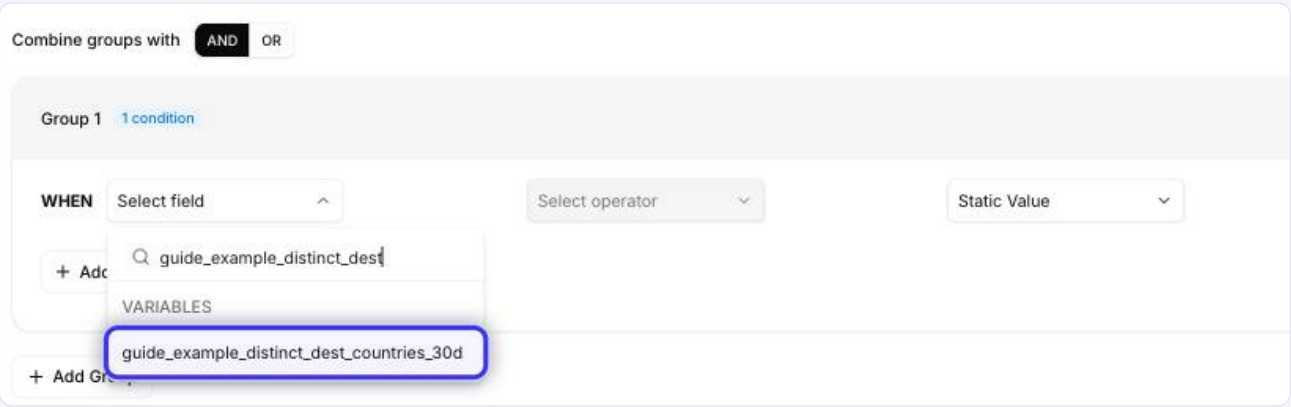


Figure 9.237 Rule 14 row 1: variable search

Step 10 **Choose Greater Than Equal and keep Static Value**

Open **Select operator** and choose **Greater Than Equal**. Keep **Static Value** in the compare-to list: the threshold is a fixed number.

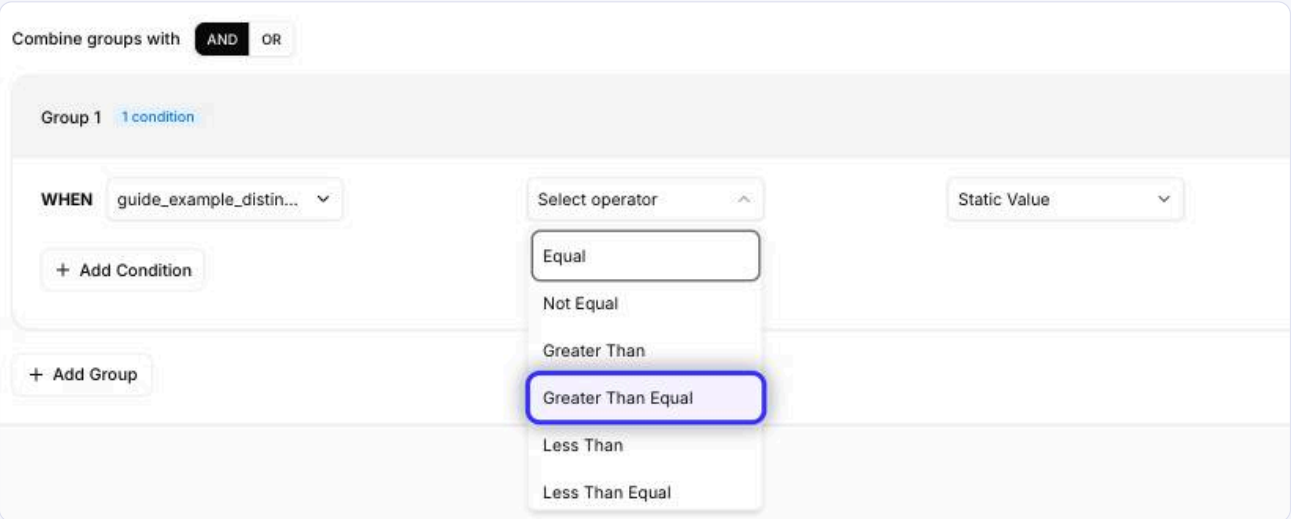


Figure 9.238 Rule 14 row 1: operator list

Step 11 **Enter 3 and go to the next step**

Type 3 in **Enter value**. Check the name (1), the type chip **Anomaly (TP103)** (2), **30 Day** (3), the description (4), **Match** AND (5) and the row (6). Click **Next Step** (7).

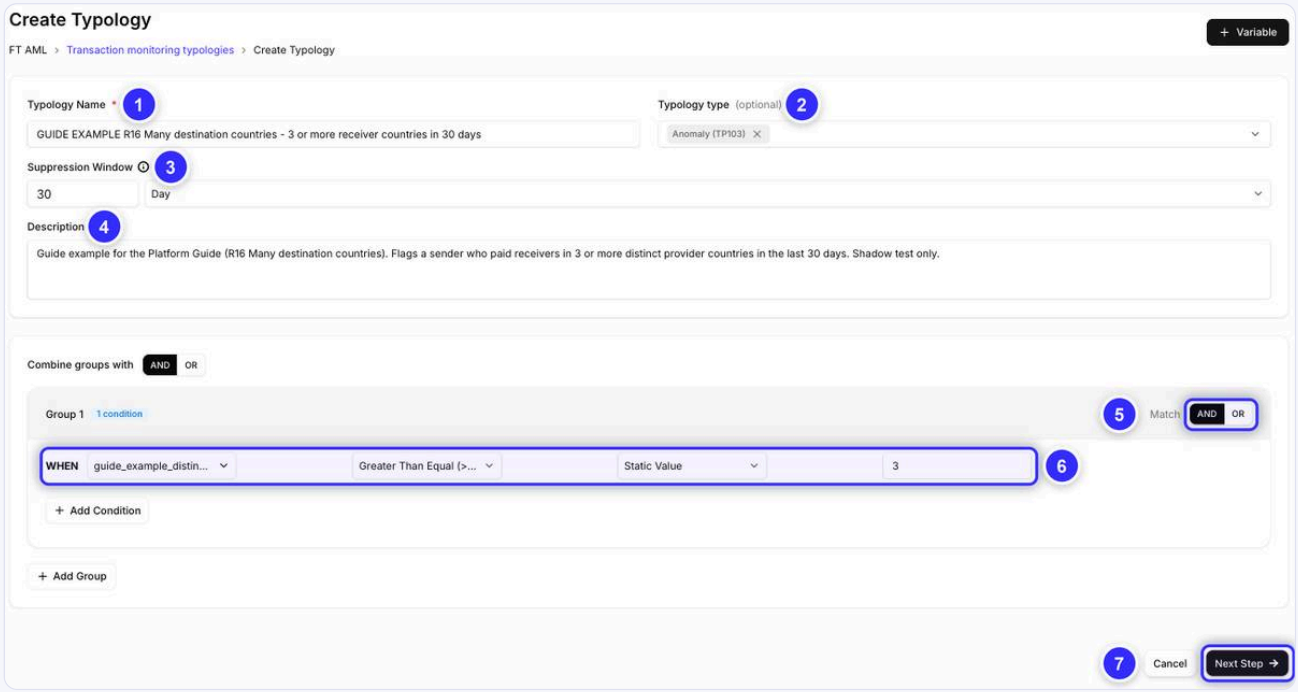


Figure 9.239 The completed Rule 14 page

Part C: Choose the schedule and save

Step 12 **Select the shared schedule and save the draft**

On **Review & schedule rule**, open **Select Schedule**, search for `schedule_2027`, click it and click **Save as Draft**, as in Rule 7.

Step 13 **Check the saved draft**

Wait a few seconds: the page becomes **Update Typology** (1) with the schedule (2), the run sentence (3), **Update** (4), **Dry Run** (5) and **Activate** (6). The screenshot shows the start in force when it was taken (01 Jan 2027).

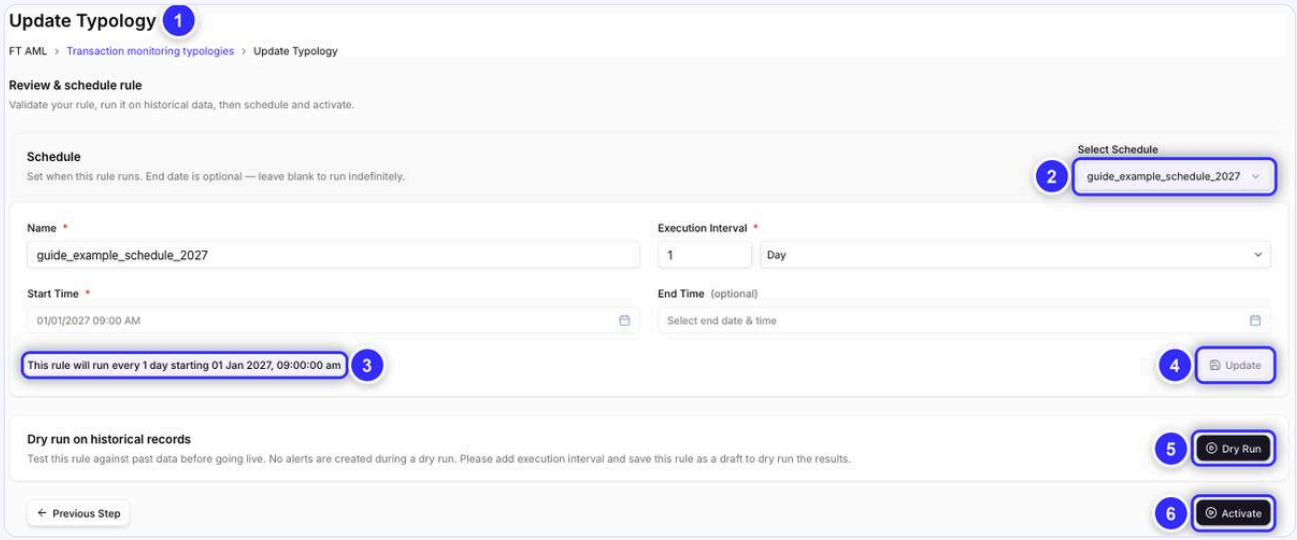


Figure 9.240 Rule 14 after Save as Draft

Step 14 **Check the rule page**

Open the rule from **Transaction Monitoring → Typology**. It shows **Draft** and the rule ID TMR-08102026-001138, created 08 Oct 2026, 06:39:17 pm (1); the summary with **INTERVAL** Every 1 day, **SUPPRESSION** 30Day and **TYPOLOGY** Anomaly (2); the condition, with the operator shown as **Greater Than Equal (>=)** (3); and the variable card `distinct_dest_countries_30d` , Str_agg_count_distinct, **WINDOW** in last 30 day, **GROUP** `sender_entity_id` (4).

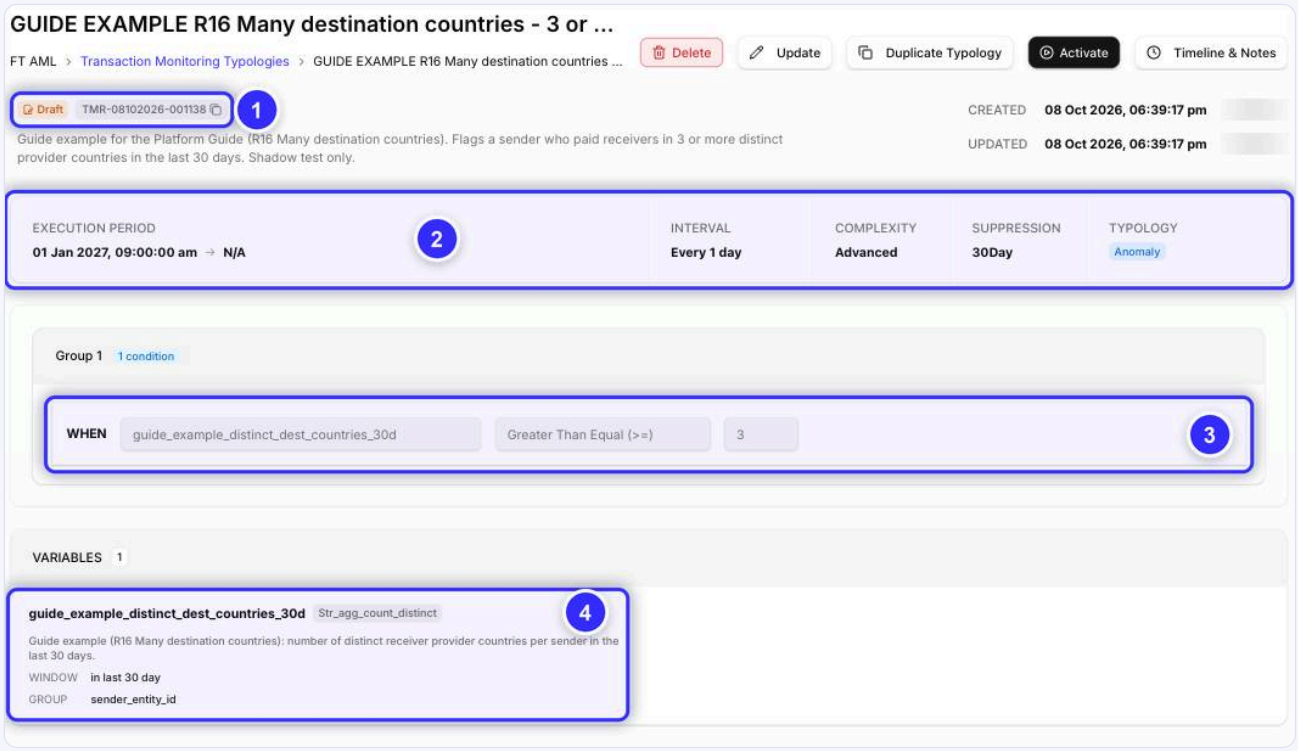


Figure 9.241 The saved Rule 14 as a Draft, TMR-08102026-001138

How it evaluates. Sender A paid receivers in 4 countries within 30 days: 4 >= 3, alert. Sender B paid 20 receivers, all in 1 country: no alert.

Dry-run result. In testing, the rule created 94 alerts at its real threshold: 31, 31, 31 and 1 across the four windows, newest first.

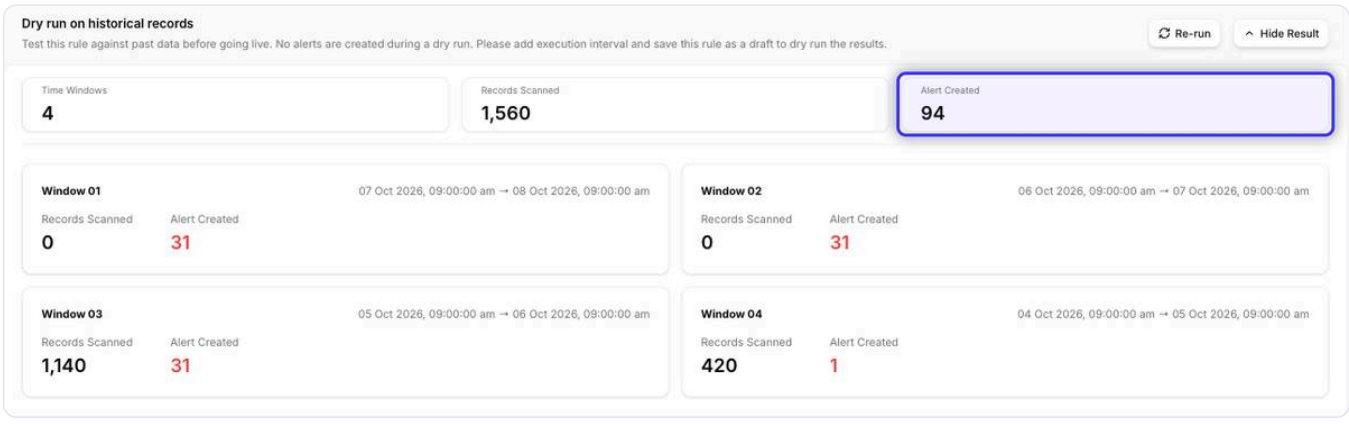


Figure 9.242 Rule 14 dry run at >= 3: 94 alerts

Tuning. Set the number of countries from your customers' normal corridors, and check the volume with a dry run.

Rule 15 · Cross-border volume

RED FLAG **A large total sent abroad**

LOGIC

Adds up the amount the sender sent to a country other than their own in the last 30 days.

WINDOW

30 to 0 Days

THRESHOLD

≥ ₱1,000,000

✓ Verified by positive control

What it detects and why. This rule flags a sender who sent ₱1,000,000 or more abroad within 30 days, counting only payments whose receiver's provider country differs from the sender's. It separates cross-border value from domestic value.

Item	Setting
Variable `crossborder_sum_30d`	**Sum** of `amount`, grouped by `sender_entity_id`, **Days** from 30 to 0, filter `receiver_provider_country` **Not Equal** `sender_provider_country` (**Dynamic**)
Typology type	High Value (HV01)
Suppression Window	30 Day
Condition	Group 1, Match AND: `crossborder_sum_30d` **Greater Than Equal (>=)** Static Value 1000000
Schedule	Existing `schedule_2027` (created in Rule 1): every 1 Day, starting 09 Oct 2026, 09:00 AM, no end time

Part A: Create the variable

Fyscal ARCX → Transaction Monitoring → Variables → + New

Step 1 **Open the form and name the variable**

Click **+ New** on **Variables** and leave **Transaction** selected. Type `crossborder_sum_30d` in **Variable name** (1) and a description such as "Total amount sent per sender in the last 30 days where the receiver provider country differs from the sender provider country." (2).

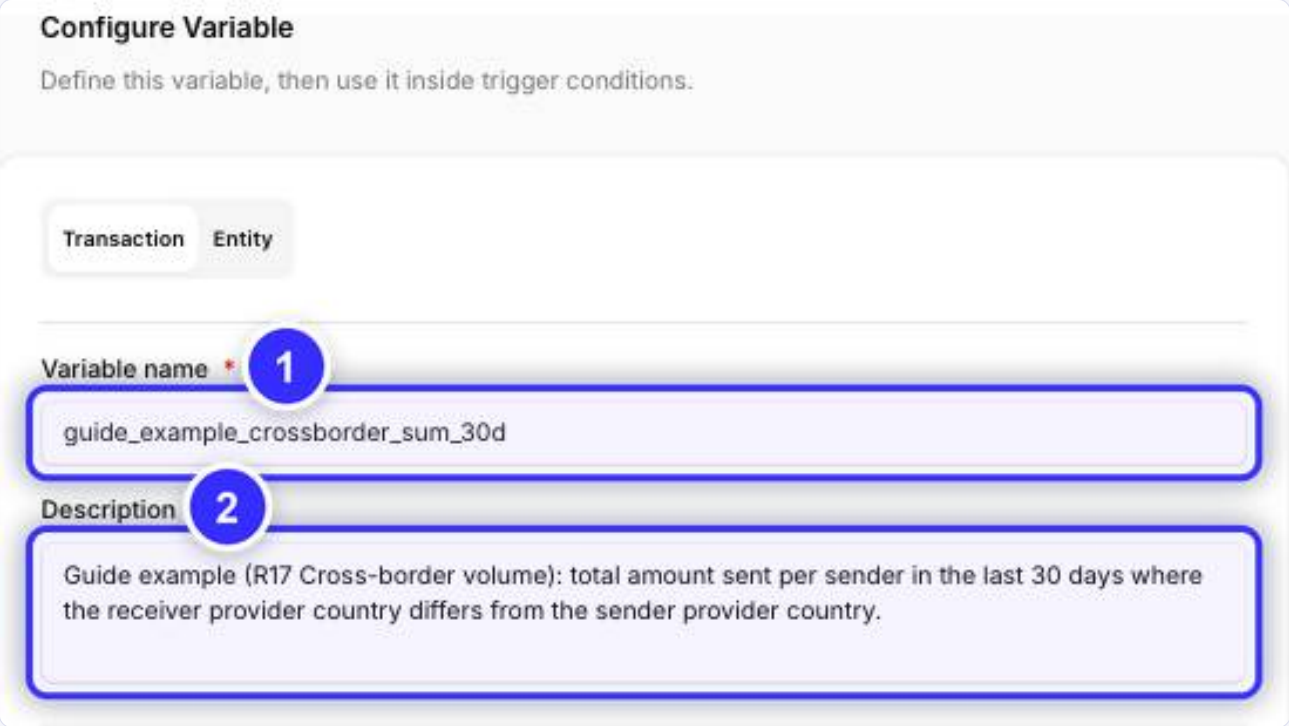


Figure 9.243 Rule 15 variable: name and description

Step 2 **Choose the Field: amount**

Open **Field**, type `amount` and choose `amount`, as in Rule 7.

Step 3 **Choose the Function: Sum**

Open **Function** and choose **Sum** to add the amounts together.

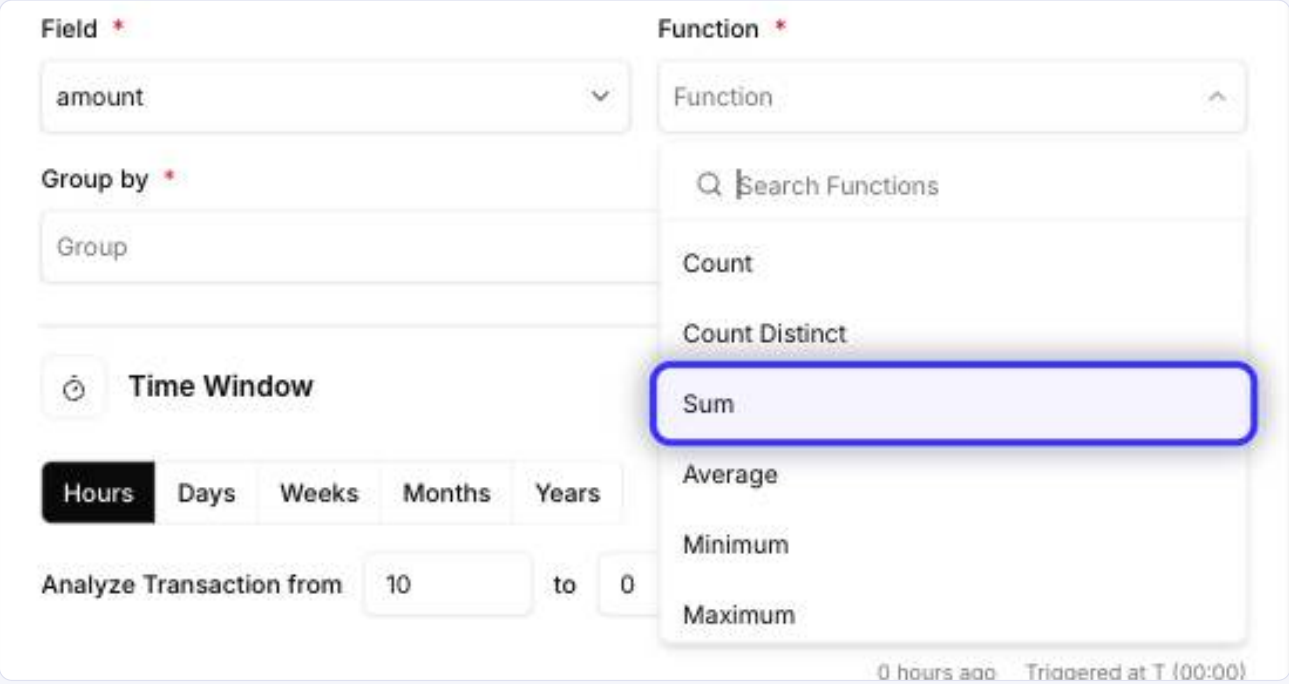


Figure 9.244 Function: Sum

Step 4 **Choose Group by: sender_entity_id**

Open **Group by**, type `sender_entity` in **Search Fields** and choose `sender_entity_id`, so the total is calculated separately for each sender.



Figure 9.245 Group by search: sender_entity_id

Step 5 **Add the filter: receiver_provider_country**

Scroll to **Filters (1)**. In the blank row open **Field**, type `country` and choose `receiver_provider_country`.

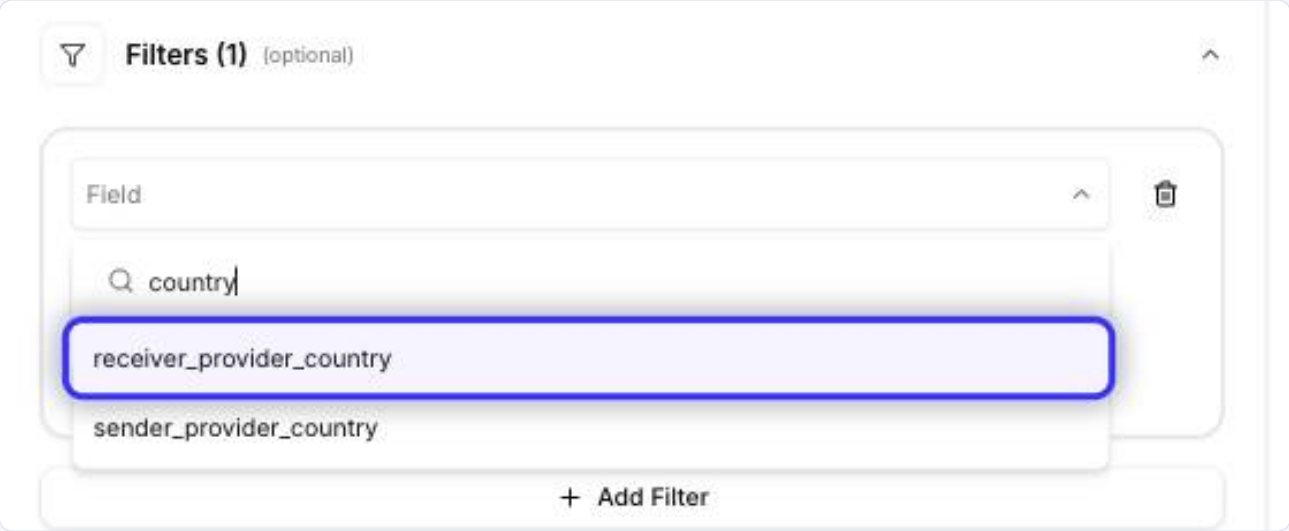


Figure 9.246 Filter row: the field search for country

Step 6 **Choose Not Equal**

Open **Operator...**. For a text field the list is **Equal**, **Not Equal**, **In**, **Not In**, **Contains**, **Not Contains**, then (scroll) **Starts With**, **Ends With**, **Is Null** and **Is Not Null**. Choose **Not Equal**.

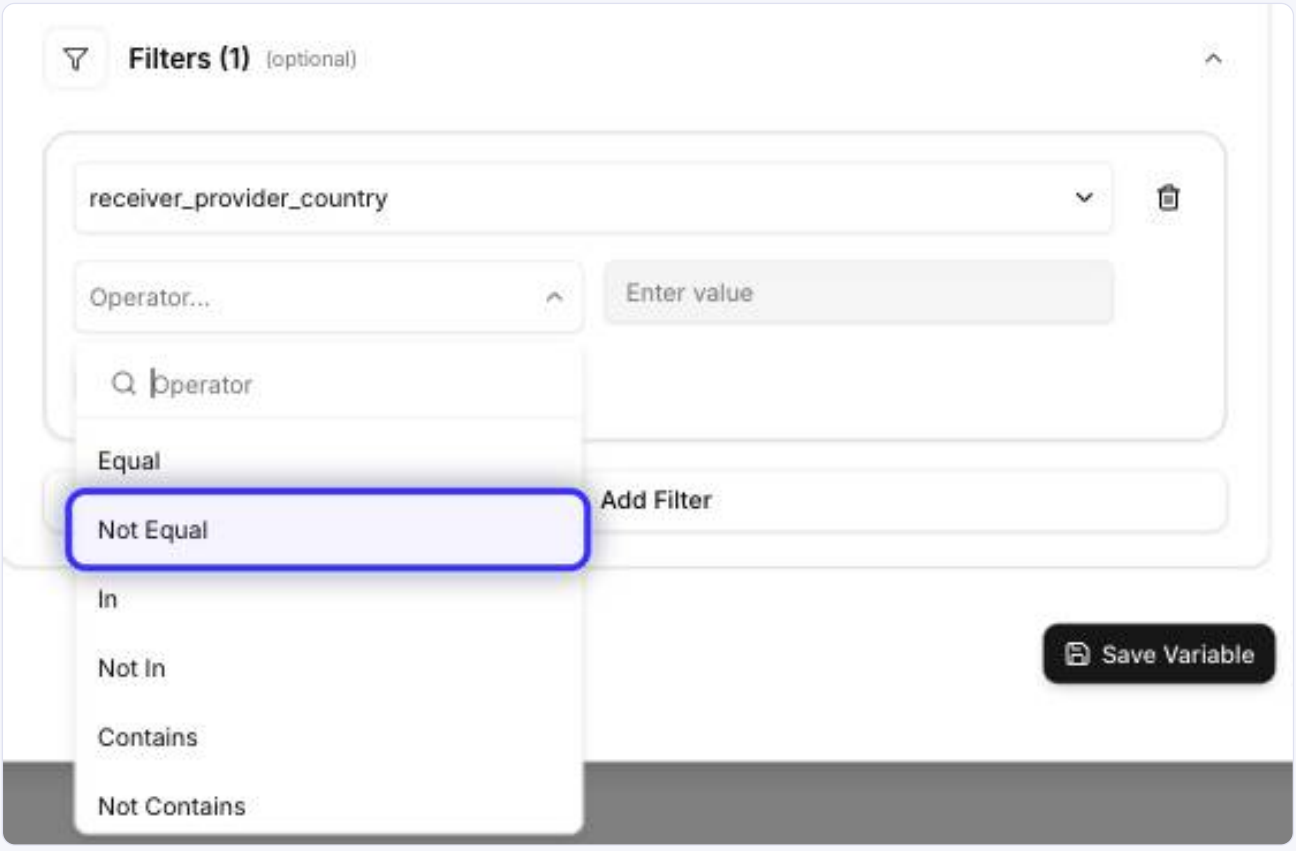


Figure 9.247 Filter operators for a text field: Not Equal

Step 7 **Compare with the sender's country: Dynamic**

Click **Dynamic** (1). The value box becomes **Field...**, a list of other fields. Type `provider_country` and choose `sender_provider_country` (2). A transaction is now counted only when the receiver's provider country differs from the sender's.

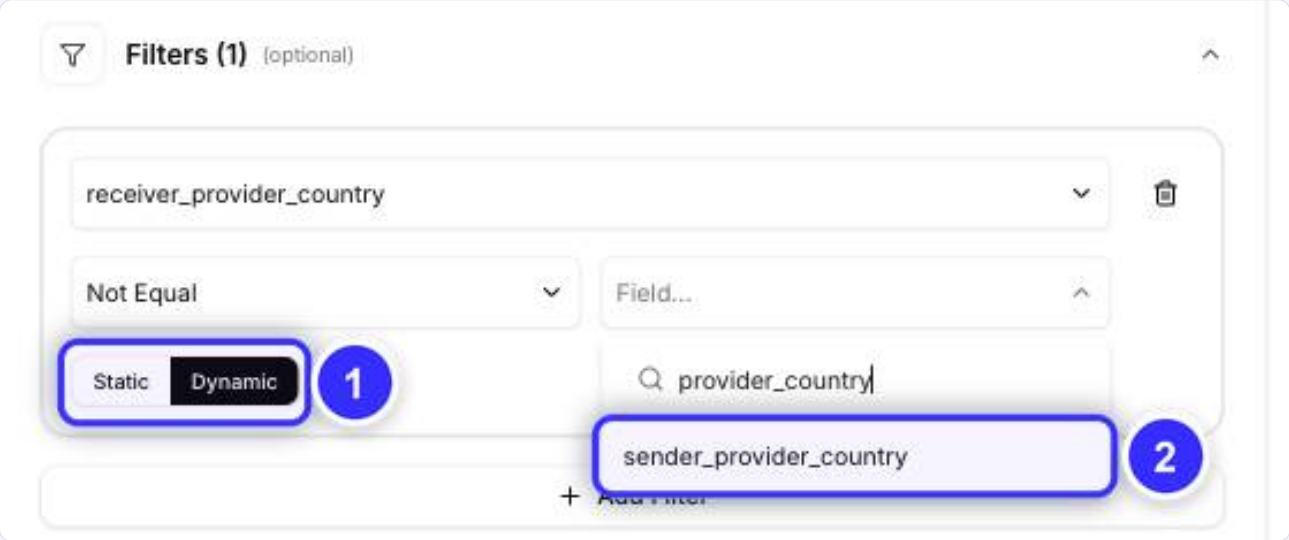


Figure 9.248 Dynamic compare: sender_provider_country

Step 8 **Set the time window: Days, 30 to 0, and save**

Scroll down. Click **Days** (1); the default is **Hours**. Enter 30 in **Analyze Transaction from** and 0 in **to** (2): the 30 days up to the trigger time T. The filter row (3) reads `receiver_provider_country` **Not Equal** `sender_provider_country`, **Dynamic**. Click **Save Variable** (4).

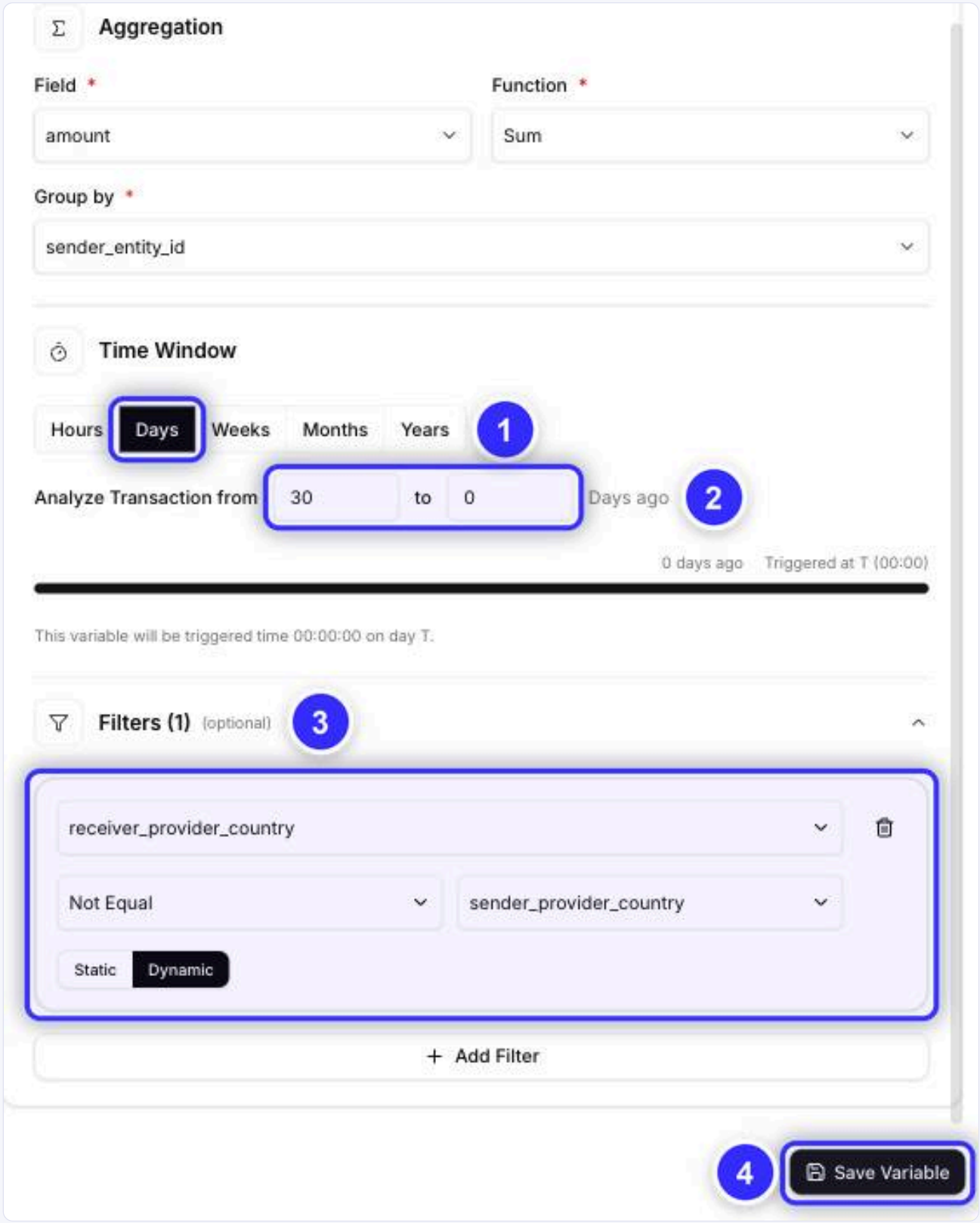


Figure 9.249 Time window 30 to 0 Days ago, the Dynamic filter and Save Variable

Step 9 **Find the variable in the list**

The dialog closes and the variable is the first row of the **Variables** list, here VAR-08102026-000805.

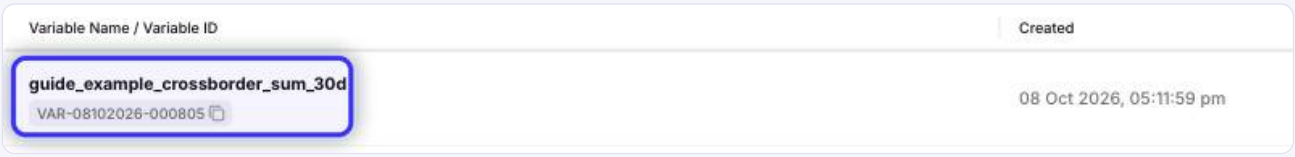


Figure 9.250 Rule 15 variable in the Variables list

Step 10 **Check the saved variable**

Click the row. **View Variable** shows the type tag **NUM_AGG_SUM** (1), the **CREATED** and **UPDATED** times and user (2), `amount` / **Sum** / `sender_entity_id` (3), 30 to 0 **Days ago** (4) and the saved **Dynamic** filter (5).

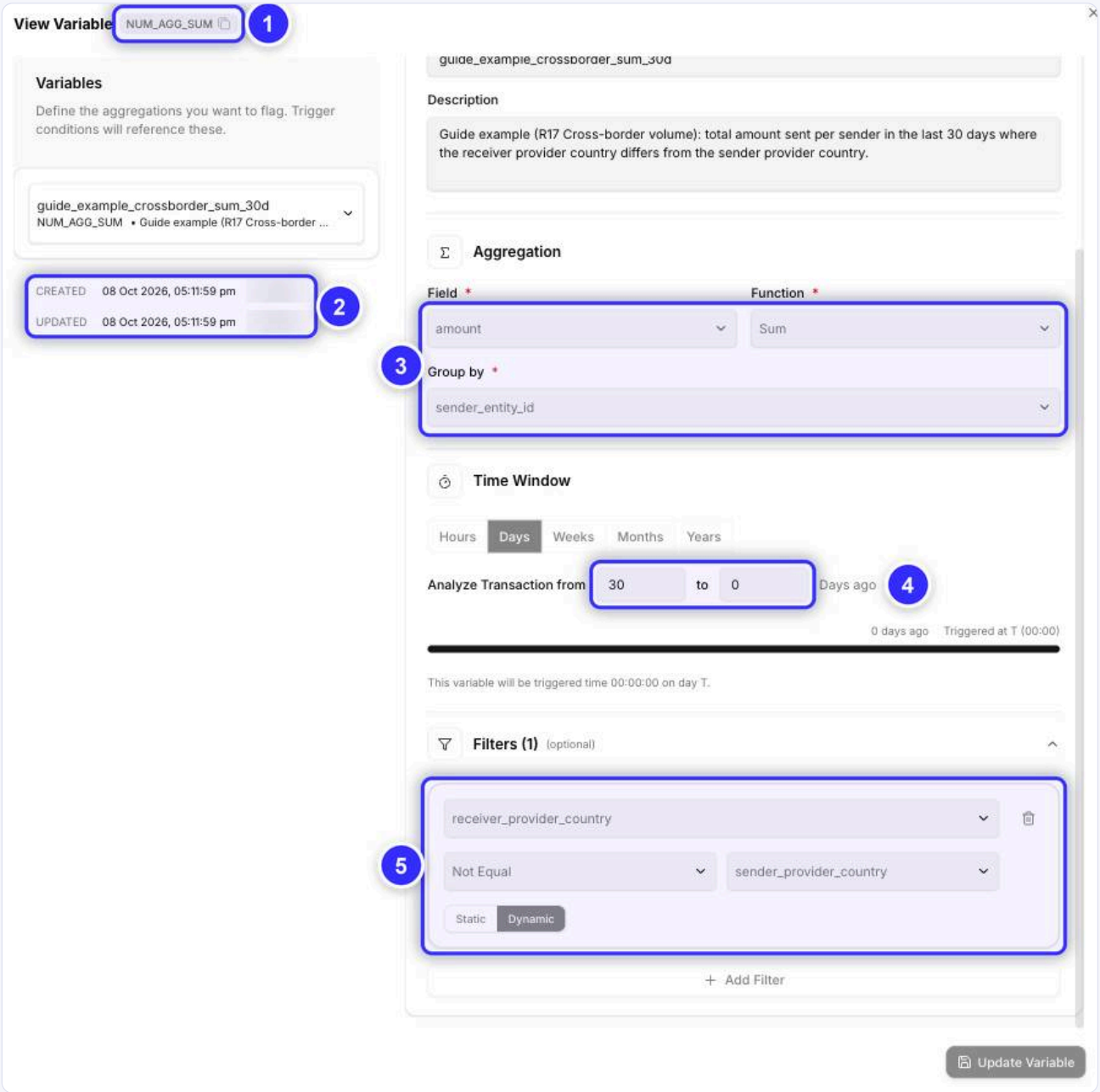


Figure 9.251 View Variable for crossborder_sum_30d

Part B: Create the typology

Fyscal ARCX → Transaction Monitoring → Typology → + New

Step 11 **Fill in the details and choose High Value**

Click **+ New** on **Typology**. Type the name `R17 Cross-border volume - PHP 1000000 or more sent abroad in 30 days` (1). Set **Suppression Window** to 30 and choose **Day** (2): it matches the 30-day window. Write a description (3). Open **Typology type** (4), type `HV01` and click **High Value HV01**.

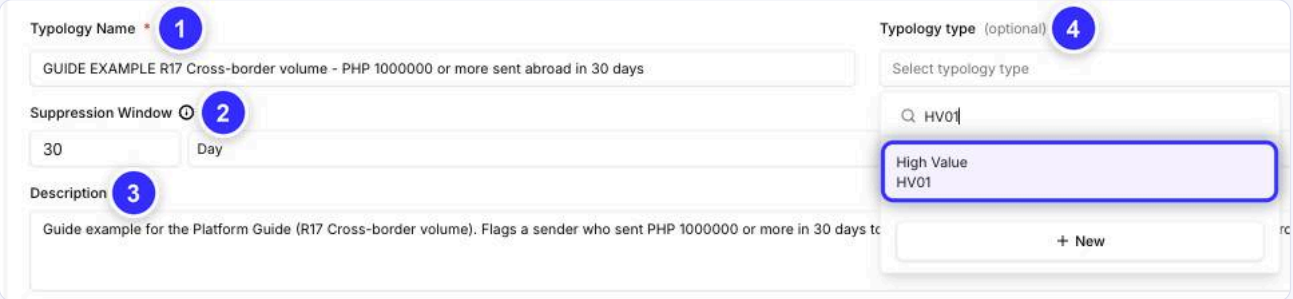


Figure 9.252 Rule 15 details and the Typology type search

Step 12 **Choose the variable, operator and compare-to in row 1**

In **Group 1**, click **Select field**, type part of the name and click `crossborder_sum_30d`. Choose **Greater Than Equal** and keep **Static Value**.

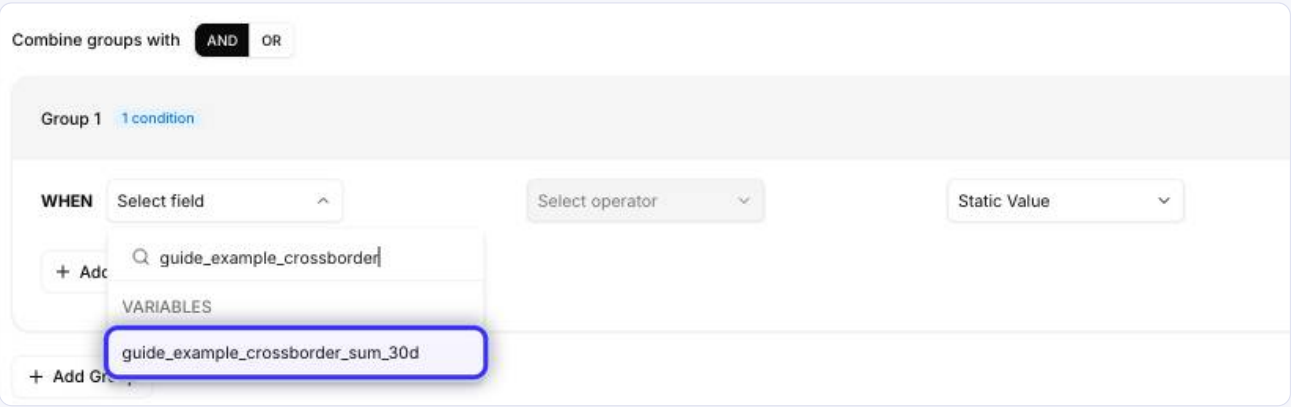


Figure 9.253 Rule 15 row 1: variable search

Step 13 **Enter 1000000 and go to the next step**

Type 1000000 in **Enter value**. Check the name (1), the type chip **High Value (HV01)** (2), **30 Day** (3), the description (4), **Match** AND (5) and the row (6). Click **Next Step** (7).

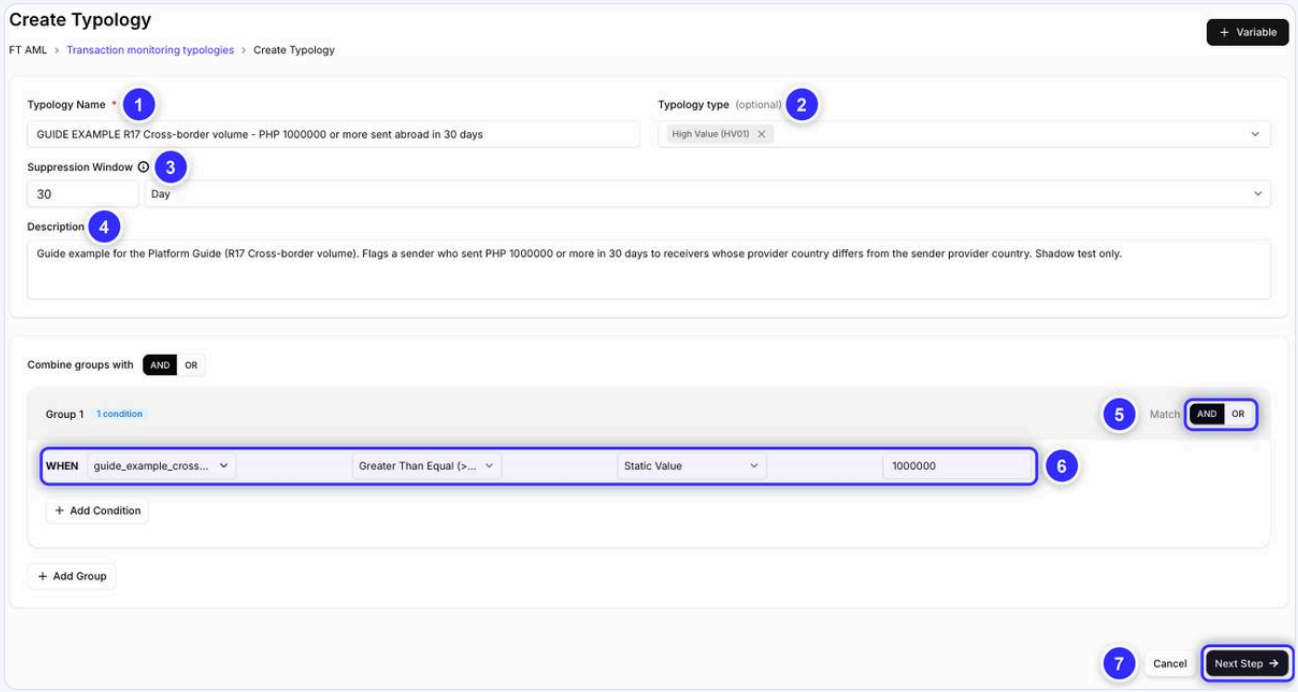


Figure 9.254 The completed Rule 15 page

Part C: Choose the schedule and save

Step 14 **Select the shared schedule and save the draft**

On **Review & schedule rule**, open **Select Schedule**, search for `schedule_2027`, click it and click **Save as Draft**, as in Rule 7.

Step 15 **Check the saved draft**

Wait a few seconds: the page becomes **Update Typology** (1) with the schedule (2), the run sentence (3), **Update** (4), **Dry Run** (5) and **Activate** (6). The screenshot shows the start in force when it was taken (01 Jan 2027).

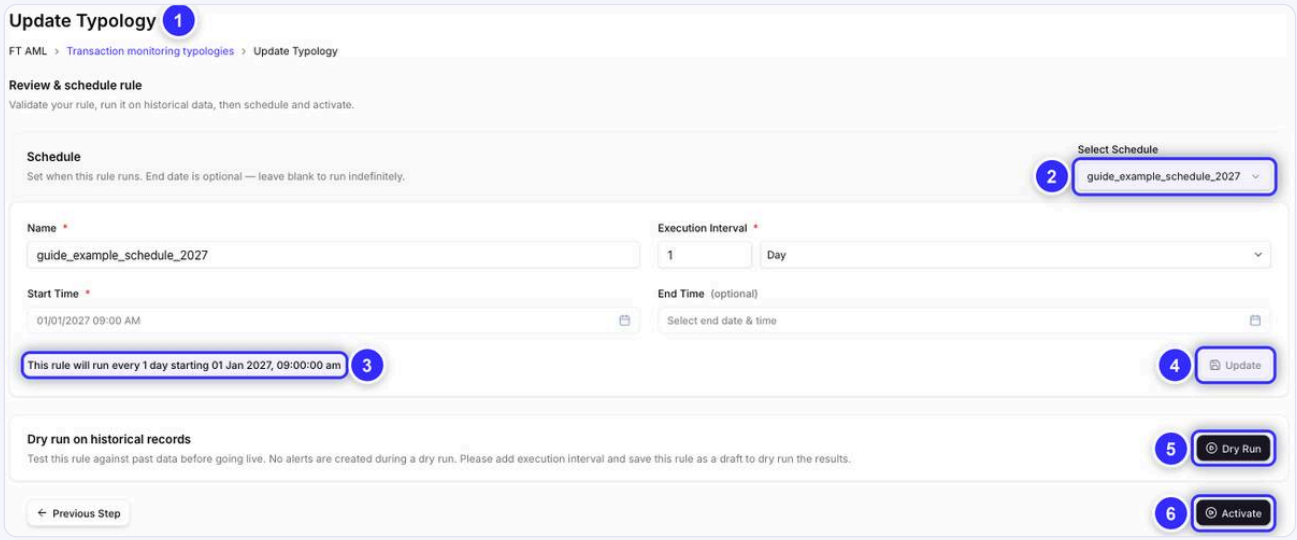


Figure 9.255 Rule 15 after Save as Draft

Step 16 **Check the rule page**

Open the rule from **Transaction Monitoring → Typology**. It shows **Draft** and the rule ID TMR-08102026-001139, created 08 Oct 2026, 06:42:04 pm (1); the summary with **INTERVAL** Every 1 day, **SUPPRESSION** 30Day and **TYPOLOGY** High Value (2); the condition, with the operator shown as **Greater Than Equal (>=)** (3); and the variable card `crossborder_sum_30d` , Num_agg_sum, **WINDOW** in last 30 day, **GROUP** `sender_entity_id` (4). The card does not show the variable's filter; check it on **View Variable**.

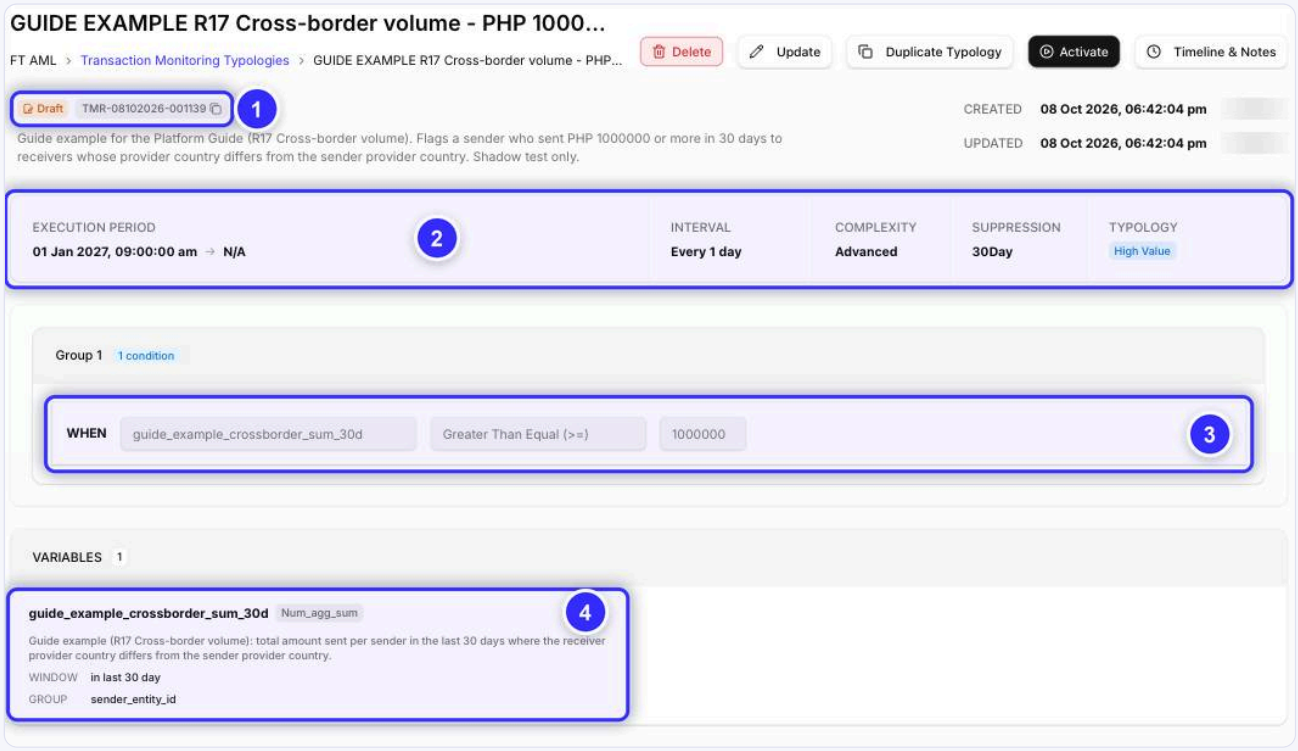


Figure 9.256 The saved Rule 15 as a Draft, TMR-08102026-001139

How it evaluates. Sender A sent ₱700,000 to a receiver abroad and ₱400,000 to another receiver abroad: ₱1,100,000, alert. Sender B sent ₱3,000,000, all to receivers in the same country: the filter leaves nothing to add, no alert.

Dry-run result. In testing, the rule created 0 alerts at its real threshold (>= 1000000) in all four windows: no sender in the test data sent ₱1,000,000 abroad in 30 days. To prove the rule works, the threshold was lowered to >= 1 for one dry run. That created 991 alerts (276 / 278 / 282 / 155 by window, newest first), then the threshold was restored and a new dry run returned 0 again. See Test a typology with Dry Run for the method. The control also shows the filter at work: 991 alerts against 6,512 for the unfiltered 30-day total of Rule 3 at the same threshold.

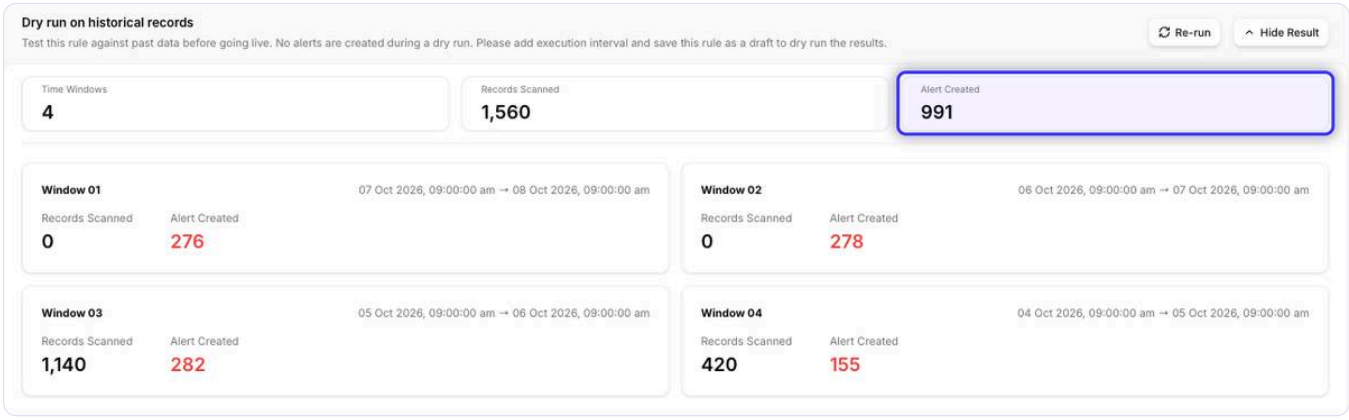


Figure 9.257 Rule 15 positive control (threshold temporarily >= 1): 991 alerts

Tuning. Set the amount from your cross-border risk appetite. Variant, not tested with Dry Run: to cover only some countries, use **In** on `receiver_provider_country` instead of the Dynamic compare (see proposal P1).

Test a typology with Dry Run

Fyscal ARCX → Transaction Monitoring → Typology → rule → Update → Next Step

A dry run runs a saved draft against past records and reports how many alerts it would have created. Every rule in this chapter was dry-run on 08 Oct 2026; the results are in the Rule index.

Step 1 **Open the rule's Review page**

Open the saved draft, click **Update**, then **Next Step**. **Review & schedule rule** shows the card **Dry run on historical records** (1): "Test this rule against past data before going live. No alerts are created during a dry run." **Dry Run** (2) is available once the rule is saved as a draft with a schedule; **Activate** (3) is next to **Previous Step**.

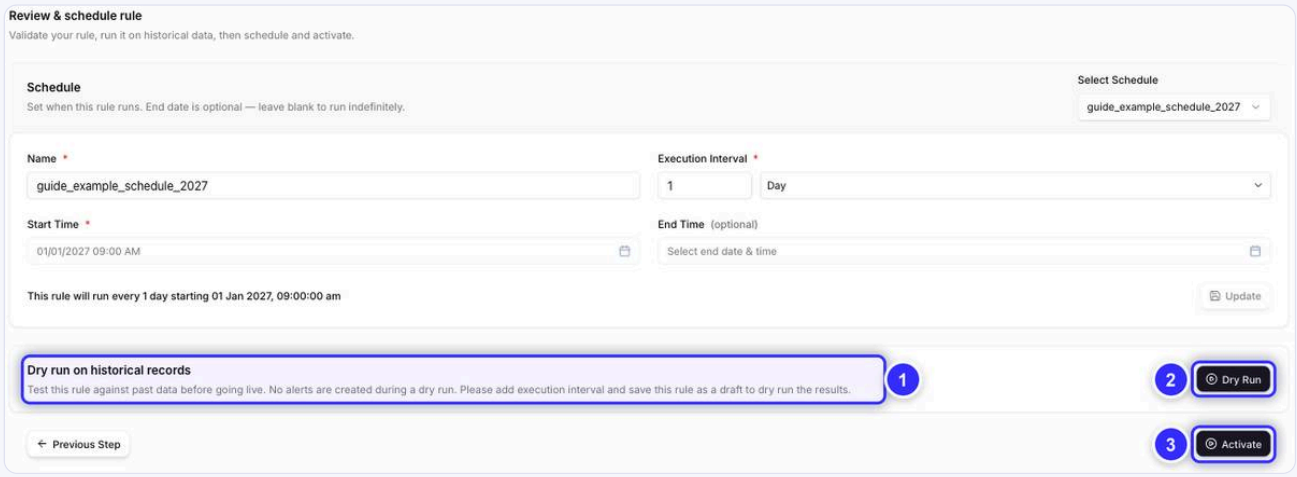


Figure 9.258 Review & schedule rule with the Dry run card (Rule 1)

Step 2 **Click Dry Run**

Click **Dry Run**. No dialog or date choice appears. When the run finishes, the result opens in the card, **Dry Run** is replaced by **Re-run** and **Hide Result** (1), and the message "Dry run executed successfully" (2) appears at the bottom right.

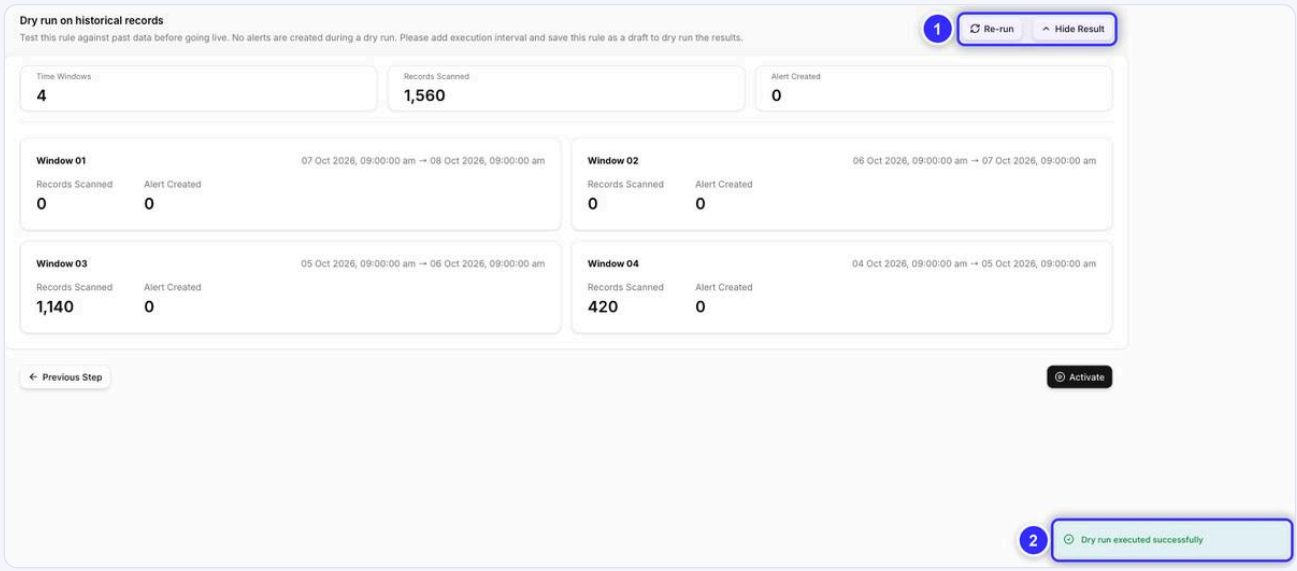


Figure 9.259 The finished dry run: Re-run, Hide Result and the success message

Step 3 **Read the result**

The top row (1) shows **Time Windows**, **Records Scanned** and **Alert Created** for the whole run. Below, one card per window (2) shows the window's dates and its own **Records Scanned** and **Alert Created**. In the example the run tested 4 windows of one day each, the schedule's interval, from 04 Oct 2026, 09:00 am to 08 Oct 2026, 09:00 am, newest first, and scanned 1,560 records. Rule 1 created 0 alerts. **Re-run** (3) runs it again.

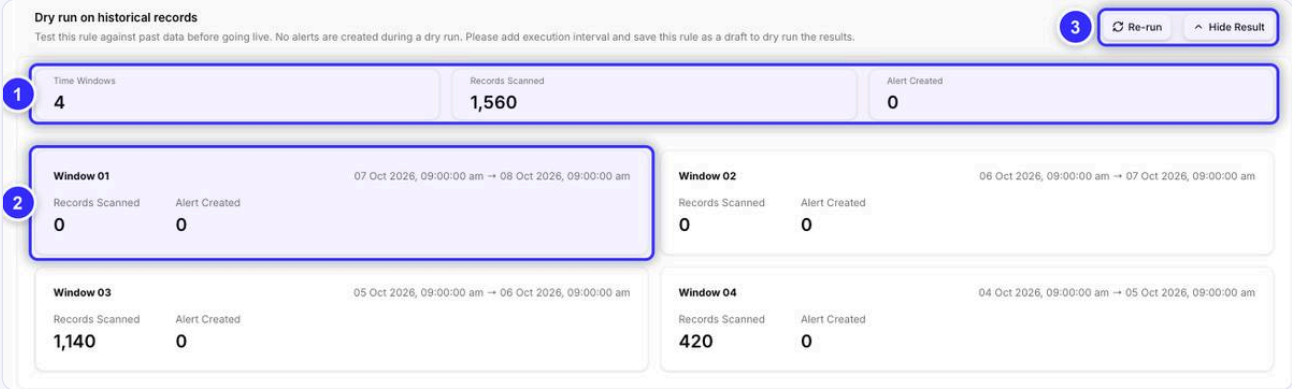


Figure 9.260 Dry-run result for Rule 1: 4 windows, 1,560 records, 0 alerts

Step 4 **Compare with a rule that finds something**

Rule 5 (fan-out) created 240 alerts (1), 60 in each window. Window 01 (2) scanned 0 records and still created 60 alerts: the window's **Records Scanned** counts the records in that day, while the rule's variable looks back 7 days. A rule with a 1-day variable, such as Rule 2, created alerts only in the windows that contained records.

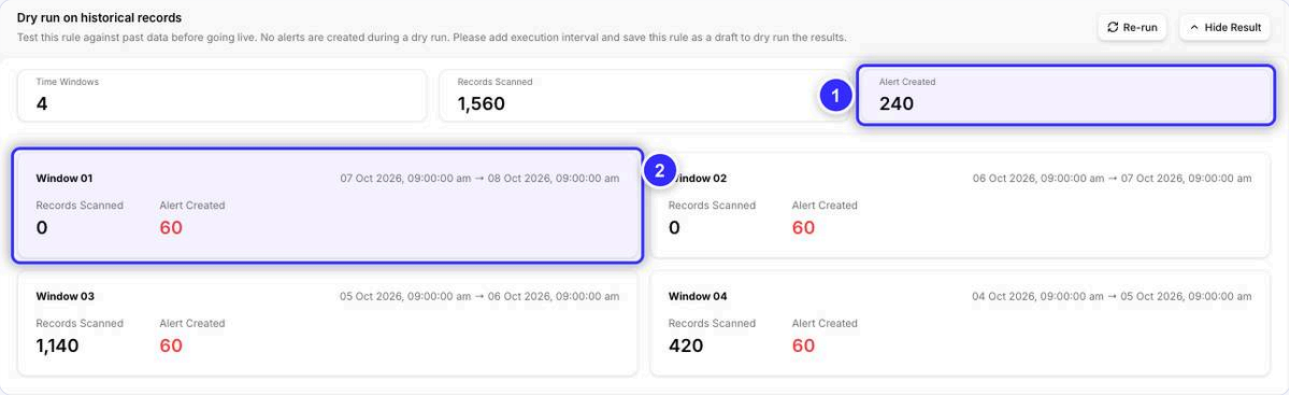


Figure 9.261 Dry-run result for Rule 5: 240 alerts, 60 per window

What a dry run shows

The result shows counts per window only. It does not list the senders or transactions that matched, and the counts cannot be opened. No alerts are created.

Step 5 **Edit the rule: the dry run is erased**

If you change the rule or its schedule and click **Update**, the dialog **Update Typology** says "Your dry run results would be erased once you update and save the rule again". Click **Update** to save; the result is cleared and you run the dry run again. Until you confirm, the page waits behind the dialog, so look for it if **Update** seems to do nothing. While the form has unsaved changes, **Re-run** and **Activate** are greyed out.

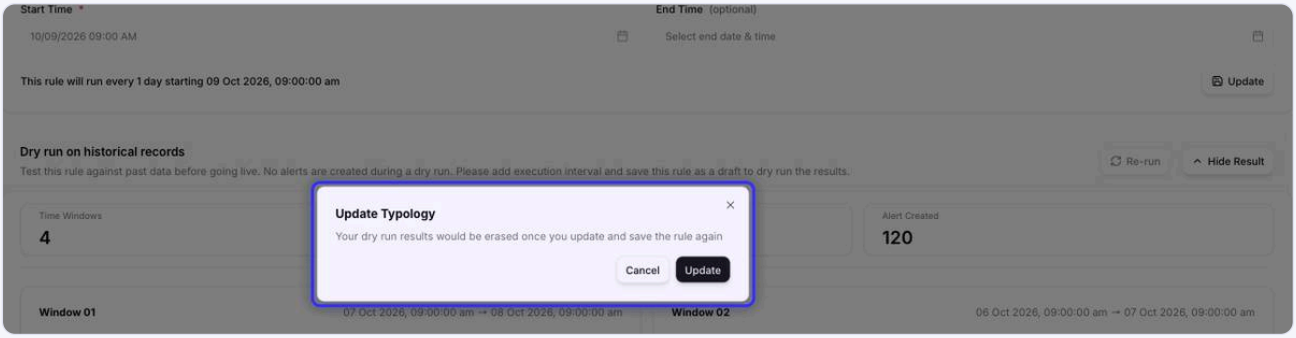


Figure 9.262 Update Typology: Your dry run results would be erased

Judge the result: 0 is not proof

A result of 0 can mean that the data has no such pattern, or that the rule cannot read the data, for example because a field is empty. To tell them apart, run a positive control: lower the threshold so that any matching record would alert, check that alerts appear, then restore the threshold. The zero-alert rules in this chapter were all checked this way. Diagram 9.2 in Building blocks summarises the decision.

Step 6 **Lower the threshold for one run**

In the rule, change the threshold to a value that must match if the data is read, here **Greater Than Equal** 1 instead of 3. Click **Update**, confirm the dialog, click **Next Step** and run **Dry Run**. Rule 1 created 4 alerts (1), so the variable, its filters and the condition work.

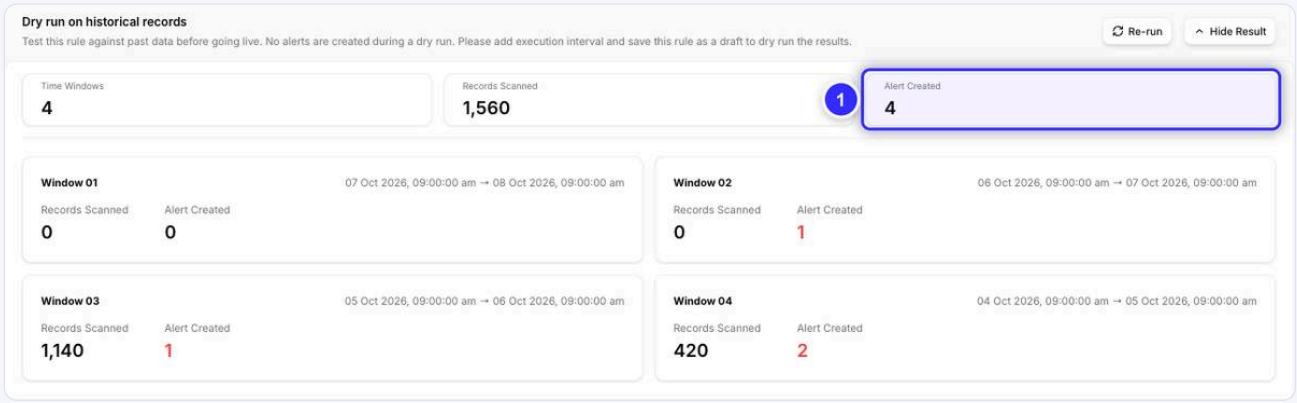


Figure 9.263 Positive control for Rule 1: threshold temporarily >= 1, 4 alerts

Step 7 **Restore the real threshold**

Change the threshold back (here 3), click **Update**, confirm, and run the dry run again. It returns to 0 alerts (1). Do not request activation with the lowered threshold.

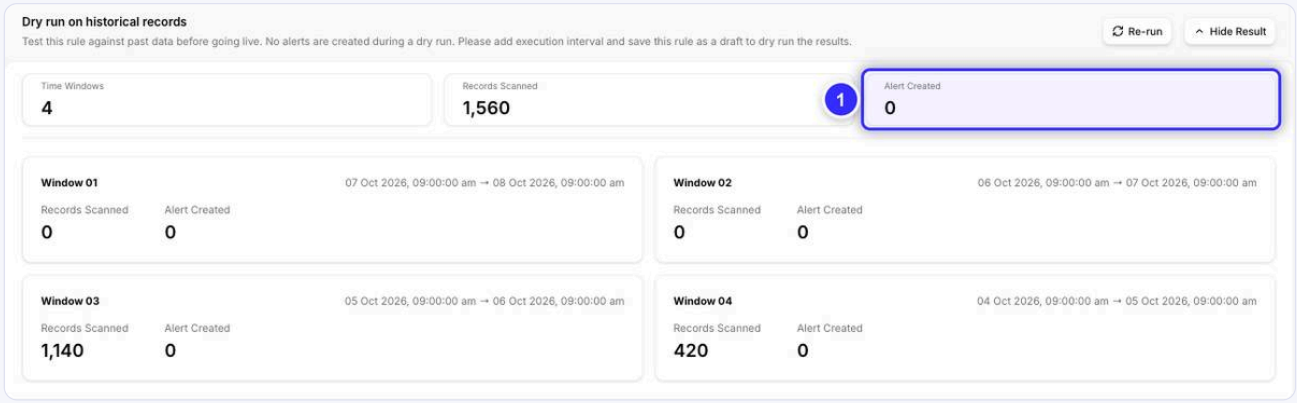


Figure 9.264 Rule 1 with the threshold restored to >= 3: 0 alerts

Tune a noisy rule

If a rule creates more alerts than your team can review, raise the threshold step by step and re-run.

Step 8 **Start from the first result**

Rule 11 (many IP addresses) was first saved at 5 or more IP addresses in 7 days. The dry run created 758 alerts in four days of data, about 190 a day.

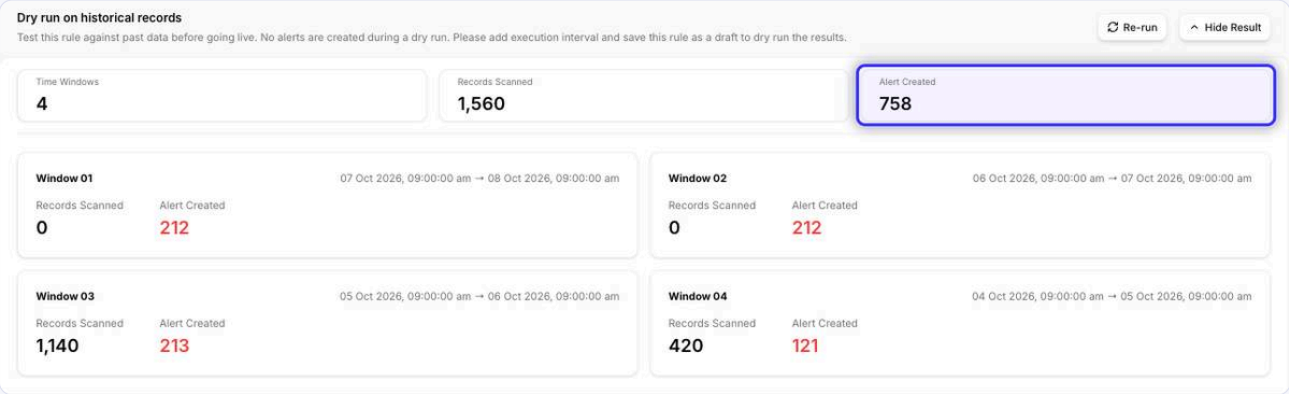


Figure 9.265 Rule 11 at >= 5: 758 alerts

Step 9 **Raise the threshold and re-run**

At 10 the rule created 240 alerts. At 20 it created none. Each change needs **Update**, the confirmation and a new dry run.

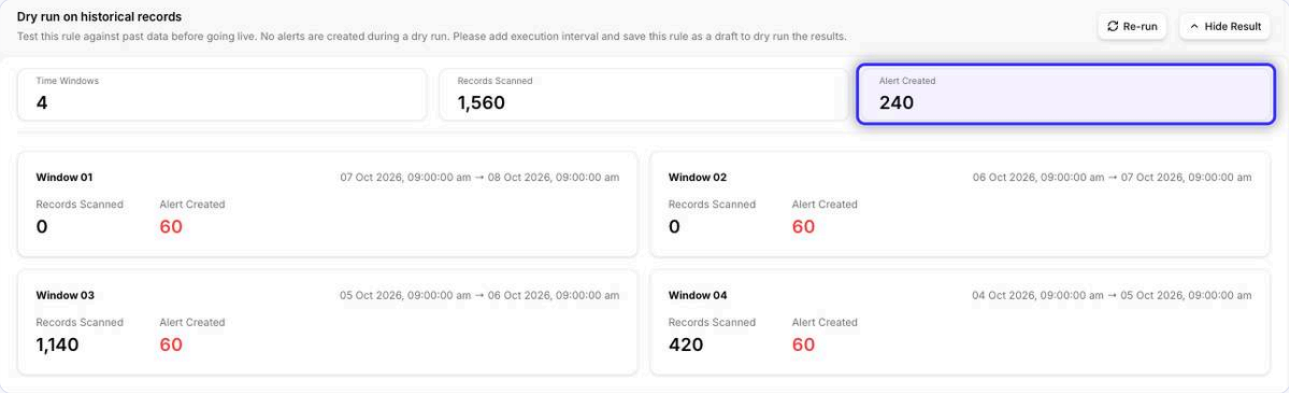


Figure 9.266 Rule 11 at >= 10: 240 alerts

Step 10 **Settle on a value and rename the rule**

At 15 the rule created 120 alerts, 30 a day (see Rule 11). The example was saved at 15 and its name and description were changed to say 15, so the name still describes the condition.

Request Shadow activation

Fyscal ARCX → Transaction Monitoring → Typology → rule → Update → Next Step → Activate

In Shadow Mode a rule runs on live data and its alerts are shown on the rule's page, not sent to Alert Manager. Activation is a Maker Checker request: you (the maker) submit it, and a checker reviews it in Maker Checker Approval. While the request waits, the rule stays a **Draft**.

Step 1 **Click Activate and read the modes**

On **Review & schedule rule**, click **Activate**. **Activation Mode** offers **Shadow Mode** (1), “Alert generated against live data will be shown in rule detail page.”, and **Published Mode** (2), “Alert from this rule will flow into Alert Manager.” Published is a separate mode and is not covered here. **Activate** (3) continues.

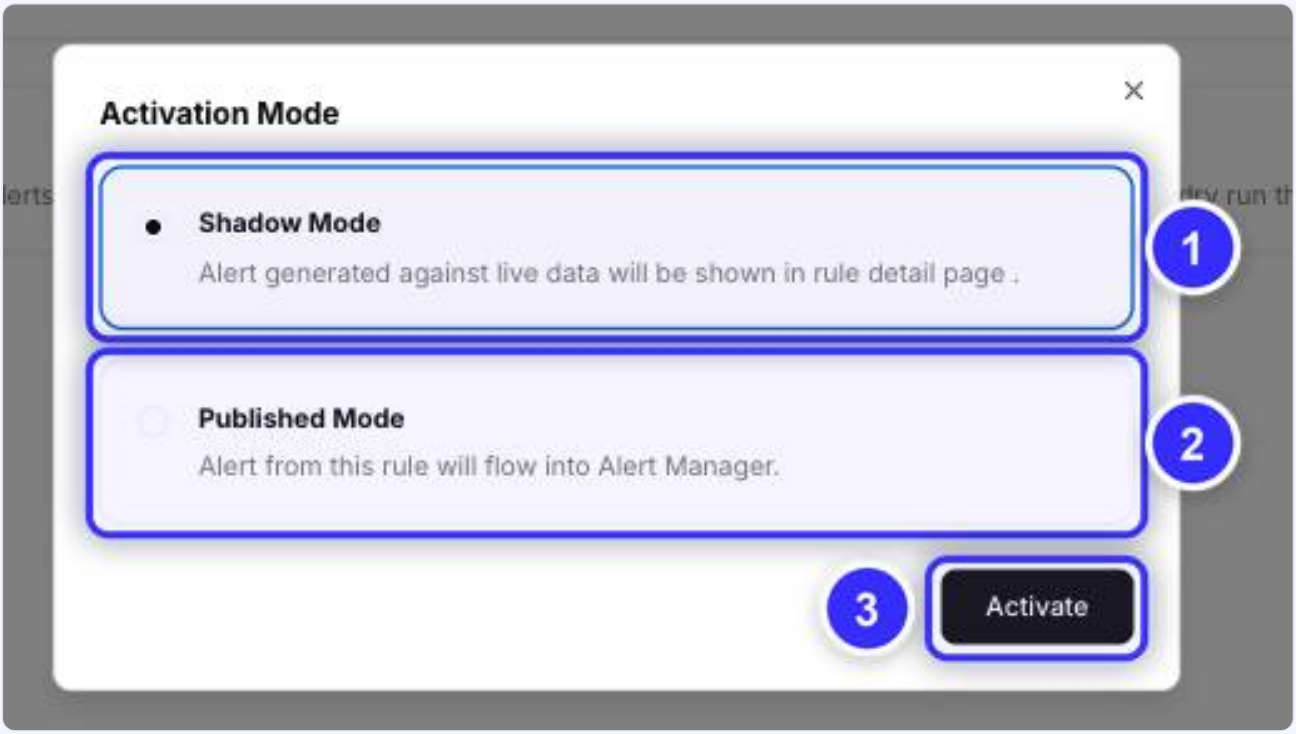


Figure 9.267 Activation Mode: Shadow Mode and Published Mode

Step 2 **Select Shadow Mode**

Click the **Shadow Mode** card so that its radio button is filled (1), then click **Activate** (2).

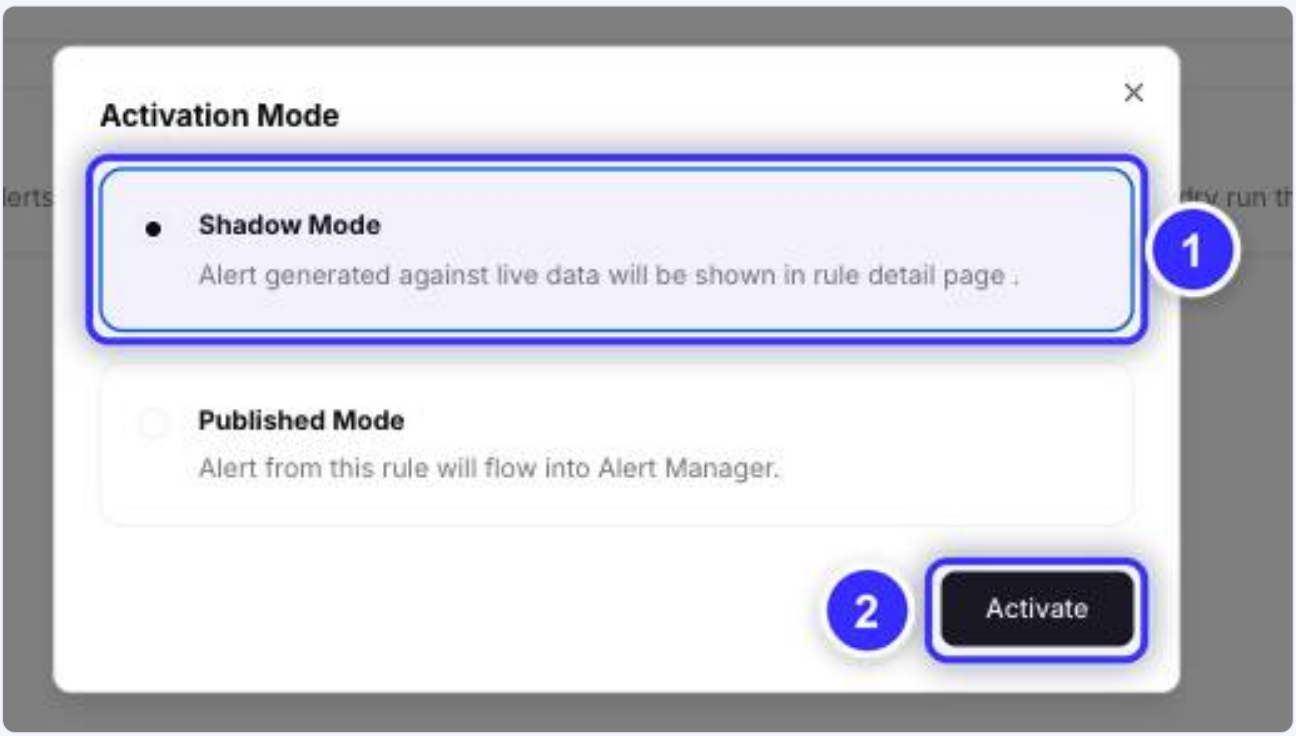


Figure 9.268 Shadow Mode selected

Step 3 **Read the Submit Request dialog**

Submit Request asks for a **Reason** (1), required, and optional **Supporting Documents** (2): 1 file, max 2 MB, .jpg, .jpeg, .jpe, .png, .pdf, .webp or .md, added with **Attach File**. **Confirm** (3) is greyed out until a reason is entered.



Figure 9.269 Submit Request: Reason, Supporting Documents and Confirm

Step 4 **Write the reason and confirm**

Type a reason the checker can act on (1), for example the rule's purpose, the dry-run result and "start in Shadow". The example used a short test reason. Click **Confirm** (2).

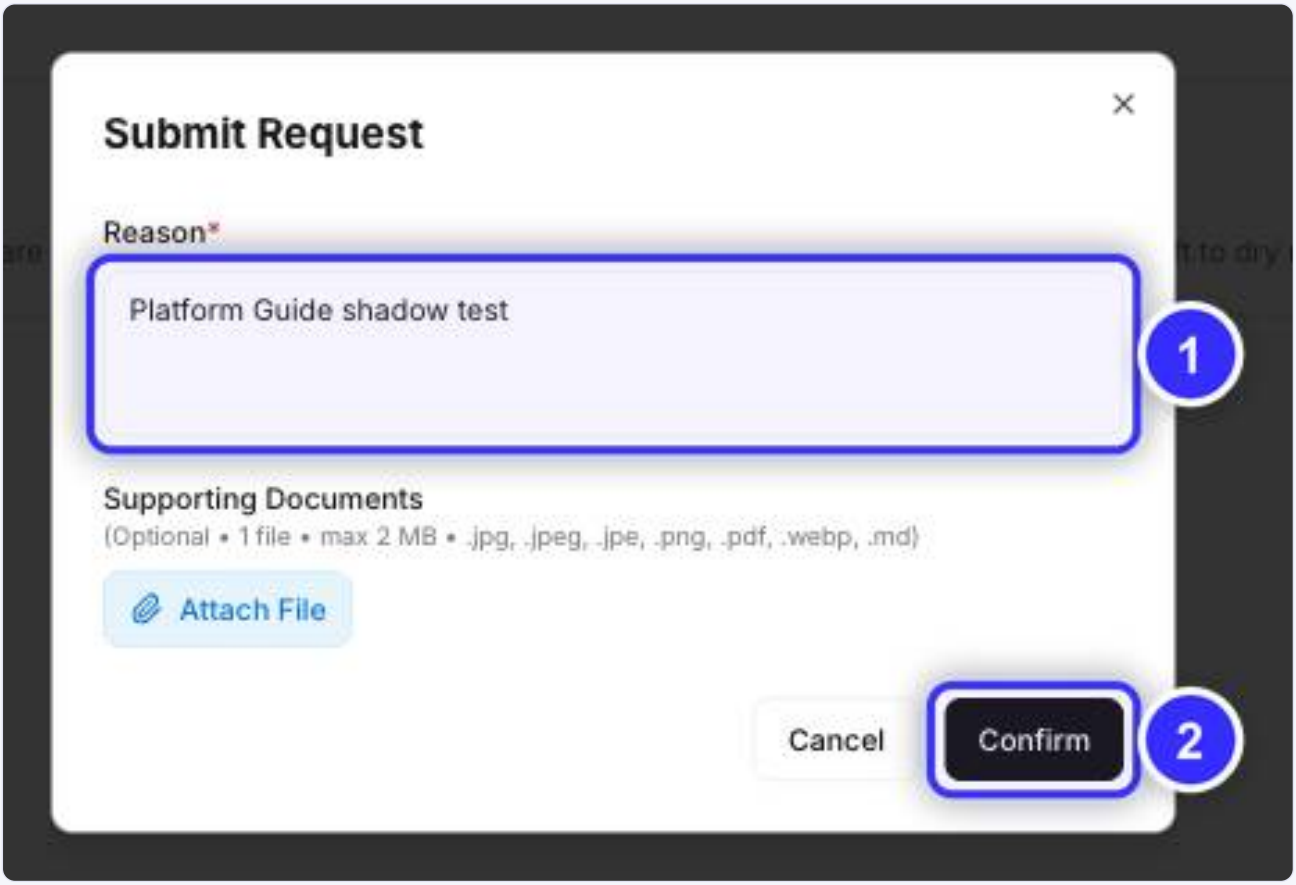


Figure 9.270 Reason entered; Confirm available

Step 5 **Read the confirmation**

The typology list opens and a message gives the request's ticket ID: "Submitted for governance review (ticket AMLTM_...). It will be applied once approved."



Figure 9.271 Submitted for governance review, with the ticket ID

Step 6 **Check the rule: it is still a Draft**

Open the rule. It still shows **Draft** (1) and **Activate** (2): the request has not changed the rule. The **EXECUTION PERIOD** (3) starts at the schedule's start, 09 Oct 2026, 09:00:00 am.

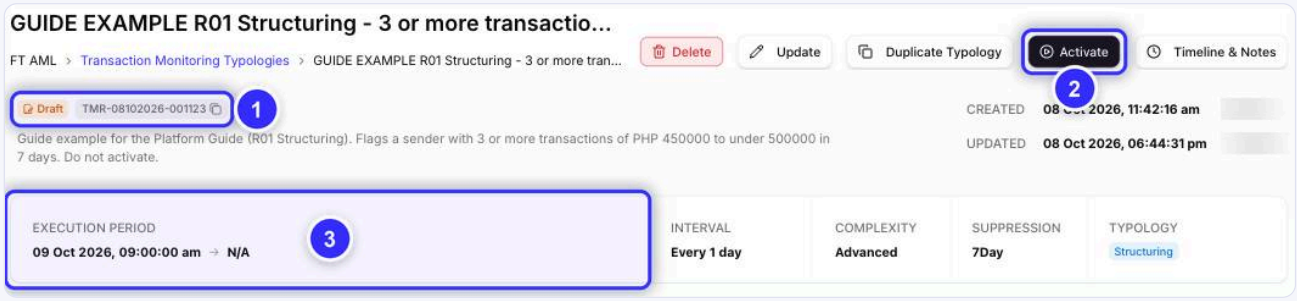


Figure 9.272 Rule 1 after the request: still Draft

Fyscal ARCX → Maker Checker Approval → Tickets

Step 7 **Find the request in Tickets**

Go to **Maker Checker Approval → Tickets**. The request is the top row: Request ID 991, **Activate Typology**, status **Pending**, with the maker and the time it was created.



Figure 9.273 Tickets: the Activate Typology request, Pending

Step 8 **Open the ticket**

Click ⋮ in **Actions** and choose **View**. (**Watch** is the other choice.)

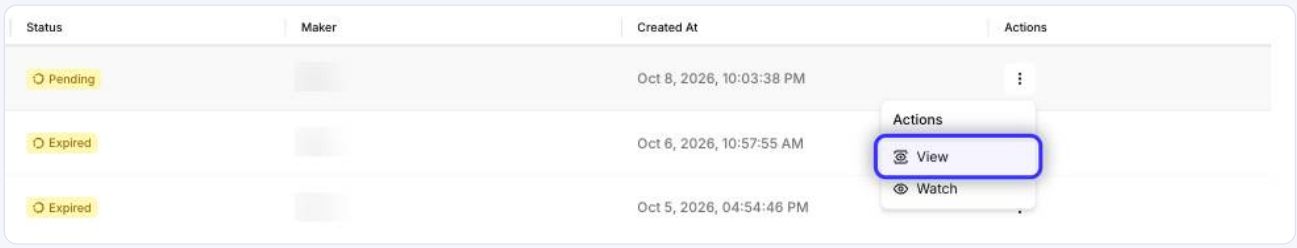


Figure 9.274 The row's Actions menu: View and Watch

Step 9 **Read the request**

Request Details shows the request ID and **Pending** (1); the **Domain** Fyscal ARCX/Transaction Monitoring/Typology, the **Action** Activate Typology and **Checker Progress** 0 / 1 checkers acted (2); the **Reason** (3); and under **Data Difference** (4) the change requested: **Activation Mode** from - to shadow. Below, **Additional Context** gives the rule name and URL. Further down, the maker's view has a **Remarks** box and **Withdraw**.

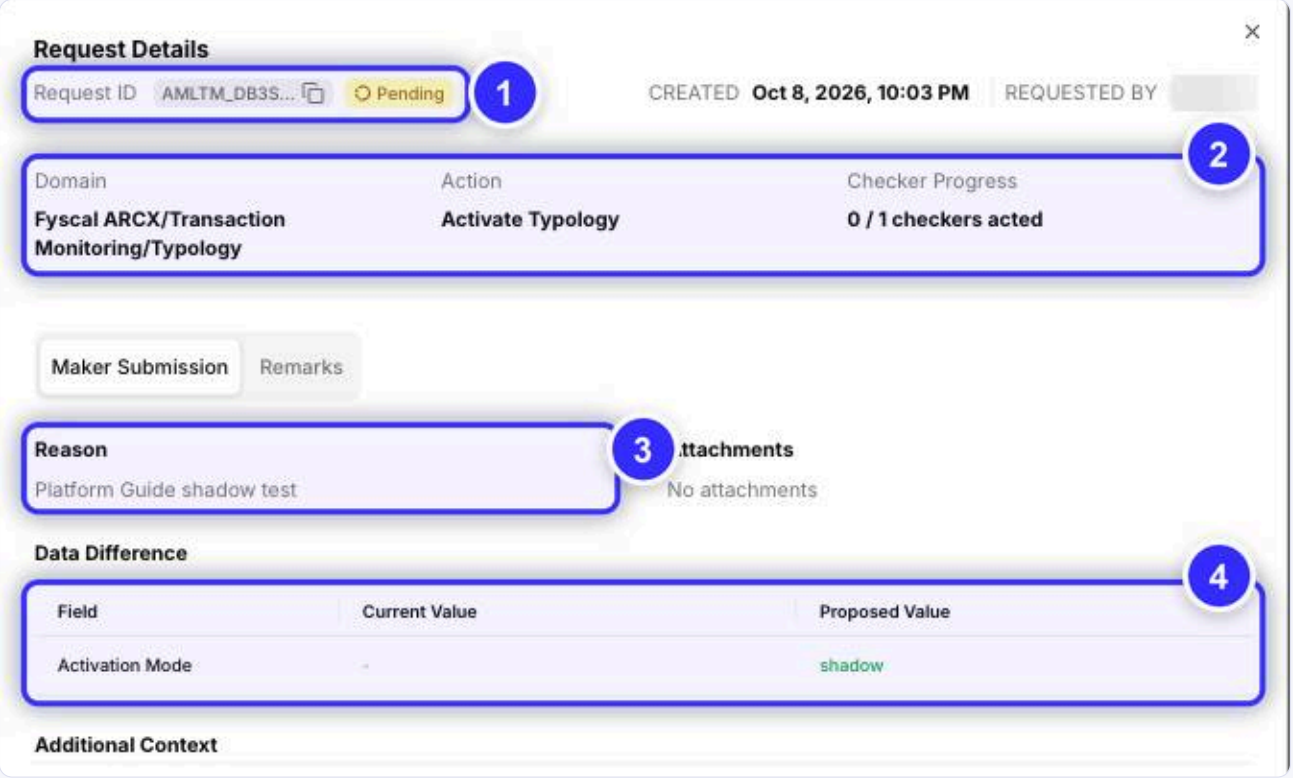


Figure 9.275 Request Details for an Activate Typology request

Every rule in this chapter was submitted for Shadow activation on 08 Oct 2026: 15 requests, numbers 991 to 1005. No checker acted on them, and by 11 Oct 2026 all 15 showed **Expired**, so the rules are still Draft. Rule 4 was rebuilt on 15 Oct 2026 as a new draft (see Rule 4). A request has to be approved before it expires; if it expires, submit a new one.

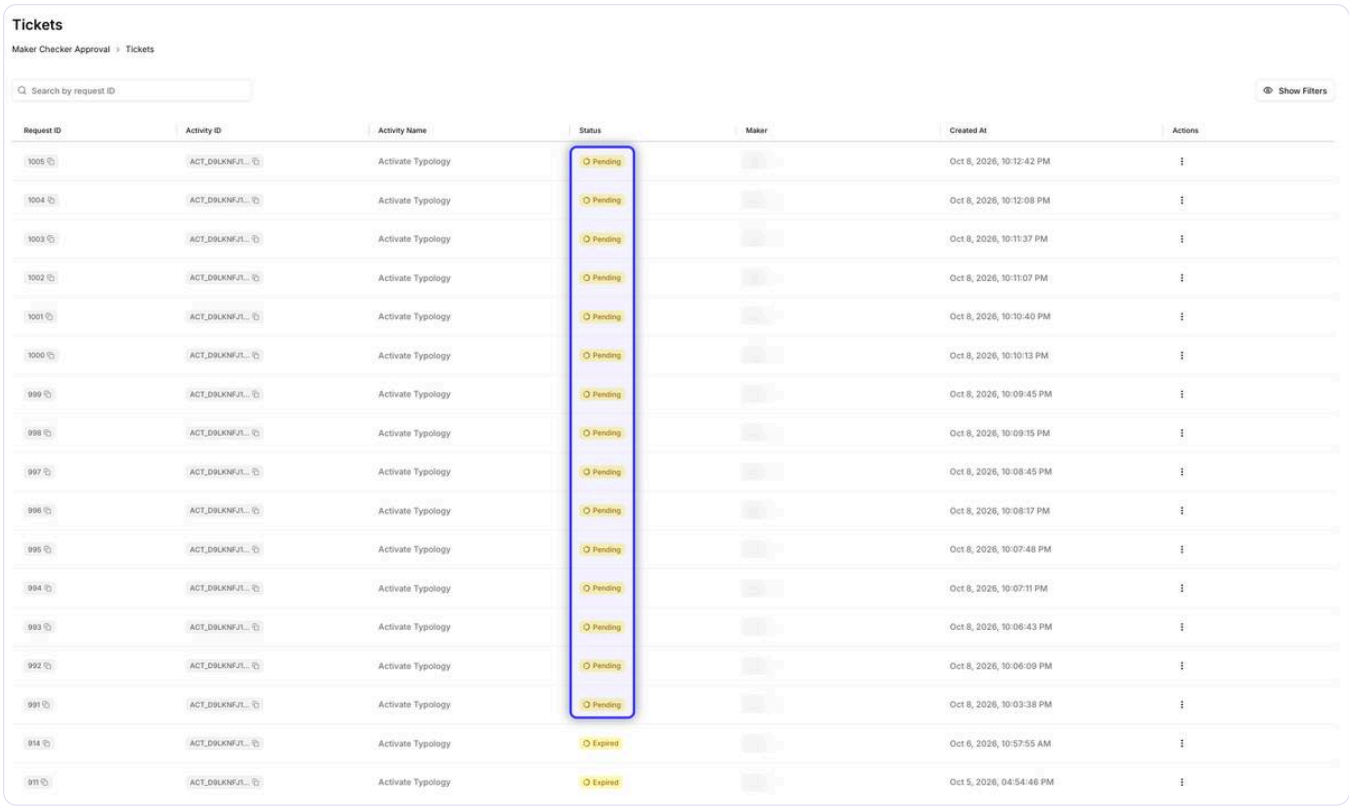


Figure 9.276 Tickets: the 15 Shadow requests for this chapter's rules, all Pending

> **Note**
> When the maker opens their own ticket, the only action offered is **Withdraw**. No approve or decline buttons appear in the maker's view. Ask a colleague with the checker role to review the ticket; see View a ticket.

Tuning and false positives

The settings each rule lets you change, and the ordinary activity that most often sets it off. The settings come from the rules above; the causes of false positives are general AML experience, not results from Fyscal ARCX. After each change, run a Dry Run and compare the alert count with the previous one.

Rule	Settings to tune	Common legitimate causes of alerts
1 · Structuring	Band edges (filter values), count, window	Instalments, rent or payroll of a fixed size that happens to sit inside the band
2 · Velocity	Count, window and its unit (Hours for shorter bursts)	Merchants, payroll and bill-payment accounts that transact many times a day
3 · High value	Amount, window	Corporate and treasury accounts, property or vehicle purchases, loan drawdowns
4 · Dormant account	Length of the quiet period, reactivation amount	Seasonal workers, customers who return from abroad, maturing deposits or annual payments
5 · Fan-out	Distinct-receiver count, window, optional amount filter	Payroll, supplier runs, remittance businesses, family support to many relatives
6 · Fan-in	Distinct-sender count, window, optional amount filter	Merchants, collection accounts, charities, landlords with many tenants
7 · Large single transaction	Amount	Known large clients, property settlements, business-to-business payments
8 · Smurfing	Small-amount limit, count, window	Micro-payment, transport, gaming top-up or e-wallet usage patterns

Rule	Settings to tune	Common legitimate causes of alerts
9 · Spike against own history	Minimum amount, multiplier	New customers with little history, salary bonuses, seasonal or one-off purchases
10 · Many devices	Distinct-device count, window	New or replaced phones, households sharing an account, business staff
11 · Many IP addresses	Distinct-IP count, window	Mobile networks that change IP addresses often, travel, public Wi-Fi
12 · Many instruments	Distinct-instrument count, optional instrument-type filter	Customers with several cards or accounts at one institution, card replacements
13 · Many currencies	Distinct-currency count, window	Foreign-exchange, remittance, travel and import-export customers
14 · Many destination countries	Distinct-country count, window	Remittance and trade customers with several regular corridors
15 · Cross-border volume	Amount, window, the country filter	Overseas workers' family support, tuition abroad, regular trade payments

AML context
Record why each threshold was chosen, test every change before it goes live, and review alert outcomes regularly. A rule that produces many alerts that are all closed as not suspicious usually needs a narrower variable (a filter) or a higher threshold, rather than more analysts.

Proposed typologies

Important
The rules in this section are proposals. None of them has been built, dry-run or submitted for activation, so none is part of the verified library above. Each uses only fields, functions and operators that the forms offer (see Building blocks), but whether a rule behaves as described is not yet known. Build one as a Draft, dry-run it with a positive control and start it in Shadow Mode before you rely on it.

Each proposal lists its variables and conditions, and the point to check first. Thresholds are placeholders for your own risk assessment.

P1 · Payments to high-risk countries · *Proposed — not yet tested*

Red flag	**A sender pays receivers in countries your policy treats as high risk.**
Variable	**Count** of `id`, grouped by `sender_entity_id`, 30 to 0 Days, filter `receiver_provider_country` **In** your list of countries
Condition	Variable **Greater Than Equal (>=)** 1
Check first	The format of `receiver_provider_country` values (for example two-letter codes or names) is not visible in the product, and the test data had no payments to the countries tried.

P2 · Pass-through account · *Proposed — not yet tested*

Red flag	**Money received is sent on almost in full within a short time (layering).**
Variables	A: **Sum** of `amount`, grouped by `receiver_entity_id`, 7 to 0 Days (received). B: **Sum** of `amount`, grouped by `sender_entity_id`, 7 to 0 Days (sent). For a faster pattern, use **Hours** as the unit.
Conditions	Match AND: A **Greater Than Equal (>=)** a minimum you choose, and B **Greater Than Equal (>=)** Variable A with **THAN MULTIPLIER** 0.9
Check first	Whether a typology that compares a variable grouped by `receiver_entity_id` with one grouped by `sender_entity_id` matches the same customer.

P3 · Repeated identical amounts · *Proposed — not yet tested*

Red flag	**Many payments of exactly the same amount, which can indicate structured or scripted transfers.**
Variables	A: **Count** of `id`, grouped by `sender_entity_id`, 7 to 0 Days. B: **Count Distinct** of `amount`, same grouping and window.

Red flag	**Many payments of exactly the same amount, which can indicate structured or scripted transfers.**
Conditions	Match AND: A **Greater Than Equal (>=)** 5, and B **Less Than Equal** 1
Check first	That **Count Distinct** on `amount` counts different amounts as expected. The typology type list includes “identical transactions”.

P4 · Jump in average payment size · *Proposed — not yet tested*

Red flag	**A sender’s typical payment becomes much larger than their own usual size.**
Variables	A: **Average** of `amount`, grouped by `sender_entity_id`, 7 to 0 Days. B: **Average** of `amount`, same grouping, 90 to 0 Days.
Condition	A **Greater Than Equal (>=)** Variable B with **THAN MULTIPLIER** 3
Check first	That the multiplier accepts values above 1 (only 0.5 has been tested). Customers with a short history can alert easily.

P5 · One device used by many customers · *Proposed — not yet tested*

Red flag	**Several customers send from the same device, a common sign of accounts controlled by one person (money mules).**
Variable	**Count Distinct** of `sender_entity_id`, grouped by `sender_device_id`, 7 to 0 Days
Condition	Variable **Greater Than Equal (>=)** 3
Check first	Which customer the alert is raised against when the variable is grouped by device rather than by customer.

P6 · One IP address used by many customers · *Proposed — not yet tested*

Red flag	**Several customers send from the same network location.**
Variable	**Count Distinct** of `sender_entity_id`, grouped by `sender_ip`, 7 to 0 Days
Condition	Variable **Greater Than Equal (>=)** a value set from a dry run
Check first	As P5. Shared networks (offices, mobile carriers) can put many legitimate customers behind one address.

P7 · Payments to merchant categories you treat as high risk · *Proposed — not yet tested*

Red flag	**Spending with merchant types your policy flags, such as gambling or money services.**
Variable	**Count** of `id`, grouped by `sender_entity_id`, 30 to 0 Days, filter `merchant_category_code` **In** your list of codes
Condition	Variable **Greater Than Equal (>=)** a value you choose
Check first	The format of `merchant_category_code` values in your data.

P8 · Activity above the customer’s declared profile · *Proposed — not yet tested*

Red flag	**A customer sends far more in a month than the expected monthly spend recorded at onboarding.**
Variables	A: an **Entity** variable on `expected_monthly_spend`. B: **Sum** of `amount`, grouped by `sender_entity_id`, 30 to 0 Days.
Condition	B **Greater Than Equal (>=)** Variable A with **THAN MULTIPLIER** 2
Check first	Whether an Entity variable can be compared with a Transaction variable in one typology, and on which customer key. The Entity field list includes `expected_monthly_spend` and `expected_txn_frequency`.

RELATED IN DETECTION & MONITORING

Name Screening | Transaction Monitoring | Data Ingestion

DETECTION & MONITORING

10 Data Ingestion

Fyscal ARCX → Data Ingestion

Data Ingestion shows how data reaches Fyscal ARCX, so administrators can check that each import ran and what it loaded. **Batch Ingestion** lists the scheduled import jobs for Customers, Accounts and Transactions files, lets you download source and error rows, and holds their schedule. **Watchlist Ingestion** lists the watchlist files loaded from LSEG and from the Internal Watchlist, and is where you upload your own Internal Watchlist file.

FOR	IN THE MENU	READING TIME
Administrators	Fyscal ARCX → Data Ingestion	About 14 min

Batch Ingestion: check each import job's records, skipped rows and status.

Filter batch jobs: find jobs by date, file type or status.

Investigate skipped rows: find jobs that did not load every row and download the rows that were skipped.

Change the ingestion schedule: set a new frequency and up to three run times a day.

Watchlist Ingestion: check which watchlist files were loaded and whether they succeeded.

Search, filter and sort watchlist files: find a file by name, status or source.

Upload an Internal Watchlist file: add subjects to, or remove them from, the Internal Watchlist with a CSV file.

The **Data Ingestion** menu under **Fyscal ARCX** has two items: **Batch Ingestion** and **Watchlist Ingestion**. Transaction data comes in through Batch Ingestion as the **Transactions** file type.

> **AML context**
> Screening and monitoring can only cover the data that was loaded. A skipped customer row is a customer who may not be screened, and a skipped transaction row is a transaction no rule sees. Checking ingestion results is part of the control, not housekeeping.

Batch Ingestion

Fyscal ARCX → Data Ingestion → Batch Ingestion

FILE TYPES	ONE JOB PER	DOWNLOADS	SCHEDULE
Customers, Accounts, Transactions	File type and run, with a Job ID	Source CSV (Total Records) and error rows CSV (Skipped Rows)	Up to 3 run times a day, set with Change Schedule

Check Batch Ingestion to confirm that customer, account and transaction files were imported, and to find the rows that were skipped. Batch Ingestion shows the ingestion schedule and a history of ingestion jobs. Each job imports one file type (Customers, Accounts or Transactions) and shows how many records it read, ingested and skipped.

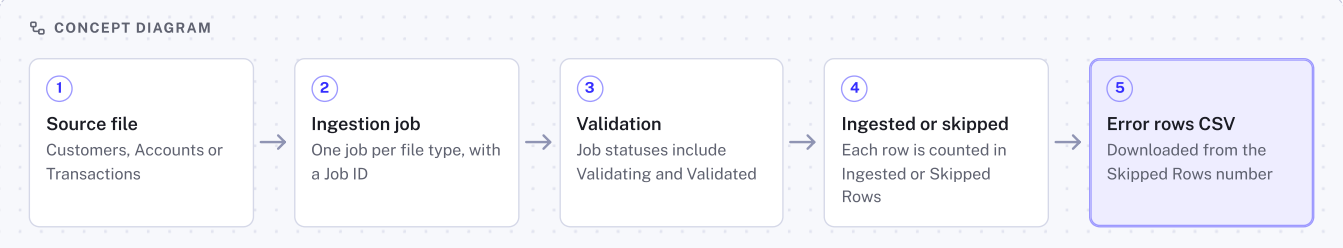


Diagram 10.1 — How a batch file is ingested

Diagram 10.1 follows one file through Batch Ingestion. A job reads the source file (**Total Records**), passes through validation, and loads the rows it can (**Ingested**). The rest are counted in **Skipped Rows**, and that number downloads them as an error rows CSV. The job's final status is shown in **Status**. See Investigate skipped rows.

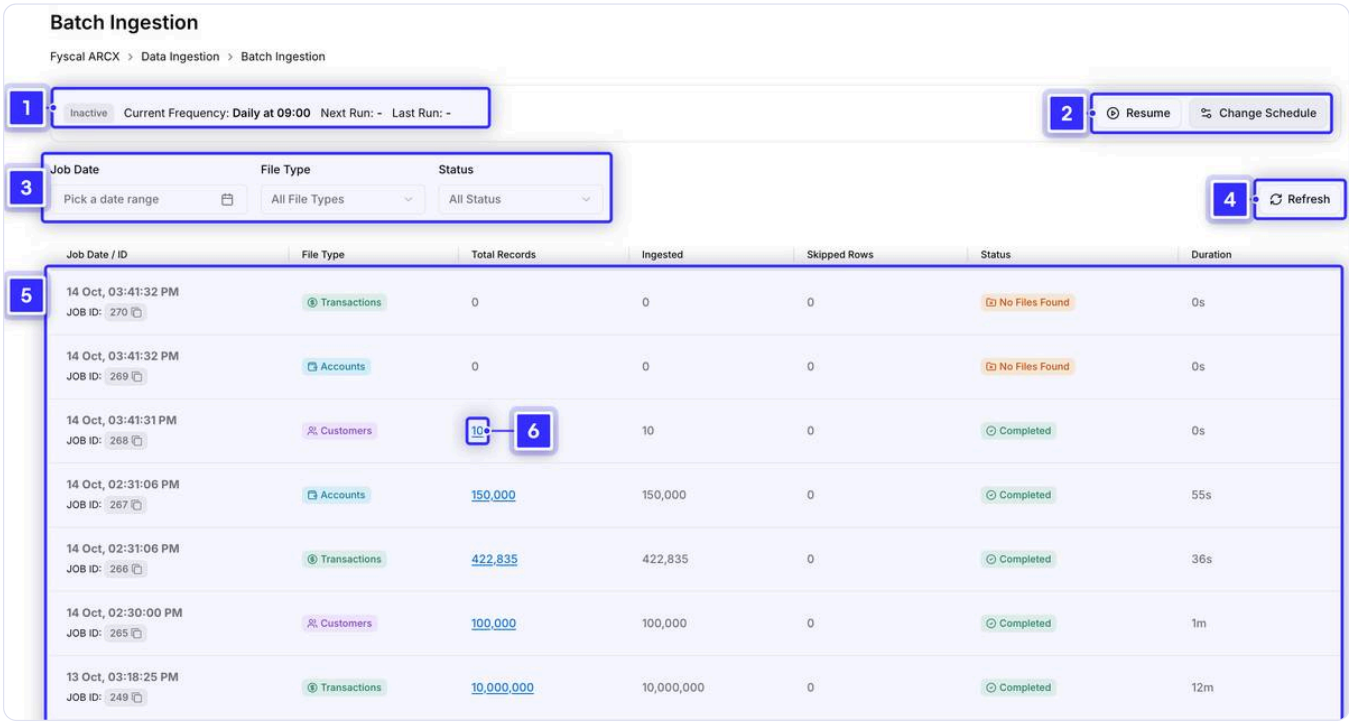


Figure 10.1 Batch Ingestion: the schedule bar (1), Resume and Change Schedule (2), the filters (3), Refresh (4), the job list (5) and a linked count (6).

1. **Schedule bar.** Shows the schedule state (**Inactive** in the example), **Current Frequency** (**Daily at 09:00**), **Next Run** and **Last Run**. When there is no value, the screen shows a dash (-).
2. **Resume** and **Change Schedule**. **Resume** is shown next to **Change Schedule** while the schedule is **Inactive**. **Change Schedule** opens the **Change Ingestion Schedule** dialog (see Change the ingestion schedule).
3. **Filters. Job Date** (**Pick a date range**), **File Type** (**All File Types**) and **Status** (**All Status**). See Filter batch jobs.
4. **Refresh** reloads the job list.
5. **Job list.** One row per job, newest first. Below the list, **Showing 1-20 of 113** gives the range and total, and **Page 1 of 6** has first, previous, next and last page buttons.
6. **Linked counts.** Underlined numbers in **Total Records** and **Skipped Rows** are download links (see the column table below).

Column	What it shows	Format or example
Job Date / ID	When the job ran, with the job number below it after **JOB ID:**. A copy icon sits next to the job number.	14 Oct, 03:41:31 PM JOB ID: 268
File Type	The data the job imported, as a coloured tag.	**Customers**, **Accounts**, **Transactions**
Total Records	Records in the source file. When the value is above 0 it is an underlined blue link that downloads the source CSV.	1,037
Ingested	Records loaded. Plain text.	1,000
Skipped Rows	Rows not loaded. When the value is above 0 it is an underlined red link that downloads the error rows CSV.	34
Status	The job's status tag (see the status table below).	Completed
Duration	How long the job ran. A dash (-) is shown for the job in **Validating** status.	4s, 8m, 2m, -



Figure 10.2 Two job rows. In job 237 the Total Records value 100,037 (1) and the Skipped Rows value 34 (2) are links; job 238 found no files and has no links.

> **Note**
> Clicking a job row does not open a detail view. The only links in a row are the underlined **Total Records** and **Skipped Rows** numbers.

In most jobs, **Ingested** plus **Skipped Rows** equals **Total Records**: job 171 (Customers) shows 1,000 = 600 + 400, and job 173 (Accounts) shows 1,500 = 130 + 1,370. In some jobs the two counts add up to 3 less than Total Records. Job 237 (Transactions) shows 100,037 records, 100,000 ingested and 34 skipped (100,034). Earlier jobs 181, 136, 137 and 139 show the same gap of 3.

Job statuses

The **Status** filter lists ten job statuses, in this order. The screen does not describe them. Where a status appears in the example job list, the table says what that row shows.

Status	As seen in the job list
Init	Not seen in the example list.
Validating	Job 138 (Transactions): 0 records and a Duration of -.
Validated	Not seen in the example list.
Published	Not seen in the example list.
Ingesting	Not seen in the example list.
Completed	Most jobs. Can still have skipped rows, for example job 173 (Accounts): 1,500 records, 130 ingested, 1,370 skipped.
Partial Success	Not seen in the example list.
Failed	Jobs 166 and 167 (Customers): 0 records, 0s.
No Valid Record	Not seen in the example list.
No Files Found	Jobs 269 (Accounts), 270 (Transactions) and 238 (Customers): 0 records, 0s.

> **Important**
> A **Completed** job can still have skipped rows. Job 173 is Completed with 1,370 of its 1,500 rows skipped. Check **Skipped Rows**, not only the status.

Filter batch jobs

Fyscal ARCX → Data Ingestion → Batch Ingestion

Use the three filters above the job list to narrow it by date, file type and status.

Step 1 **Filter by Job Date**

Click **Pick a date range** (1) under **Job Date**. A two-month calendar opens, with arrows (2) to move back and forward a month. Click the first day, then the last day of the range.

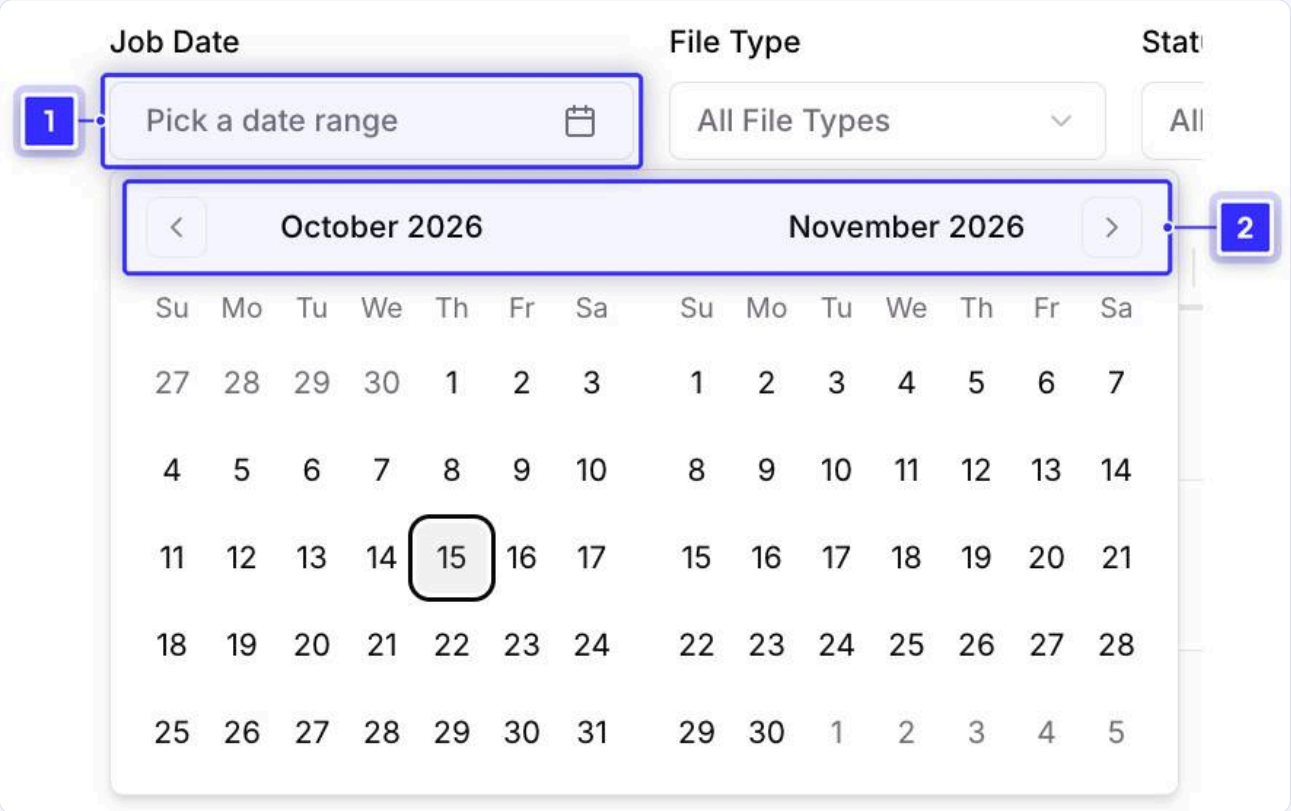


Figure 10.3 The Job Date field (1) and its calendar, showing October and November 2026 with the month arrows (2).

Step 2 **Filter by File Type**

Click **All File Types** (1) under **File Type**. The list has a search box (2) and three options (3): **Customers**, **Accounts** and **Transactions**. Click one.

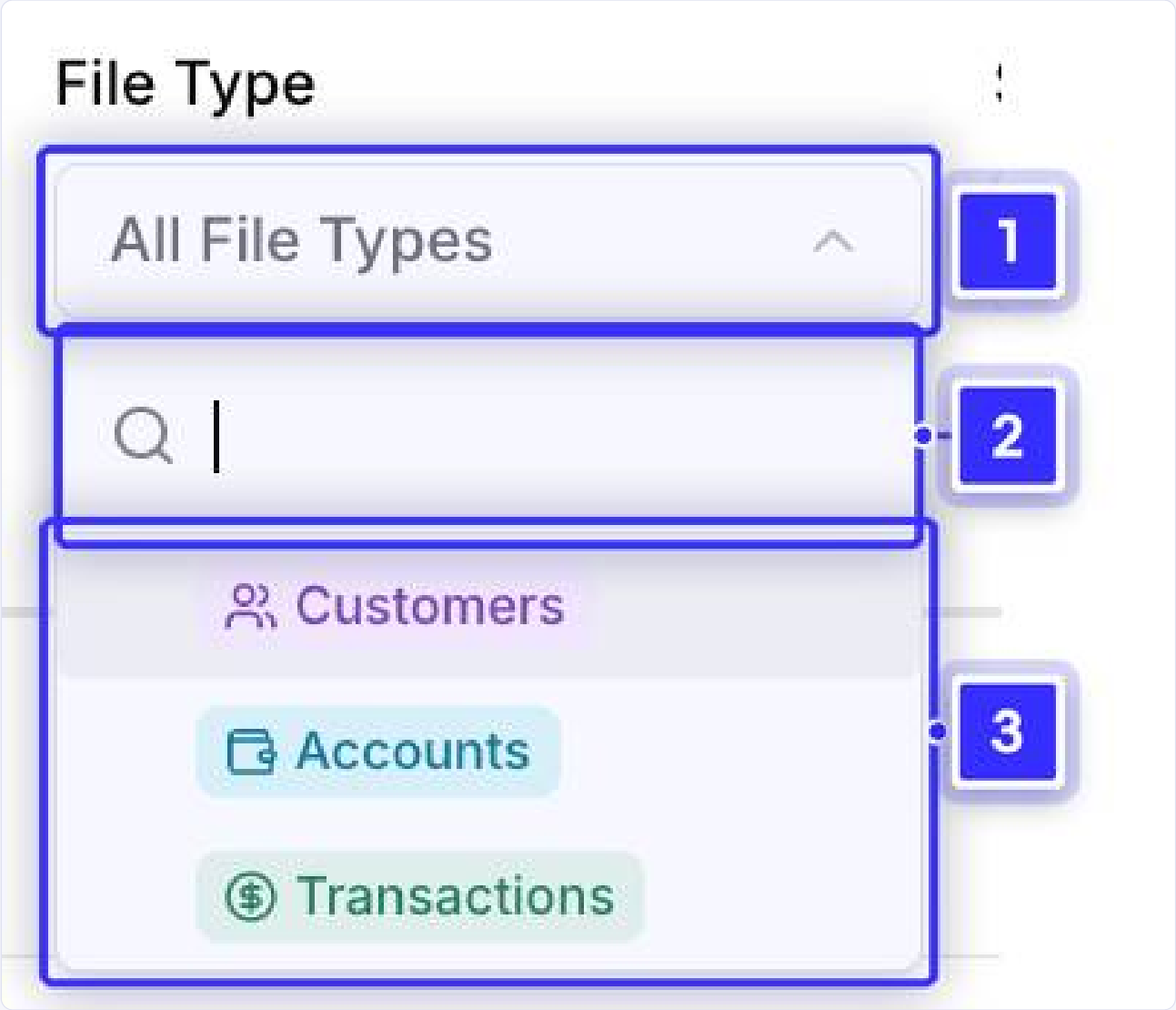


Figure 10.4 The File Type filter (1), its search box (2) and the options Customers, Accounts and Transactions (3).

Step 3 **Filter by Status**

Click **All Status** (1) under **Status**. The list has a search box and the ten statuses (2): **Init**, **Validating**, **Validated**, **Published**, **Ingesting**, **Completed**, **Partial Success**, **Failed**, **No Valid Record** and **No Files Found**. Scroll the list to see **No Files Found**. Click a status.


Status
All Status
1
Init
Validating
Validated
Published
Ingesting
2
Completed
Partial Success
Failed
No Valid Record



Figure 10.5 The Status filter (1): the statuses from Init to No Valid Record (2). No Files Found is further down the list.

Step 4 **Reload the list**

Click **Refresh** to reload the job list.

Investigate skipped rows

Fyscal ARCX → Data Ingestion → Batch Ingestion

LOOK FOR	DOWNLOAD	COMPARE WITH
A red, underlined **Skipped Rows** number	The job's error rows CSV	The source CSV, from **Total Records**

Use these steps when a job did not load every row. Skipped rows are records that were not loaded, so the customers, accounts or transactions in them are missing from the platform until they are loaded.

Step 1 **Find jobs with skipped rows**

On **Batch Ingestion**, narrow the list with **Job Date** and **File Type** if you need to (see Filter batch jobs). Look down the **Skipped Rows** column. A value above 0 is a red, underlined number, for example 34 on job 237 in Figure 10.2.

Step 2 **Download the error rows**

Click the **Skipped Rows** number. The job's error rows CSV downloads. The number does not say that it is a download, and clicking the row itself does nothing.

Step 3 **Download the source file if you need it**

Click the blue **Total Records** number to download the source CSV, so that you can compare the skipped rows with the file that was sent.

Step 4 **Have the data corrected**

Pass the error rows to the team that produces the file, so that the records can be corrected and sent again.

Tip

Missing data also shows up downstream. A Transaction Monitoring run with **Records Scanned** 0 had no transaction data to read; check Batch Ingestion for that period (see Schedule Details).

Change the ingestion schedule

Fyscal ARCX → Data Ingestion → Batch Ingestion → Change Schedule

Change the schedule when batch ingestion needs to run at a different frequency or at different times. **Change Schedule** opens the **Change Ingestion Schedule** dialog. Its subtitle reads: "Select the new frequency and run times, then review before confirming."

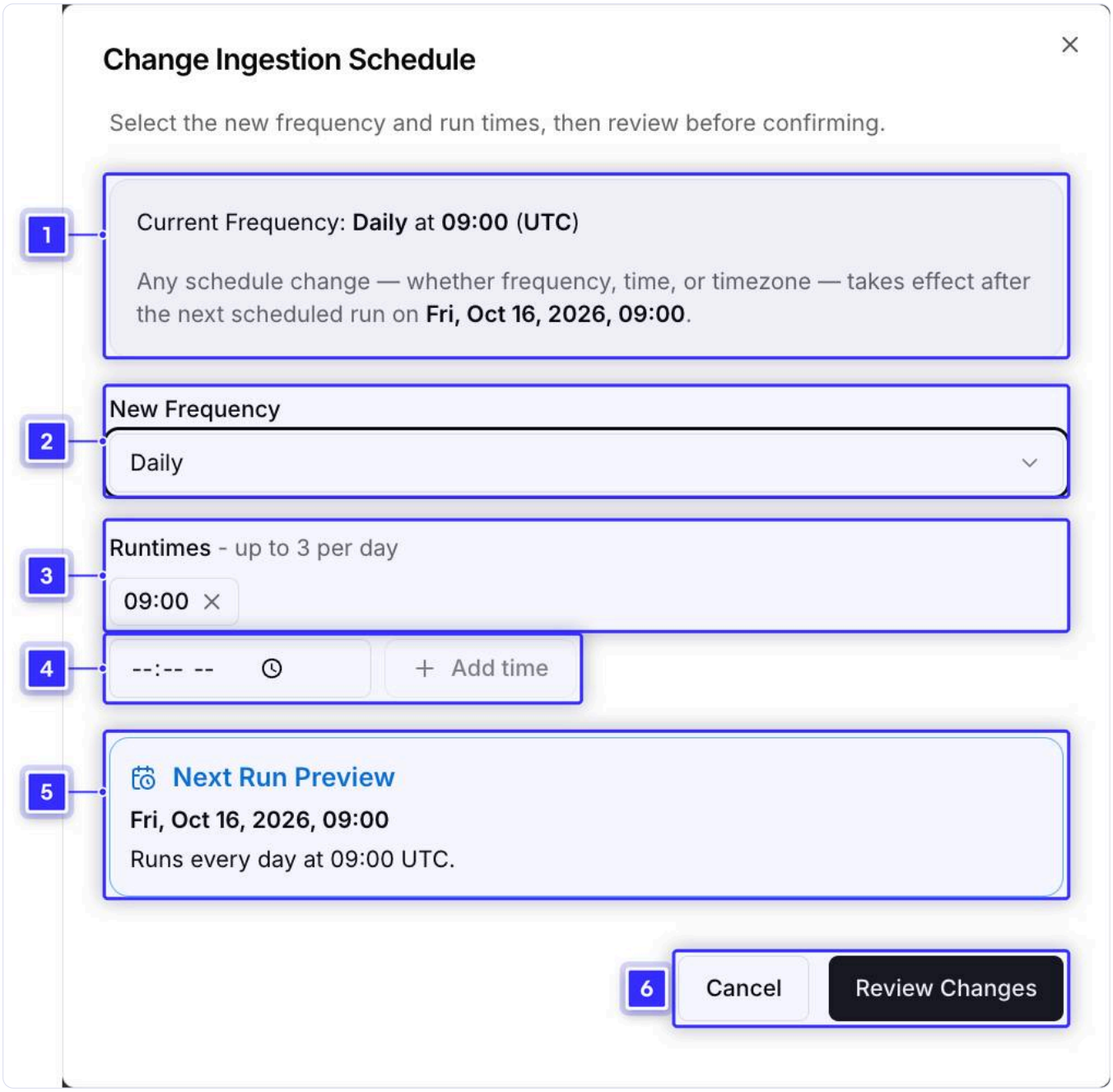


Figure 10.6 Change Ingestion Schedule: current frequency (1), New Frequency (2), Runtimes (3), the time field and Add time (4), Next Run Preview (5), and Cancel and Review Changes (6).

1. **Current Frequency**, with its time zone: **Daily at 09:00 (UTC)** in the example. Below it the dialog states: "Any schedule change — whether frequency, time, or timezone — takes effect after the next scheduled run on Fri, Oct 16, 2026, 09:00."
2. **New Frequency**: a drop-down, set to **Daily** in the example.
3. **Runtimes - up to 3 per day**: each run time is a chip (for example **09:00**) with an × to remove it.
4. A time field (**--:--**) and **+ Add time**, to add another run time.
5. **Next Run Preview**: the next run date and time (**Fri, Oct 16, 2026, 09:00**) and a summary, for example "Runs every day at 09:00 UTC."
6. **Cancel** closes the dialog. **Review Changes** moves on to review the change before confirming it.

Step 1 **Open the dialog**

On **Batch Ingestion**, click **Change Schedule**.

Step 2 **Choose the frequency**

Select a value in **New Frequency**.

Step 3 **Set the run times**

To add a run time, enter it in the time field and click **+ Add time**. To remove one, click the × on its chip. You can have up to 3 run times per day.

Step 4 **Check the preview and continue**

Check **Next Run Preview**, then click **Review Changes**. To leave without changing the schedule, click **Cancel** or the × at the top right.

Note

As the dialog states, a schedule change takes effect after the next scheduled run, not straight away.

Watchlist Ingestion

Fyscal ARCX → Data Ingestion → Watchlist Ingestion

Check Watchlist Ingestion to confirm that watchlist files were loaded and to see any errors. Watchlist Ingestion lists each watchlist file loaded into the platform, with its source, status, start and end times and the number of rows processed. LSEG files appear in pairs named *watchlist_delta__...* and *watchlist_deleted__...*. Files you upload yourself appear with the source **Internal Watchlist** and names beginning *internal_watchlist_delta__* or *internal_watchlist_deleted__*.

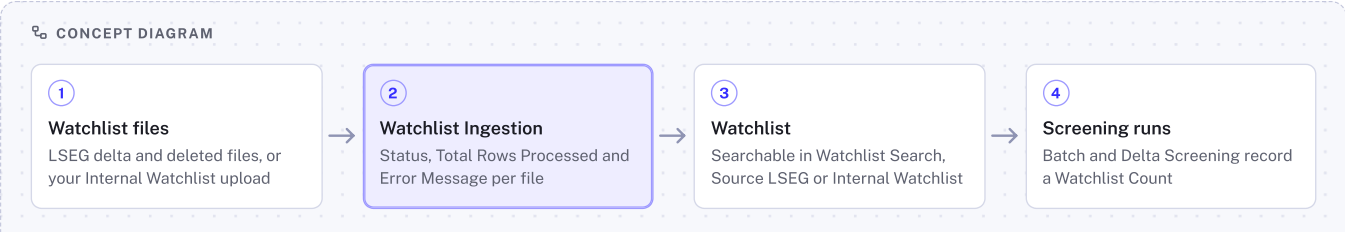


Diagram 10.2 — How watchlist data reaches screening

Diagram 10.2 shows the watchlist side. LSEG files and Internal Watchlist uploads are listed here, one row per file. Their records can be looked up in Watchlist Search, where the **Source** filter offers **LSEG** and **Internal Watchlist**, and each Batch Screening or Delta Screening run shows the **Watchlist Count** it recorded.

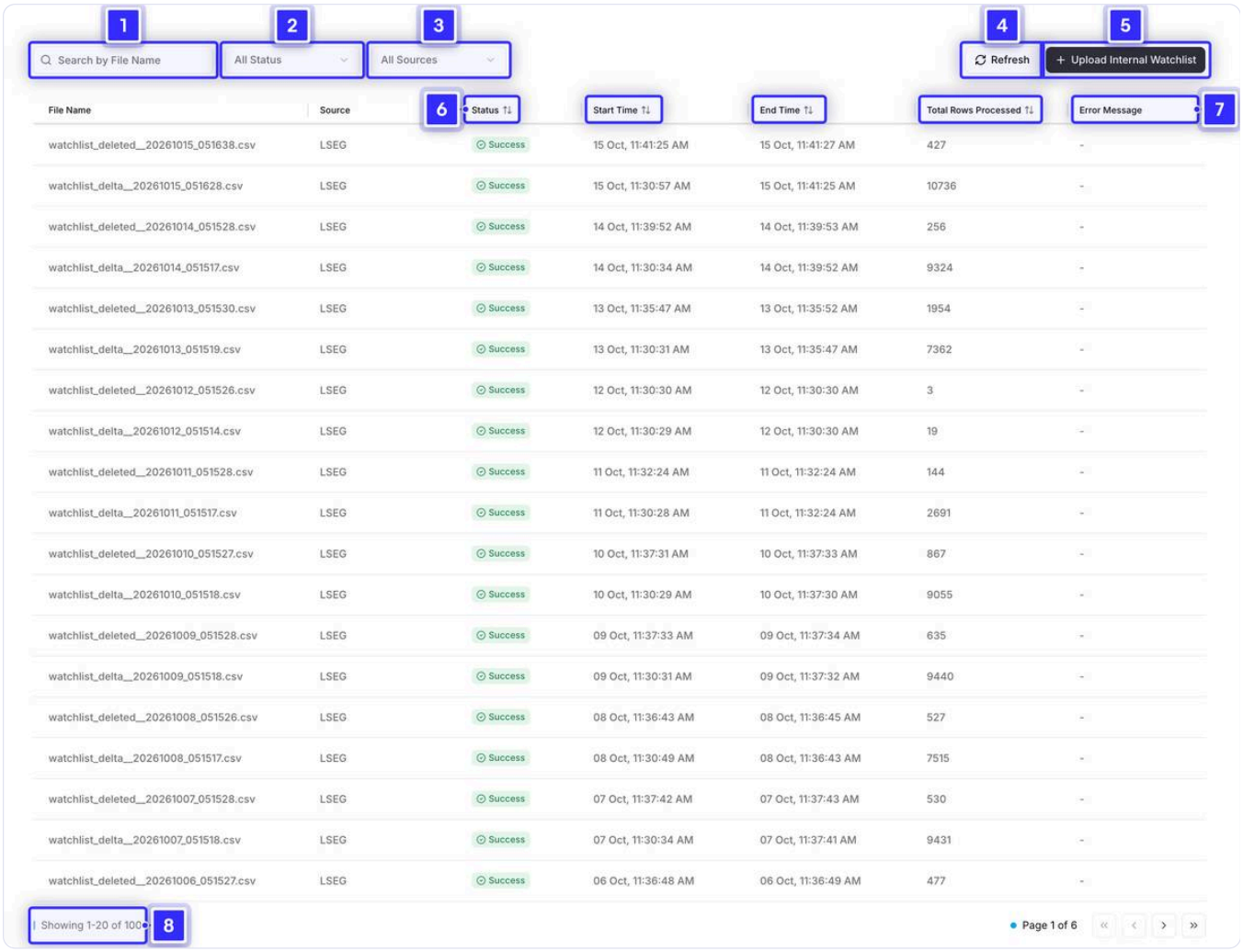


Figure 10.7 Watchlist Ingestion: search (1), Status (2) and Source (3) filters, Refresh (4), Upload Internal Watchlist (5), sortable columns (6), Error Message (7) and paging (8).

1. **Search by File Name**.
2. **Status** filter (**All Status**).
3. **Source** filter (**All Sources**).
4. **Refresh** reloads the list.
5. **+ Upload Internal Watchlist** opens the upload dialog (see Upload an Internal Watchlist file).
6. **Sortable columns. Status**, **Start Time**, **End Time** and **Total Rows Processed** have a sort icon (↑↓).
7. **Error Message** shows the error for a file, or a dash (-) when there is none.
8. Paging: **Showing 1-20 of 100** gives the range and total, and **Page 1 of 6** has first, previous, next and last page buttons.

Column	What it shows	Sortable	Example
File Name	Name of the ingested file. Long names are cut short with "...".	No	watchlist_delta__20261006_051519.csv
Source	Where the file came from.	No	LSEG, Internal Watchlist
Status	Status tag of the ingestion.	Yes	Success
Start Time	When ingestion of the file started.	Yes	06 Oct, 11:30:37 AM
End Time	When ingestion of the file ended.	Yes	06 Oct, 11:36:48 AM
Total Rows Processed	Rows processed from the file.	Yes	7487
Error Message	Error reported for the file; a dash (-) when there is none.	No	-

Status	As seen on screen
Success	Shown on every file in the example list.
In Progress	Listed in the Status filter; not seen in the example list.
Failed	Listed in the Status filter; not seen in the example list.

Search, filter and sort watchlist files

Fyscal ARCX → Data Ingestion → Watchlist Ingestion

Use these controls to find a particular watchlist file, or to list only the files of one status or source.

Step 1 **Search by file name**

Type part of a file name in **Search by File Name**.

Step 2 **Filter by status**

Click **All Status** (1) and choose **All Status**, **Success**, **In Progress** or **Failed** (2). A tick marks the current choice.

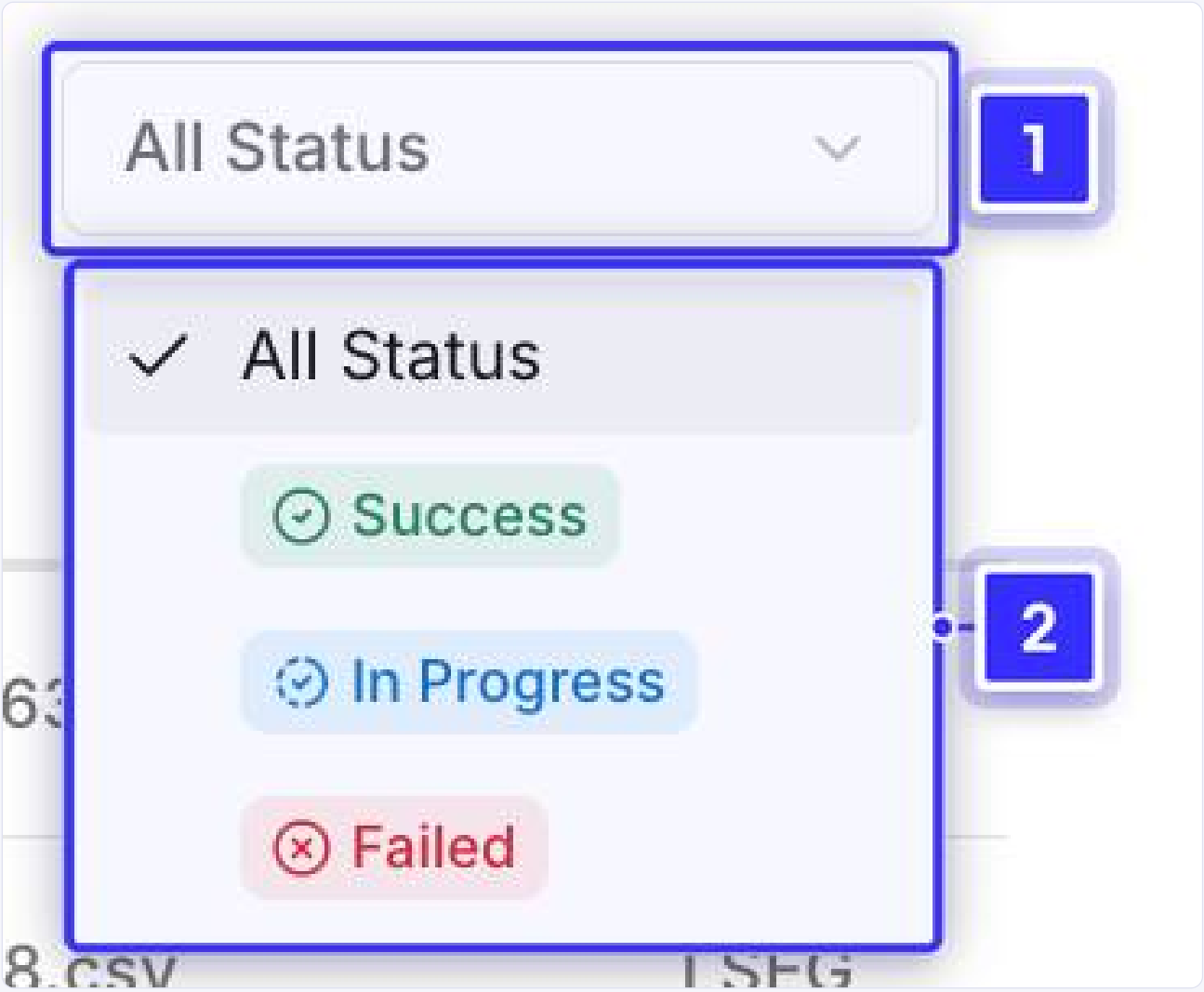


Figure 10.8 The Status filter (1): All Status, Success, In Progress and Failed (2).

Step 3 **Filter by source**

Click **All Sources** (1) and choose (2) **All Sources**, **Internal Watchlist** or **LSEG**.

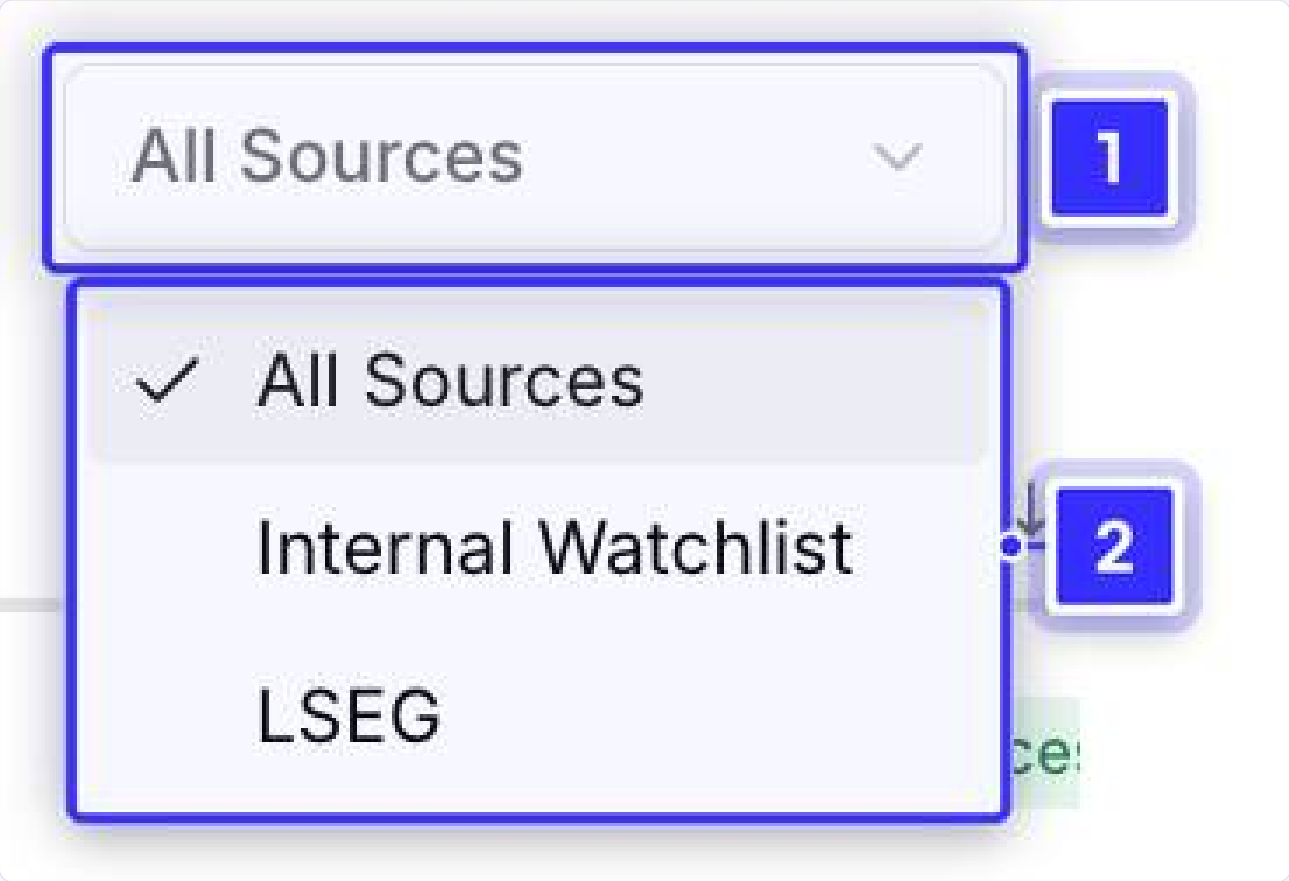


Figure 10.9 The Source filter (1): All Sources, Internal Watchlist and LSEG (2).

Step 4 **Sort the list**

Click a sortable column heading: **Status**, **Start Time**, **End Time** or **Total Rows Processed**. The ↑↓ icon on that column changes to an arrow showing the sort direction. In the example below, the list is sorted by **Total Rows Processed**, lowest first.

Start Time ↑↓	End Time ↑↓	Total Rows Processed ↑ 1	Error Message
18 Feb, 09:32:29 PM	18 Feb, 09:32:29 PM	0	-
18 Feb, 10:22:41 PM	18 Feb, 10:22:41 PM	0 2	-
23 Feb, 11:30:34 AM	23 Feb, 11:30:34 AM	0	-
18 Feb, 09:25:03 PM	18 Feb, 09:25:03 PM	0	-

Figure 10.10 The list sorted by Total Rows Processed: the ascending arrow on the column heading (1) and the lowest values first (2).

Upload an Internal Watchlist file

Fyscal ARCX → Data Ingestion → Watchlist Ingestion → Upload Internal Watchlist

Use this dialog when you need to add subjects to, or remove them from, your own Internal Watchlist. The **Upload Internal Watchlist** dialog does this using a CSV file. Its subtitle reads: "Add new subjects to the Internal Watchlist, or remove existing ones".

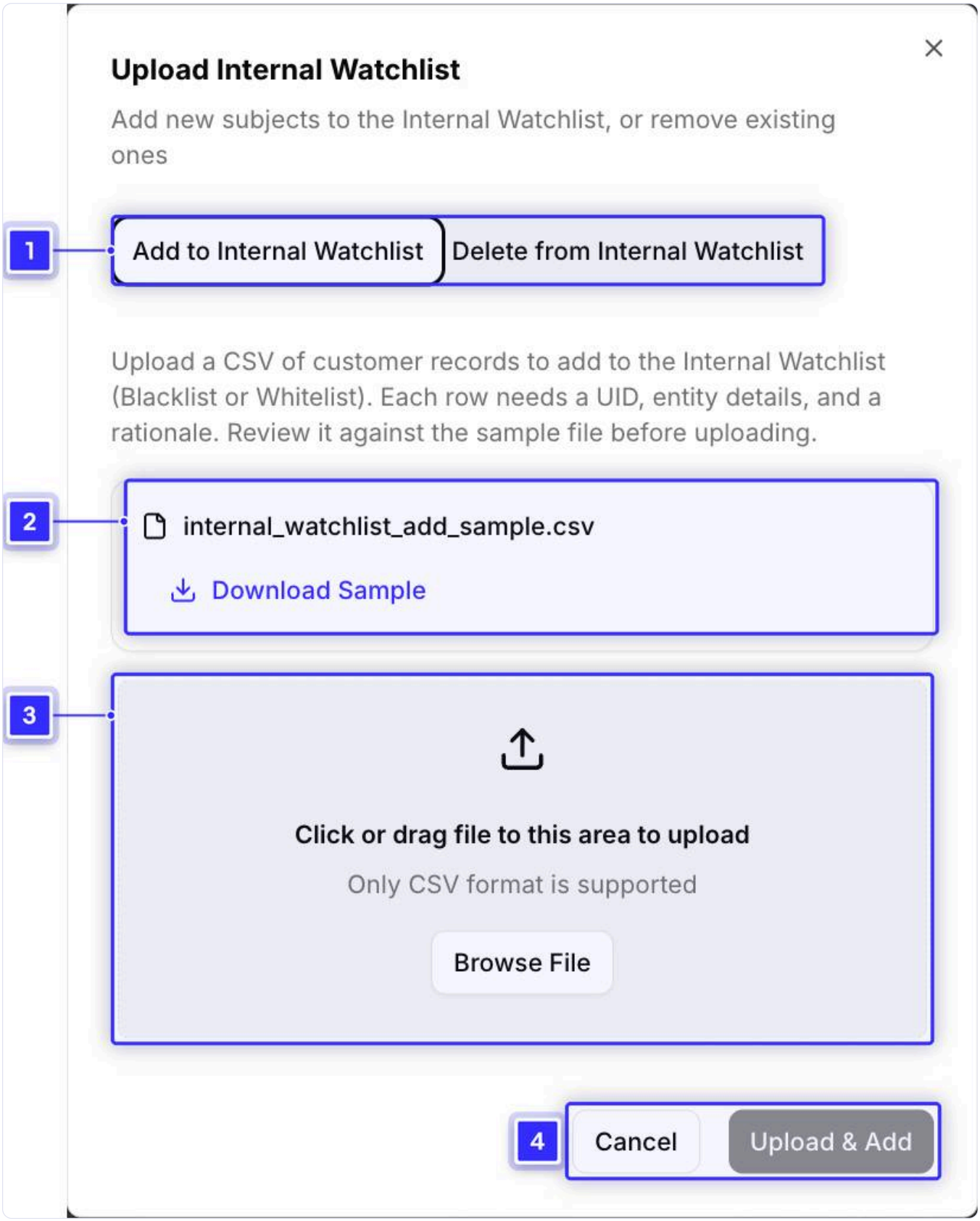


Figure 10.11 Upload Internal Watchlist: Add or Delete (1), the sample file (2), the upload area (3), and Cancel and Upload & Add (4).

1. **Add to Internal Watchlist** / **Delete from Internal Watchlist**: chooses whether the file adds or removes subjects. **Add to Internal Watchlist** is selected when the dialog opens.
2. The sample file **internal_watchlist_add_sample.csv** and **Download Sample**.
3. The upload area: "Click or drag file to this area to upload", "Only CSV format is supported", and **Browse File**.
4. **Cancel** and **Upload & Add**. **Upload & Add** is greyed out until a file is chosen.

Field or control	What it expects	Format
Add to Internal Watchlist / Delete from Internal Watchlist	Choose the action for the file.	Toggle; Add is selected by default.
Instructions (Add)	"Upload a CSV of customer records to add to the Internal Watchlist (Blacklist or Whitelist). Each row needs a UID, entity details, and a rationale. Review it against the sample file before uploading."	Text
Download Sample	Downloads the sample file **internal_watchlist_add_sample.csv**.	CSV
Upload area / Browse File	The file to upload. Drag it onto the area, click the area, or click **Browse File**.	"Only CSV format is supported"
Upload & Add	Uploads the chosen file.	Greyed out until a file is chosen.

Step 1 **Open the dialog**

On **Watchlist Ingestion**, click **+ Upload Internal Watchlist**.

Step 2 **Choose add or delete**

Leave **Add to Internal Watchlist** selected to add subjects, or click **Delete from Internal Watchlist** to remove them.

Step 3 **Check your file against the sample**

Click **Download Sample** and compare your CSV with it. For an add, each row needs a UID, entity details and a rationale.

Step 4 **Choose the file**

Drag the CSV onto the upload area, or click **Browse File** and select it. Only CSV files are accepted.

Step 5 **Upload**

Click **Upload & Add**. To leave without uploading, click **Cancel**.

RELATED IN DETECTION & MONITORING

Name Screening | Transaction Monitoring | Typology Library

ADMINISTRATION

11 Maker Checker Approval

Maker Checker Approval

Maker Checker Approval is where actions that need approval are set up and where the resulting requests are tracked. Administrators use **Configs** to define each activity that needs approval, with its SLA, warning point, approval count and the maker and checker permissions. **Tickets** lists the approval requests raised against those activities, so you can follow their status, review them and withdraw a request you raised.

FOR	IN THE MENU	READING TIME
Administrators	Maker Checker Approval	About 13 min

Configs: see which activities need approval and the rules set for each.

Search and filter activities: find an activity by UID, name, domain or status.

Activity actions: edit, view or deactivate an activity.

Create an activity: set up a new activity with its timing, approvals and permissions.

Tickets: follow the approval requests raised against activities.

Search and filter tickets: find a ticket by request ID, domain, activity, maker or status.

Ticket statuses: look up the eight ticket statuses.

View a ticket: review a request's details and remarks, or withdraw your own request.

Maker Checker Approval is its own item in the sidebar, below **Fyscal ARCX**. It expands into **Configs** and **Tickets**.

> **AML context**
> Maker checker is the four-eyes principle: one person proposes a change and a different person approves it. Auditors and supervisors expect this separation of duties for changes to detection rules and screening settings. An SLA and a warning point turn each approval into a timed control.

Configs

Maker Checker Approval → Configs

Use Configs to see which actions need approval and the approval rules for each. Configs lists every activity configuration. An activity names an action somewhere in the platform, for example **AML Name Screening Config** under *Fyscal ARCX/Name Screening/Configuration/Screening*, and sets the approval rules for it.

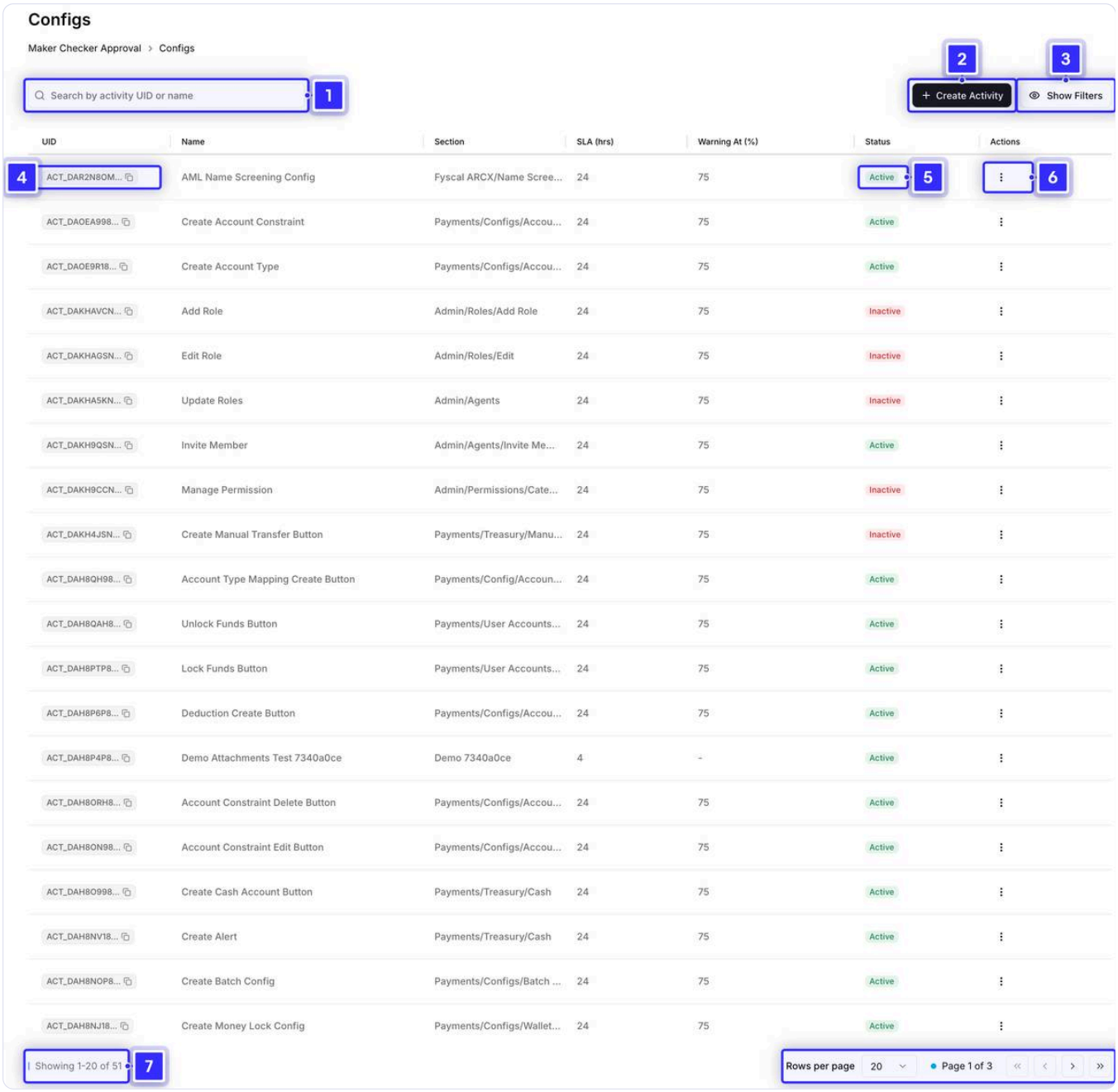


Figure 11.1 Configs: search (1), Create Activity (2), Show Filters (3), a UID (4), Status (5), the row menu (6) and paging (7).

1. **Search by activity UID or name**.
2. **+ Create Activity** opens the **Create Activity** form (see Create an activity).
3. **Show Filters** shows the **Domain** and **Status** filters; the button then reads **Hide Filters**.
4. **UID**: the activity's code, beginning **ACT_**, shortened with "..." and with a copy icon.
5. **Status**: **Active** (green) or **Inactive** (red).
6. **Actions** (⋮): opens the row menu (see Activity actions).
7. Paging: **Showing 1-20 of 51**, **Rows per page** (20), **Page 1 of 3**, and first, previous, next and last page buttons.

Column	What it shows	Example
UID	Activity code, shortened, with a copy icon.	ACT_DAR2N8OM...
Name	Activity name.	AML Name Screening Config, Add Role, Create Account Type
Section	Path of the part of the platform the activity belongs to. Long paths are cut short with "...".	Fyscal ARCX/Name Screening/Configuration/Screening; Admin/Roles/Add Role; Payments/Treasury/Cash
SLA (hrs)	SLA in hours.	24

Column	What it shows	Example
Warning At (%)	Warning point as a percentage; a dash (-) when not set.	75
Status	Whether the activity is active.	Active, Inactive
Actions	Row menu (⋮).	Edit, View, Deactivate

AML activities seen in the example

The example lists 51 activities. Those seen belong mostly to other parts of the platform (for example Admin and Payments). Two AML actions were seen:

Activity	Section or domain	Where it was seen
Activate Typology	Fyscal ARCX/Transaction Monitoring/Typology	Tickets raised when a typology is activated (see Tickets)
AML Name Screening Config	Fyscal ARCX/Name Screening/Configuration/Screening	The Configs list and the ticket **Activity Name** filter

Search and filter activities

Maker Checker Approval → Configs

Use search and the filters to find an activity by UID, name, domain or status.

Step 1 **Search**

Type an activity UID or name in **Search by activity UID or name**.

Step 2 **Show the filters**

Click **Show Filters**. The **Domain** (**Select Domain**) and **Status** (**Select Status**) filters appear above the list.

Step 3 **Filter by domain**

Click **Select Domain** (1) and choose a domain. In the example below, the list is empty and shows **No options found** (2).

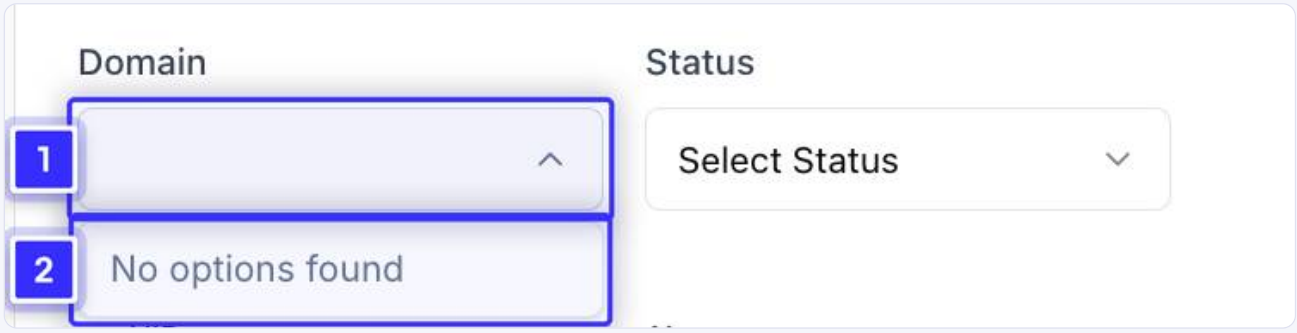


Figure 11.2 The Domain filter (1) open, showing No options found (2).

Step 4 **Filter by status**

Click **Select Status** (1) and choose **Active** or **Inactive** (2).

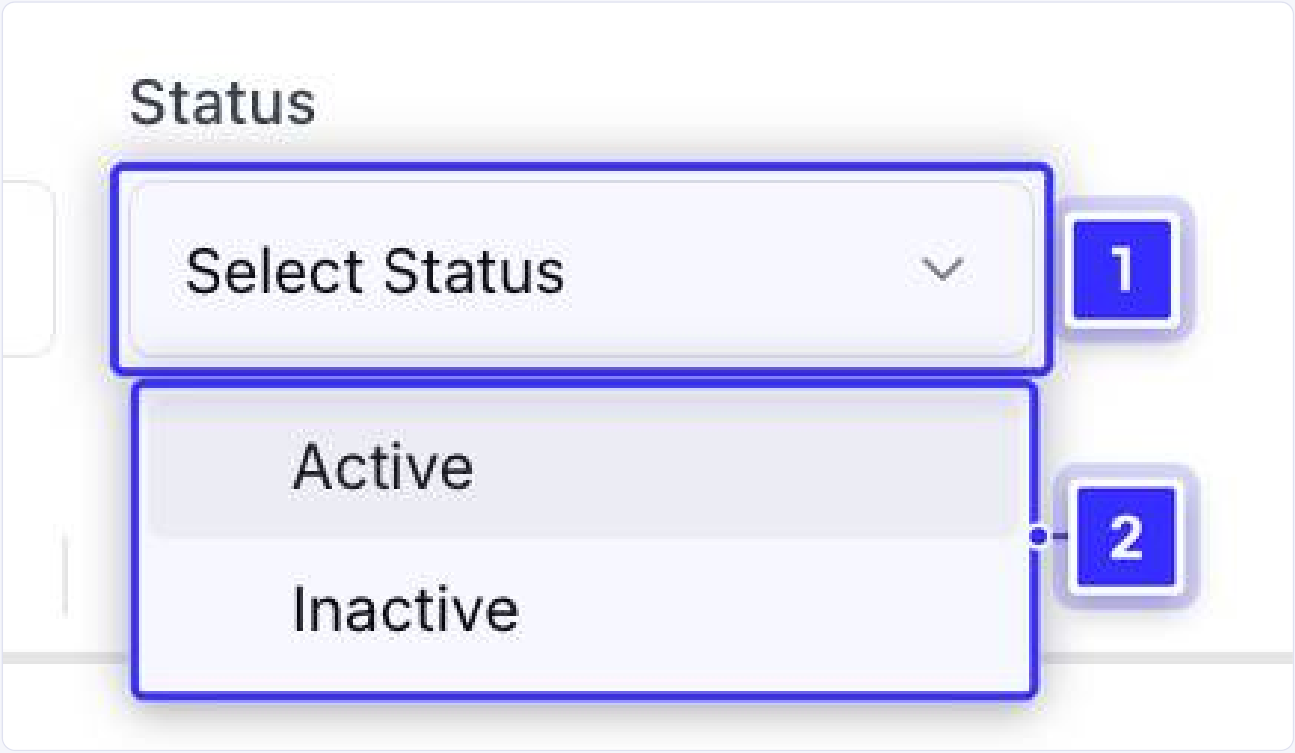


Figure 11.3 The Status filter (1): Active and Inactive (2).

Activity actions

Maker Checker Approval → Configs → ⋮

Use the row menu to change, inspect or deactivate an existing activity. Click ⋮ (1) in the **Actions** column of an activity. The **Actions** menu offers **Edit** (2), **View** (3) and **Deactivate** (4, in red).

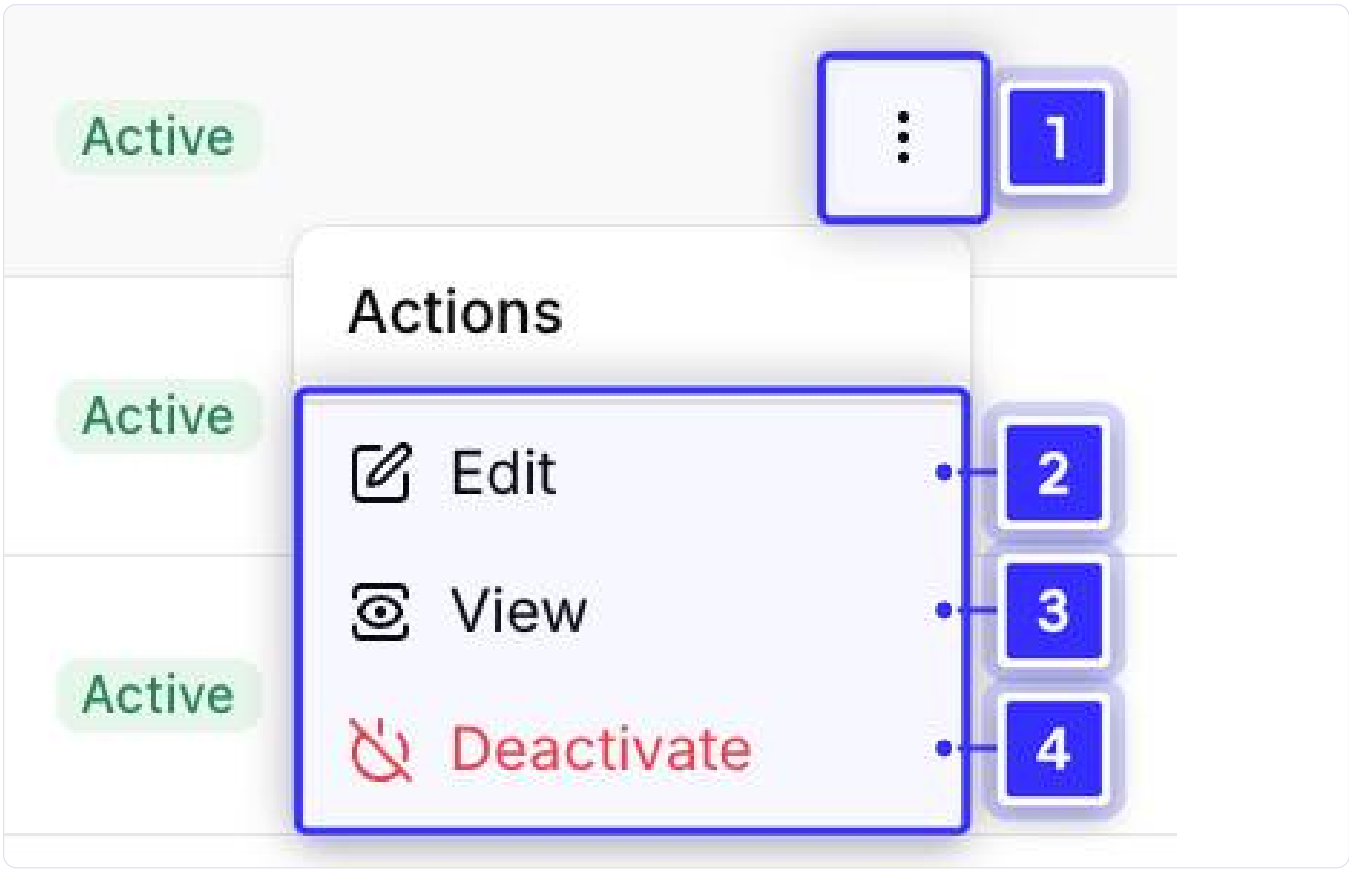


Figure 11.4 The Actions menu (1) of an active activity: Edit (2), View (3) and Deactivate (4).

Action	What the screen shows
Edit	Opens the **Edit Activity** form, subtitled "Configure the approval flow, context queries, and permission gates for this MCA activity." It has the same fields as **Create Activity** (see Create an activity), with **Close** and **Save**. The activity's values are loaded: for **AML Name Screening Config**, the **Domain** (Fyscal ARCX/Name Screening/Configura...), **SLA Duration (hrs)** 24, **Warning At (%)** 75 and **Approval Count** 1. In that example **Operation Point** shows its placeholder, **Select modal/screen**.
View	Opens a window headed with the activity name and its full UID (for example **AML Name Screening Config**, **ACT_dar2n8om2lbc73do21eg**), with **Close**.
Deactivate	Shown in red in the menu.



Figure 11.5 View for AML Name Screening Config: the activity name and UID (1), the error Unable to load MCA config: insufficient scopes in the provided token (2), and Close (3).

Note
View can show the error **Unable to load MCA config** with the message **insufficient scopes in the provided token**, as in Figure 11.5. In that case Edit shows the same message (**insufficient scopes in the provided token**) in the **Diff Fields** box.

Create an activity

Maker Checker Approval → Configs → + Create Activity

Create an activity when an action in the platform needs to go through approval. **+ Create Activity** opens the **Create Activity** form. The form scrolls: the top part sets the activity and its timing, and the lower part sets the context queries and permissions. Fields marked * are required.

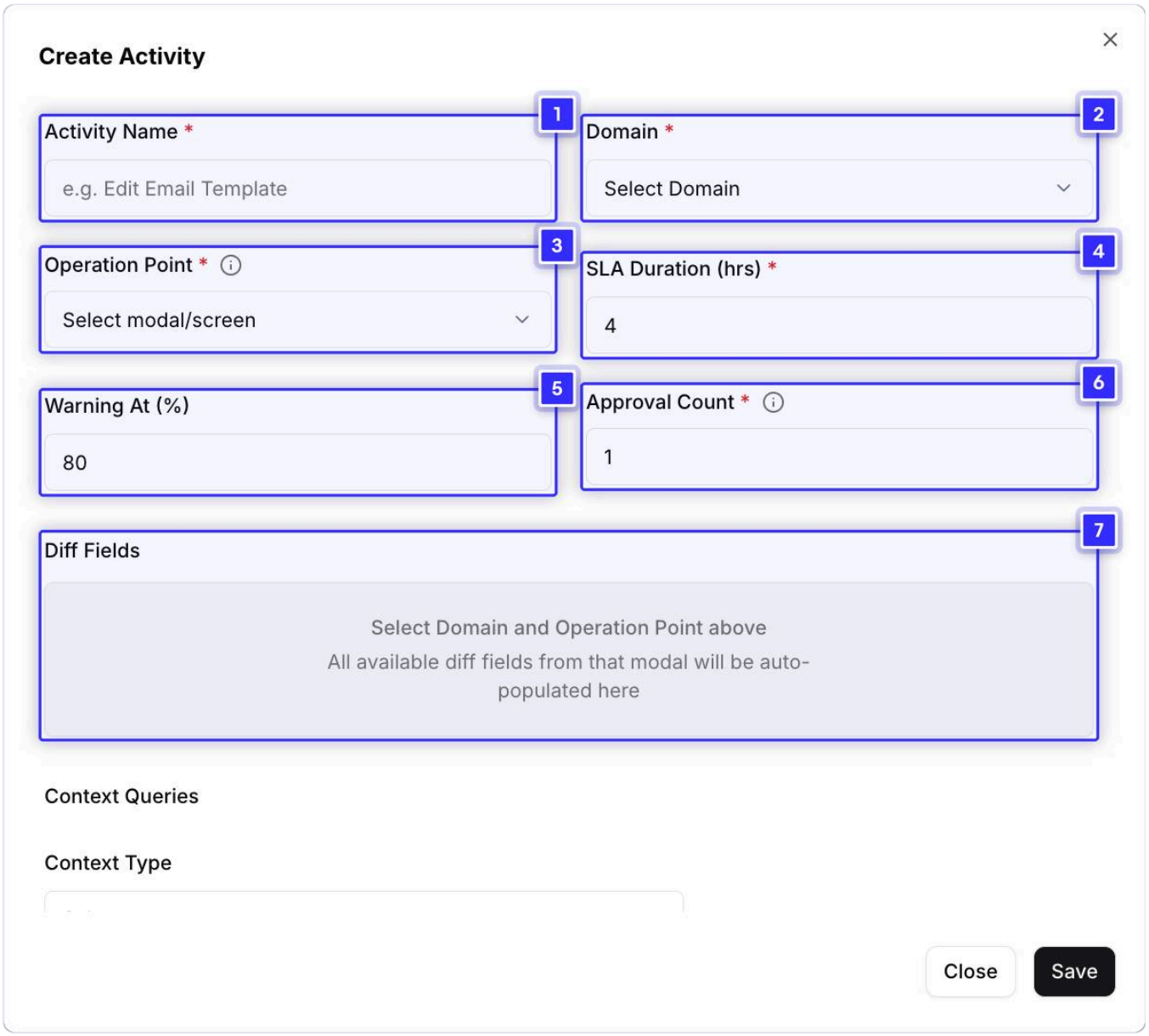


Figure 11.6 Create Activity, top part: Activity Name (1), Domain (2), Operation Point (3), SLA Duration (hrs) (4), Warning At (%) (5), Approval Count (6) and Diff Fields (7).

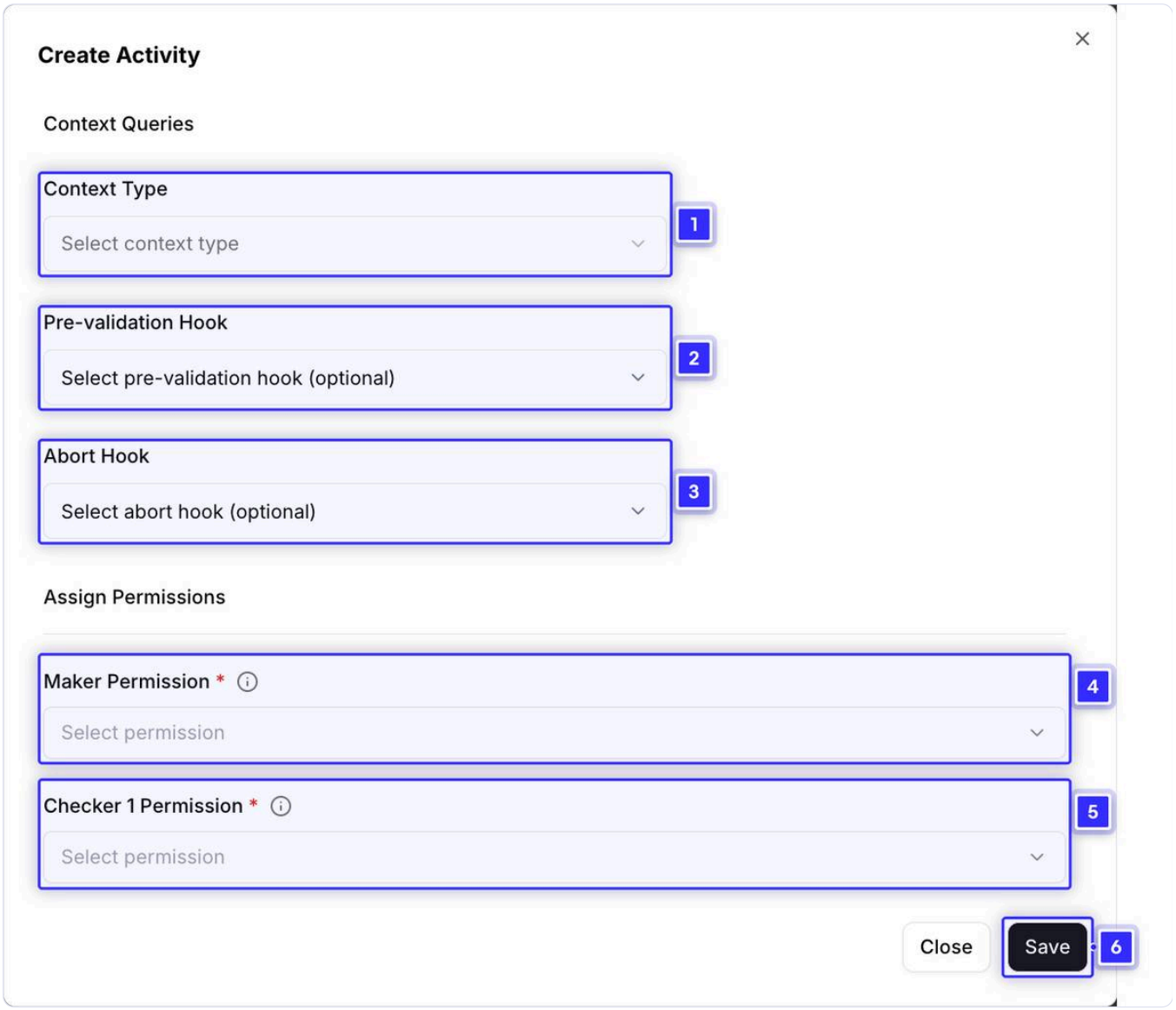


Figure 11.7 Create Activity, lower part: Context Type (1), Pre-validation Hook (2), Abort Hook (3), Maker Permission (4), Checker 1 Permission (5) and Save (6).

Field	What it expects	Required	Default, placeholder or options
Activity Name	Name of the activity.	Yes	Placeholder: e.g. Edit Email Template
Domain	The domain the activity belongs to.	Yes	Drop-down: Select Domain
Operation Point	The modal or screen the activity applies to. Has an info icon (ⓘ).	Yes	Drop-down: Select modal/screen
SLA Duration (hrs)	SLA in hours.	Yes	4
Warning At (%)	Warning point as a percentage.	No	80
Approval Count	Number of approvals. Has an info icon (ⓘ).	Yes	1
Diff Fields	Filled in by the form: "Select Domain and Operation Point above. All available diff fields from that modal will be auto-populated here".	No	Read-only until Domain and Operation Point are chosen
Context Queries			

Field	What it expects	Required	Default, placeholder or options
Context Type	The type of additional context for the request.	No	Drop-down: Select context type. Options: **Generic Additional Context**, **Tailored Additional Context**
Pre-validation Hook	A pre-validation hook.	No	Drop-down: Select pre-validation hook (optional)
Abort Hook	An abort hook.	No	Drop-down: Select abort hook (optional)
Assign Permissions			
Maker Permission	The permission for the maker. Has an info icon (ⓘ).	Yes	Drop-down: Select permission
Checker 1 Permission	The permission for the first checker. Has an info icon (ⓘ).	Yes	Drop-down: Select permission

Step 1 **Open the form**

On **Configs**, click **+ Create Activity**.

Step 2 **Name the activity and choose where it applies**

Enter the **Activity Name**, then select the **Domain** and the **Operation Point**. **Diff Fields** fills in from the chosen modal or screen.

Step 3 **Set the timing and approvals**

Change **SLA Duration (hrs)** (4), **Warning At (%)** (80) and **Approval Count** (1) if the defaults do not fit.

Step 4 **Set the context queries**

Scroll down. Under **Context Queries**, select a **Context Type** and, if you need them, a **Pre-validation Hook** and an **Abort Hook**.

Step 5 **Assign the permissions**

Under **Assign Permissions**, select the **Maker Permission** and the **Checker 1 Permission**. Both are required.

Step 6 **Save**

Click **Save**. To leave without saving, click **Close** or the × at the top right.

Tickets

Maker Checker Approval → Tickets

Use Tickets to follow approval requests and see where each one stands. A ticket is a request raised for an activity and waiting for approval. For example, activating a typology in Transaction Monitoring raises a ticket for the **Activate Typology** activity, with the domain *Fyscal ARCX/Transaction Monitoring/Typology*. Tickets lists these requests.

RAISED BY	DECIDED BY	PROGRESS	THE MAKER CAN
The maker's action, for example Activate Typology	A checker; the maker's view offers no approve or decline buttons	**Checker Progress**, for example 0 / 1 checkers acted	View, Watch, and Withdraw a Pending ticket

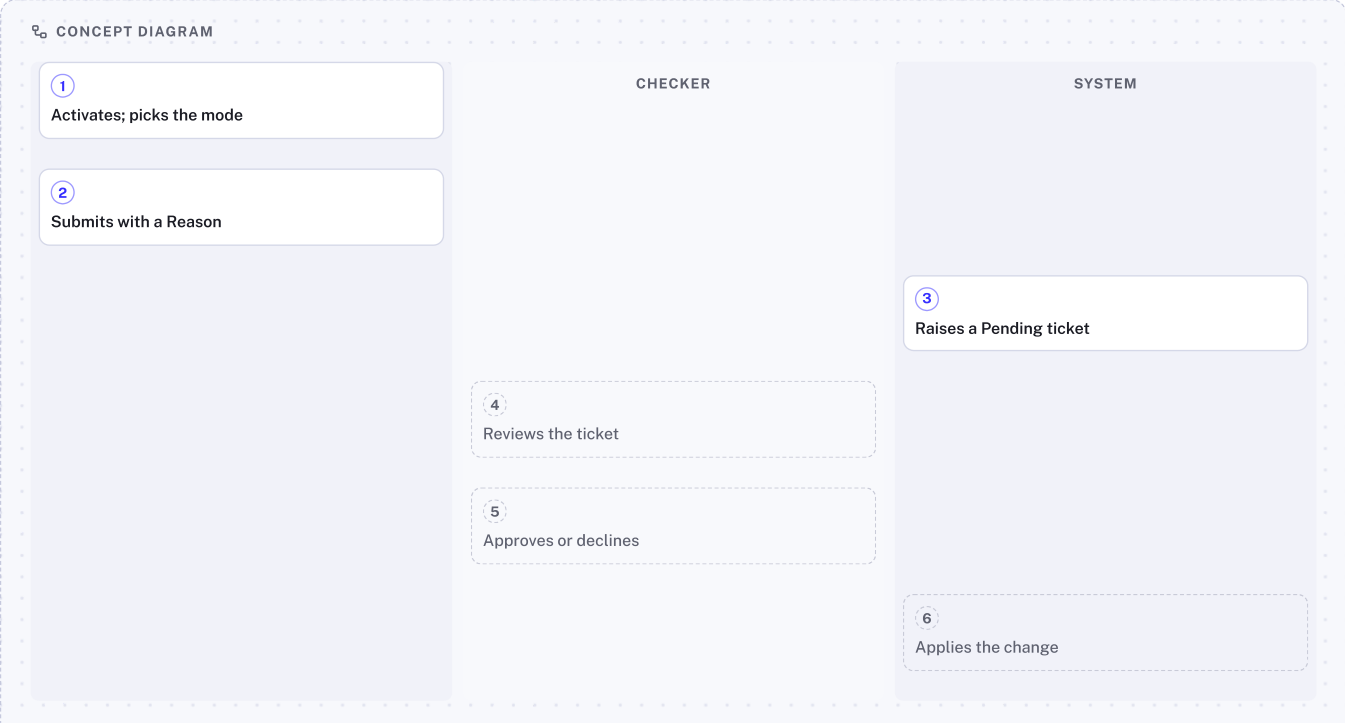


Diagram 11.1 — Maker, checker and system steps for an Activate Typology request

Dashed items are steps not shown in this guide's screenshots.

Diagram 11.1 follows one request. The maker's steps and the system's response were seen on screen: after **Submit Request** the confirmation reads "Submitted for governance review (ticket AMLTM_...). It will be applied once approved.", the typology stays **Draft**, and a **Pending** ticket appears here with **Checker Progress** "0 / 1 checkers acted". The maker's side is described step by step in Request Shadow activation. While the ticket is Pending, the maker can withdraw it (see View a ticket).

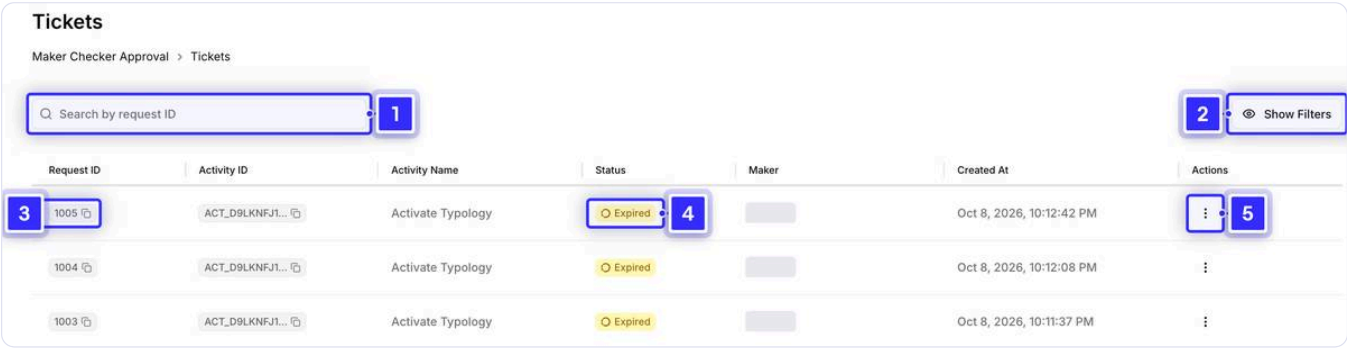


Figure 11.8 Tickets: search by request ID (1), Show Filters (2), the request ID (3), the status (4) and the row menu (5); maker names hidden.

1. **Search by request ID**.
2. **Show Filters** shows the **Domain**, **Activity Name**, **Maker** and **Status** filters.
3. **Request ID**, with a copy icon.
4. **Status** of the ticket (see Ticket statuses).
5. **Actions** (⋮): **View** and **Watch**.

Column	What it shows	Example
Request ID	Ticket number, with a copy icon. The ticket's details and the confirmation message show a longer ticket ID beginning **AMLTM_** instead (see View a ticket).	914
Activity ID	UID of the activity, shortened, with a copy icon.	ACT_D9LKNFJ1...
Activity Name	Name of the activity.	Activate Typology
Status	Ticket status tag.	Pending, Expired
Maker	The user who raised the request.	(user name)

Column	What it shows	Example
Created At	When the ticket was raised.	Oct 6, 2026, 10:57:55 AM
Actions	Row menu (⋮).	View, Watch

Below the list, **Page** shows the current page number with previous and next buttons.

Search and filter tickets

Maker Checker Approval → Tickets → Show Filters

Use the search box and filters to find a ticket by request ID, domain, activity, maker or status. Click **Show Filters**. Four filters appear above the list, and the button reads **Hide Filters**.

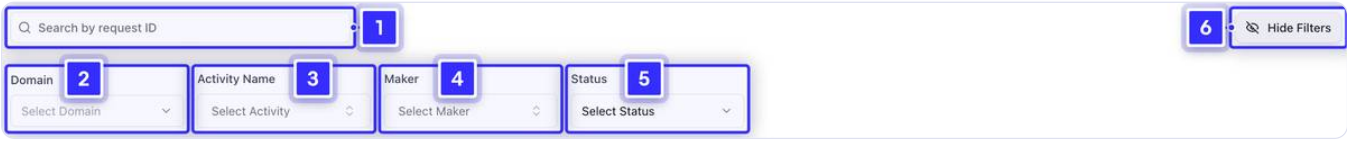


Figure 11.9 Ticket search (1) and the Domain (2), Activity Name (3), Maker (4) and Status (5) filters, with Hide Filters (6).

Filter	Placeholder	Options
Search	Search by request ID	Free text
Domain	Select Domain	On Configs, the Domain filter lists **No options found** (Figure 11.2).
Activity Name	Select Activity	The activity names from Configs, for example AML Name Screening Config, Create Account Constraint, Add Role, Edit Role, Unfreeze Account
Maker	Select Maker	-
Status	Select Status	Pending, In Progress, Execution Pending, Approved, Declined, Withdrawn, Expired, Execution Failed

Step 1 **Find a ticket by number**

Type the request ID in **Search by request ID**.

Step 2 **Filter by status**

Click **Select Status** and choose a status.

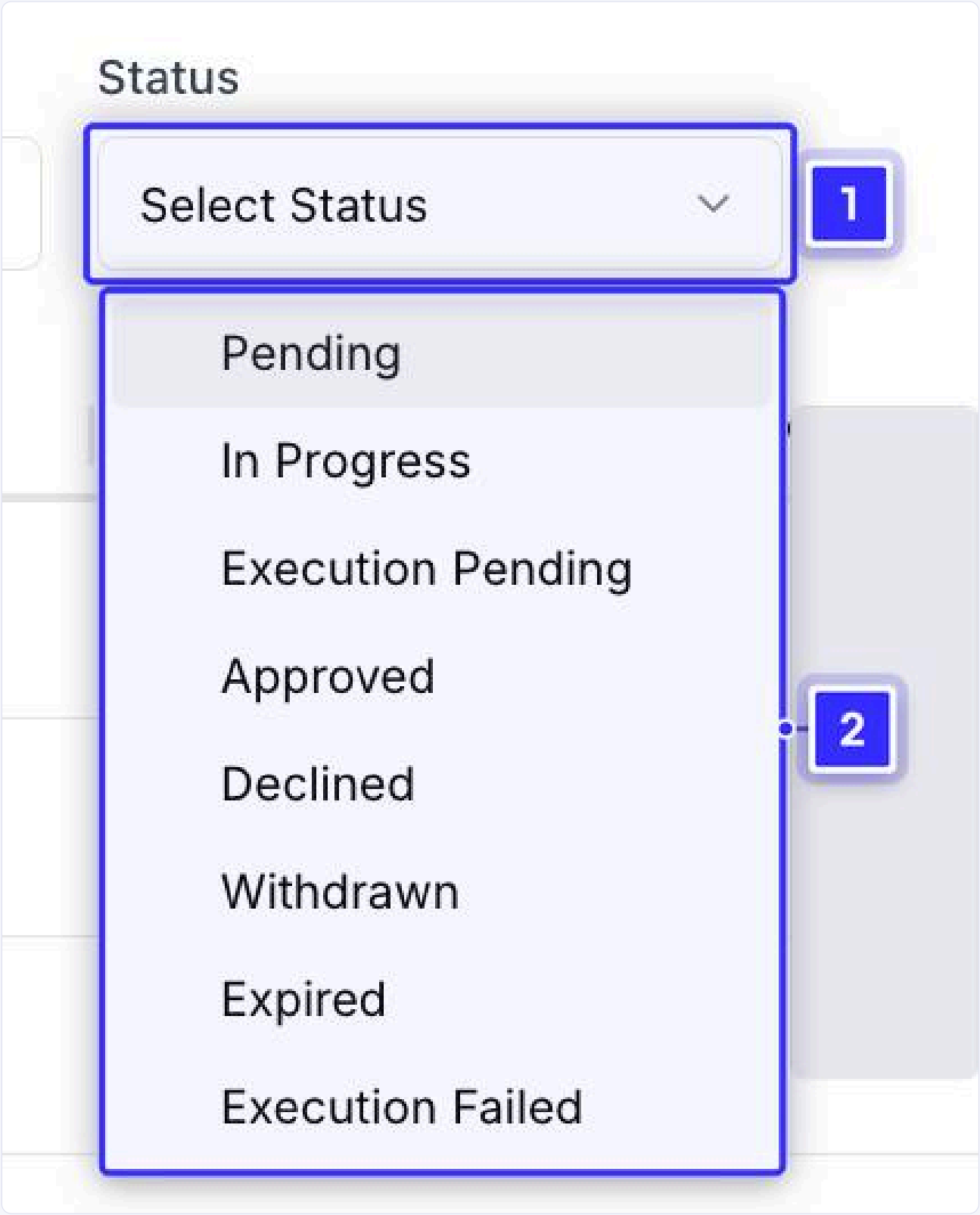


Figure 11.10 The ticket Status filter (1): Pending, In Progress, Execution Pending, Approved, Declined, Withdrawn, Expired and Execution Failed (2).

Step 3 **Filter by activity or maker**

Click **Select Activity** and choose an activity name, or click **Select Maker** and choose a maker.

Ticket statuses

Maker Checker Approval → Tickets

Use this table to look up a status shown on a ticket or in the **Status** filter. The **Status** filter lists eight ticket statuses. The screen does not describe them; the table notes what the example tickets show. Only **Pending** and **Expired** have been seen on tickets.

Status	As seen on screen
Pending	Tickets 991 to 1005 (Activate Typology, raised on 8 Oct 2026) while they waited, and ticket 914 when it was first seen on 6 Oct. The details show **Checker Progress** "0 / 1 checkers acted", and the maker can withdraw the ticket.
In Progress	Listed in the Status filter only.
Execution Pending	Listed in the Status filter only.
Approved	Listed in the Status filter only.
Declined	Listed in the Status filter only.
Withdrawn	Listed in the Status filter only.
Expired	Tickets 911 and 914, and tickets 991 to 1005 by 11 Oct (raised 8 Oct, no checker acted). Ticket 914 was Pending on 6 Oct, with "0 / 1 checkers acted", and Expired on 8 Oct. The tag is the same yellow as Pending.
Execution Failed	Listed in the Status filter only.

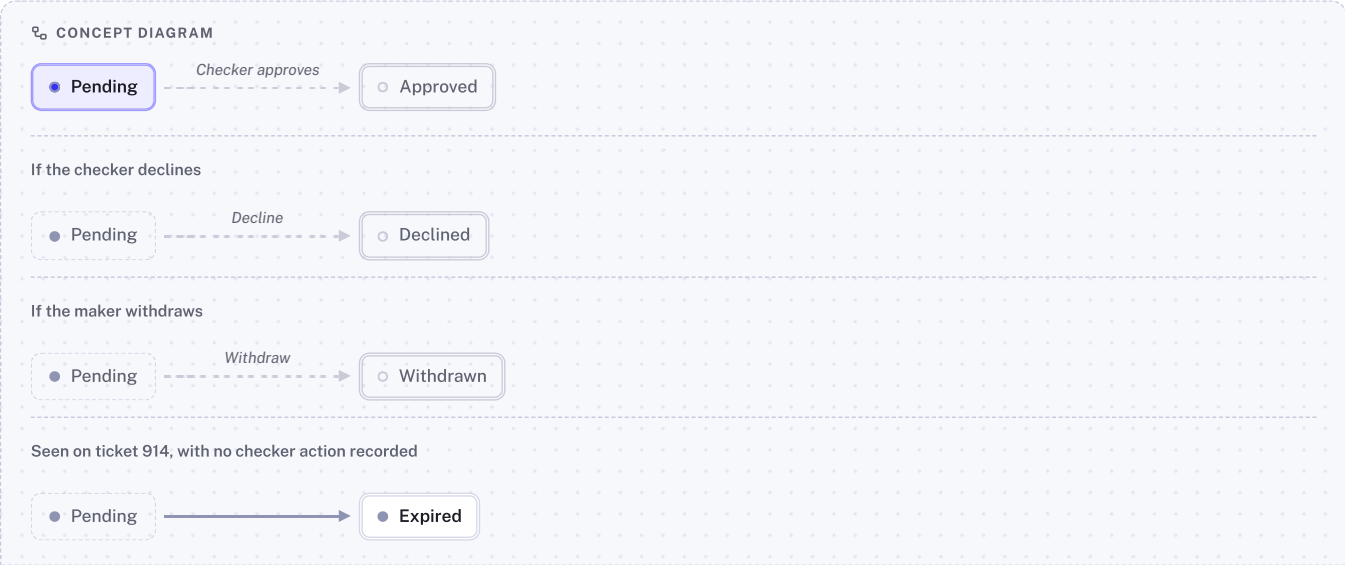


Diagram 11.2 — Ticket statuses and the paths out of Pending

Dashed items are steps not shown in this guide's screenshots.

Diagram 11.2 shows the paths a ticket can take out of **Pending**. Only Pending to **Expired** appears in this guide's screenshots (ticket 914, above). The other paths follow the actions on screen (**Withdraw** in the maker's view) and the status names in the filter (**Approved**, **Declined**, **Withdrawn**).

View a ticket

Maker Checker Approval → Tickets → ⋮ → View

Open a ticket to review what was requested, the proposed change and any checker remarks, or to withdraw a request you raised. Click ⋮ in the **Actions** column of a ticket. The **Actions** menu offers **View** and **Watch**. **View** opens **Request Details**.

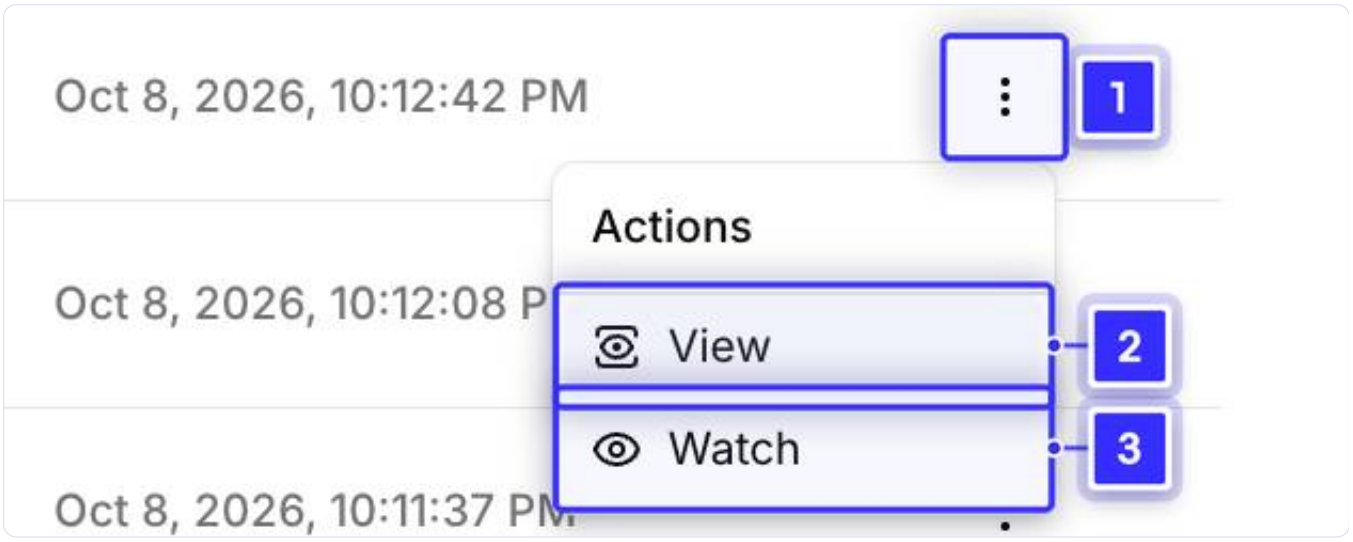


Figure 11.11 The ticket Actions menu (1): View (2) and Watch (3).

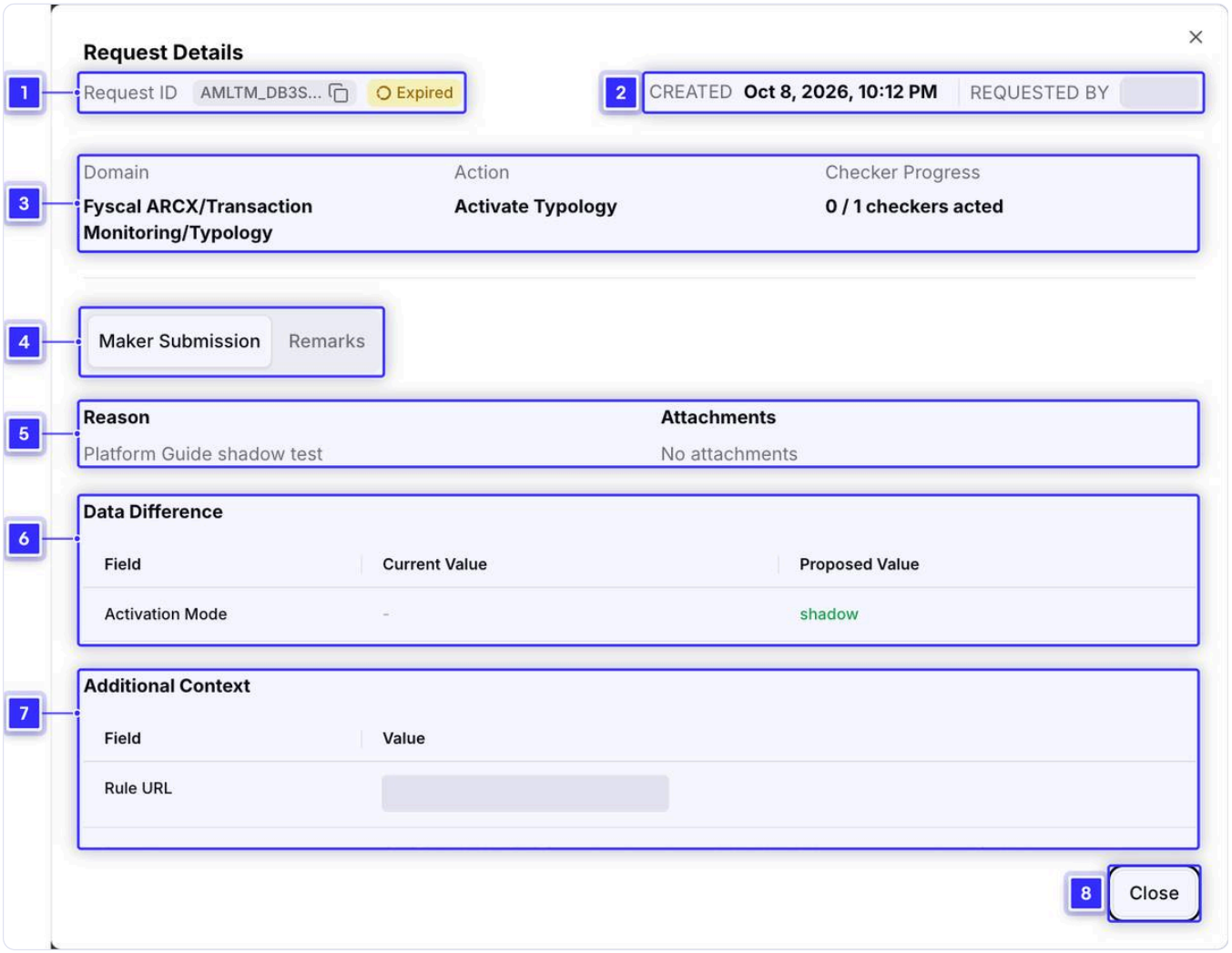


Figure 11.12 Request Details for an Expired Activate Typology ticket, Maker Submission tab: request ID and status (1), created and requested by (2), domain, action and checker progress (3), tabs (4), reason and attachments (5), Data Difference (6), Additional Context (7) and Close (8).

1. **Request ID**, beginning **AMLTM_** (shortened, with a copy icon), and the status tag. The Tickets list shows the same ticket by its number, here 1005.
2. **CREATED** date and time and **REQUESTED BY** with the maker's name (hidden here).
3. **Domain** (*Fyscal ARCX/Transaction Monitoring/Typology*), **Action** (**Activate Typology**) and **Checker Progress** ("0 / 1 checkers acted").
4. Tabs: **Maker Submission** and **Remarks**.
5. **Reason** given by the maker, and **Attachments** ("No attachments" when there are none).
6. **Data Difference**: a table of **Field**, **Current Value** and **Proposed Value**. In the example, **Activation Mode** changes from - to **shadow**.

7 **Additional Context**: a table of **Field** and **Value**, for example the **Rule URL** (a link to the rule, hidden here) and, further down, the **Rule Name**.

8 **Close**. While a ticket is **Pending**, its maker also sees a **Remarks *** box ("Required for withdrawal") and **Withdraw** here; once the ticket has expired they are no longer shown.

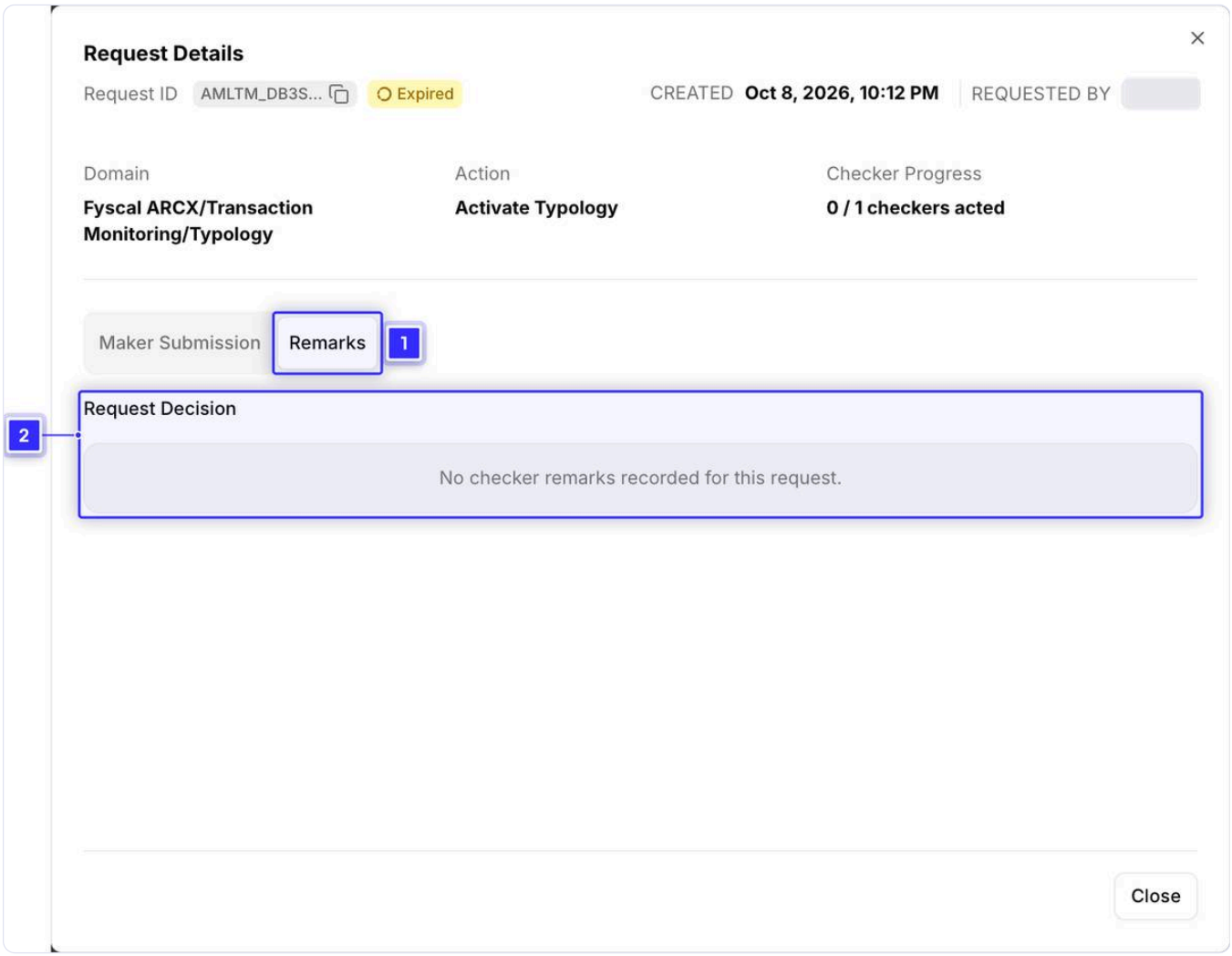


Figure 11.13 The Remarks tab (1): Request Decision (2), showing No checker remarks recorded for this request.

The **Remarks** tab shows **Request Decision**. When no checker has added remarks, it reads "No checker remarks recorded for this request." On a **Pending** ticket, the maker's **Remarks *** box and **Withdraw** stay at the bottom on both tabs.

Step 1 **Open the ticket**

On **Tickets**, click ⋮ on the ticket, then **View**.

Step 2 **Review the request**

On **Maker Submission**, read the **Reason**, **Attachments**, **Data Difference** and **Additional Context**. Click **Remarks** to see any checker remarks.

Step 3 **Withdraw your own request**

If you raised the ticket, enter a reason in **Remarks**, which is required for withdrawal, then click **Withdraw**. To leave without changes, click the × at the top right.

Note

When the maker opens their own ticket, the only action offered is **Withdraw**; no approve or decline buttons appear in the maker's view. The checker's view is not shown in this guide (see Tickets). Ask your administrator which users act as checkers for each activity, or contact support at hello@fyscaltech.com.

REFERENCE & SUPPORT

12 FAQ & Glossary

Short answers to common questions about each module, the terms used in this guide, and how to contact Fyscal Technologies. Each answer links to the section of the guide that describes the screen.

READING TIME
About 43 min

Frequently Asked Questions

The questions are grouped by module, in the order of the sidebar.

Getting started

How do I sign in? +

How do I change my password? +

Where do I see my notifications? +

Why can a colleague see options that I cannot? +

AML Dashboard

What do the six tiles at the top count? +

How do I switch the charts between cases and alerts, or change the period? +

Why do some charts disappear when I switch views? +

How do I read the Daily Jobs grid? +

Cases

How does a case relate to its alerts? +

What statuses can a case have? +

What do I need to dispose of an alert? +

How do I review a case that is in Pending Review?

Can a closed case be reopened?

Where is the history of a case recorded?

Alerts

How do I tell a Name Screening alert from a Transaction Monitoring alert?

What does the SLA Deadline column show?

Why is Disposition greyed out on an alert?

What are hibernated alerts?

Does generating an AI Summary have a cost?

How do I put an alert into a case?

Case Manager Config

How are alerts merged into cases?

How are new cases assigned?

Can I see an earlier configuration?

How do I change the prompt behind Case Copilot or an AI Summary?

Why do I have to enter the Agent Key every time I update the model?

Customer 360

How do I find a customer?

Why don't the KYC Level filter options match the values in the list?

Why are incoming and outgoing totals shown per currency?

Why are the transaction charts empty when the table lists transactions?

Where can I see a customer's earlier cases, screening runs and STRs?

Regulatory Reports

Can I create an STR from Regulatory Reports?

Can I edit a filed STR?

What does the filing deadline next to the Date of determination mean?

How do I get an STR's file?

Why does the total amount read "Mixed"?

Name Screening

What is the difference between Watchlist Search and Manual Screening?

Can I screen a company as well as a person?

How much does each field count towards the screening score?

How are alerts banded by score?

What is the difference between the Batch Screening and Delta Screening pages?

Where does the watchlist data come from?

Transaction Monitoring

Where are monitoring typologies set up?

What happens when I activate a typology?

Does a dry run create alerts?

Why does my condition "Equal 0" never match customers with no transactions?

Why is Save as Draft greyed out?

Why is my typology name rejected?

Why did my dry-run result disappear?

Why does a dry-run window with 0 records scanned show alerts?

How do I see why a Transaction Monitoring alert was raised?

How do I check that monitoring ran?

Data Ingestion

What data does Batch Ingestion import?

How do I see the rows that were not loaded?

What do the job statuses mean?

When does a schedule change take effect?

What file can I upload to the Internal Watchlist?

Maker Checker Approval

What is the difference between Configs and Tickets?

What does an activity define?

Can I approve my own request?

How do I withdraw a request?

What ticket statuses are there?

Glossary

Terms used in this guide, in alphabetical order. Labels are spelled as they appear on screen.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Term	Definition
Activation Mode	The choice made when you click **Activate** on a typology: **Shadow Mode**, "Alert generated against live data will be shown in rule detail page.", or **Published Mode**, "Alert from this rule will flow into Alert Manager." The choice goes to a checker as an **Activate Typology** request, and the typology stays **Draft** while the request waits. See Request Shadow activation.
Activity	In Maker Checker Approval, a configuration that names an action somewhere in the platform and sets its approval rules: SLA, warning point, approval count, and maker and checker permissions. Activity codes begin **ACT_**. See Configs.
Activity Timeline	The panel opened by **Timeline & Notes** on a case or alert. It holds notes and a dated log of events, newest first. See Timeline and notes.
Agentic Workflows	The Case Manager Config page that holds the prompts (**Prompt Config**) and the model configuration (**Model Config**) used by Case Copilot and the AI Summary. See Agentic Workflows: Prompt Config.
Aggregation	The part of Create Variables where you set what a variable calculates: **Field**, **Function** and **Group by**, all required. See Create a variable.
AI Summary	A card on Alert Details that generates a summary of the alert: a verdict, rationale, findings and a recommended action, with the prompt version and model. Each generation costs one run against the daily limit. See Alert Details: Name Screening.
Alert	A single detection that needs review: one screening match or one rule breach. In Fyscal ARCX an alert is raised by Name Screening (ID starting **ALT-NS**) or Transaction Monitoring (ID starting **ALT-TMS**) and listed in **Case Manager → Alerts**. Alerts have six statuses. See Alerts list.
Alert band	A named score range in Name Screening Alert Configuration, with a colour, **Min %** and **Max %**, a **No Alert** setting, an **SLA Deadline** and an **Auto Hibernate** setting. The band and percentage appear as an alert's score, for example **Low 75.76%**. See Alert Configuration.
Alert Manager	A name shown in the **Activation Mode** dialog: in **Published Mode**, "Alert from this rule will flow into Alert Manager." No sidebar item is called Alert Manager. See Request Shadow activation.
AML	Anti-money laundering: the laws, controls and checks that stop criminal money being made to look legitimate. Fyscal ARCX is an AML platform for screening, monitoring, case work and reporting. See How Fyscal ARCX fits together.
AMLC	Anti-Money Laundering Council (Philippines). The STR wizard prepares a GoTRACS-compliant STR for the AMLC. See File an STR.
AND, OR (Match)	How conditions combine. Inside a group, **Match** AND means every row must be true ("AND — all must match"); OR means one true row is enough ("OR — any one matches"). **Combine groups with** does the same between groups. See Building blocks and How conditions are evaluated.
Approval Count	The number of approvals set on a Maker Checker activity. The default on the Create Activity form is 1. See Create an activity.
Auto Assignment of Cases	The part of Case Creation & Assignment that maps a group of alert types to people, with a method such as **Sequential**. See Case Creation & Assignment: Active Configuration.
Auto Hibernate	A Yes or No setting on each alert band in Alert Configuration. See Alert Configuration.
Average	A variable **Function** for numeric fields such as amount: the average value of the field over the window. See Create a variable.
Batch Ingestion	The Data Ingestion page that holds the ingestion schedule and lists the import jobs for Customers, Accounts and Transactions files. See Batch Ingestion.
Batch Screening	The Name Screening page that lists the batch screening runs, with customers scanned, alerts created, errors, watchlist count, status and duration for each run. See Batch Screening.
Beneficiary	The person or organisation that receives the funds or the benefit of a transaction. In an STR, party role **B**. See Step 4: Transaction.
Between, Not Between	Filter operators for number fields: the value falls inside, or outside, a range you give. Rule 1 uses two amount filters to set its band instead. See Building blocks.
BSP	Bangko Sentral ng Pilipinas. The STR **Institution code** is described on screen as an "18-digit code assigned by AMLC/BSP". See Step 2: Report Type.

Term	Definition
Case	A record in **Case Manager → Cases** that holds one or more alerts for a customer, with its own status, assignee and disposition. Case IDs look like **CASE-2026-0034617**. See Case Details.
Case Copilot	An AI Investigation Assistant: a chat panel on Case Details that answers questions about the open case, from prompts such as **Summarize case** or **Explain match scores**. Check its answers against the case. See Case Copilot.
Case Origin	How a case was created: **Manual** or **Automated**. See Cases list.
Checker	The second person in a Maker Checker request: the user who approves or declines it. An activity sets the **Checker 1 Permission** and the **Approval Count**, and a ticket shows **Checker Progress**, for example "0 / 1 checkers acted". No approve or decline buttons appear in the maker's view of their own ticket, which offers only **Withdraw**. See View a ticket.
Condition	One row of a typology group: **WHEN** a variable, an operator, and a **Static Value** or another **Variable** to compare with. A variable only calculates a value; the condition decides whether that value is suspicious. See Create Typology form.
Config version	The unique ID of a saved configuration. Saved configurations are listed in a history tab, where one is **ACTIVE** and the rest **INACTIVE**. See Configuration History.
Count	A variable **Function** that counts the transactions in the window, for example Count of `id` per sender (Rule 1). See Create a variable.
Count Distinct	A variable **Function** that counts the different values of a field, for example the different receivers a sender paid (Count Distinct of `receiver_entity_id`, Rule 5). See Rule 5 · Fan-out.
Counterparty	The other party to a customer's transaction: the receiver when the customer sends, the sender when the customer receives. Customer 360 shows the top counterparties; in an STR, party role **C**. See Analytics tab.
Covered person	In Philippine AML rules, an institution such as a bank that must report suspicious transactions to the AMLC. The phrase appears in the help text of **Date of determination**. See Step 2: Report Type.
Covered Transaction Report (CTR)	A report to the AMLC of a covered transaction, in general one of more than ₱500,000. Fyscal ARCX creates CTRs automatically once a day from ingested transactions, with a CSV in the GoTRACS format. See The CTR register.
Cross-border	A transaction between parties in different countries. Rule 15 adds up what a sender sent to a country other than their own in the last 30 days. See Rule 15 · Cross-border volume.
Customer 360	The module that lists customers and opens a Customer Profile for each: identity and KYC details, accounts, analytics, transactions, prior cases and alerts, screening history and STR history. See The customer list.
Customer due diligence (CDD)	The checks an institution makes on a customer: who they are, their risk rating, whether they are a PEP, their income and source of funds, and how much and how often they expect to transact. Customer 360 shows these details. See The Customer Profile.
Daily Jobs	The AML Dashboard panel that shows the outcome of the platform's scheduled jobs: **Screening & Monitoring Runs** and **Data Ingestion**. See Daily Jobs.
Data Difference	The table on a Maker Checker ticket that shows each changed **Field** with its **Current Value** and **Proposed Value**. See View a ticket.
Date of determination	An STR field, described on screen as the "Date the covered person knew or should have known of the suspicious nature of the transaction. Starts the filing deadline clock." See Step 2: Report Type.
Delta Screening	The Name Screening page that shows the delta screening schedule and lists its runs, including the next scheduled run. Its schedule can be changed with **Change Schedule**. See Delta Screening.
Device, IP address	The device and network address a payment was made from, held in the transaction fields `sender_device_id` and `sender_ip`. Rules 10 and 11 count how many a sender uses; proposals P5 and P6 count how many customers share one. See Rule 10 · Many devices and Rule 11 · Many IP addresses.
Disposition	The outcome recorded for an alert or a case: **True Match**, **False Match** or **Potential Match**. Lists show - until one is recorded. See Case statuses and dispositions.
Dormant account	An account with no activity for a long period. A sudden payment after a quiet spell is a common red flag; Rule 4 looks for no transactions from 100 to 1 days ago, then a payment in the last day. See Rule 4 · Dormant account.

Term	Definition
Draft	A typology status: the rule is saved but not activated. New typologies are saved as Draft, and a rule stays Draft while its activation request is Pending. Dry Run works on a saved draft. See Typology list.
Dry Run	A test of a saved draft typology against past records, started with **Dry Run** on the **Review & schedule rule** page. "No alerts are created during a dry run." The result gives **Records Scanned** and **Alert Created** for each time window, without listing the matches, and is erased when the rule is updated. See Test a typology with Dry Run.
Duplicate	Makes a copy of a typology (the Actions menu of a Draft rule, or **Duplicate Typology** on its page) or of a variable. A variable used in a live rule cannot be edited: duplicate it and change the copy. See View Variable.
Enhanced due diligence (EDD)	Extra checks applied to customers an institution rates as higher risk, such as PEPs: more information on the source of funds and closer review of their activity.
Entity	In Create Variables, the **Transaction** and **Entity** tabs choose whether a variable is calculated from transactions (the default) or from entity data. In the Rule index, Entity is the field a rule's variables are grouped by: sender or receiver. See Create a variable.
Escalated	A status of cases and alerts. In AML work, escalation passes an alert or case to a more senior reviewer. The dashboard tiles **Escalated Alerts** and **Escalated Cases** carry the sub-label **Pending Supervisor Review**, and **All Alerts** and **All Cases** each have an **Escalated** chip. See Case statuses and dispositions.
Execution Interval	How often a Transaction Monitoring schedule runs: a number and a unit, for example every 1 day. See Schedules: Schedule List.
Expired	A Maker Checker ticket status. The activation requests made for this guide expired with no checker action, and their rules stayed Draft: a request has to be approved before it expires, and an expired one needs a new request. See Ticket statuses.
False Match	A disposition value. For an alert it is chosen in the **Dispose Alert** dialog, together with a required **Rationale Code** and **Rationale Details**; a case has its own **Disposition** in the case bar. The other values are True Match and Potential Match. See Dispose alerts and close a case.
False negative	Suspicious activity that a rule or screening check does not alert on. Raising thresholds cuts false positives but can create false negatives, which is why changes are tested first.
False positive	An alert that turns out, on review, not to be suspicious or not to be the listed party. Many false positives usually mean a rule needs tuning. See Tuning and false positives.
Fan-in	Many different senders paying one receiver, a pattern typical of money-mule and pooling accounts. See Rule 6 · Fan-in.
Fan-out	One sender paying many different receivers, for example to spread funds quickly. See Rule 5 · Fan-out.
Field	In Create Variables, the transaction field a variable calculates on, for example `amount`, `id` or `receiver_entity_id`. The field decides which functions are offered. See Create a variable.
Filters	Optional rows in Create Variables (field · operator · value) that limit a variable to matching transactions. Rows combine as "AND — all must match". See Create a variable.
Financial intelligence unit (FIU)	The national agency that receives and analyses suspicious transaction reports. STRs in this guide are prepared for the AMLC. See File an STR.
Four-eyes principle	A control in which one person proposes or decides and a different person checks and approves. Maker Checker Approval and the review of a case in Pending Review apply it. See Configs.
FT AML	The breadcrumb shown at the top of the Transaction Monitoring screens (typologies, variables and schedules). It is a label on those screens, not a separate module: you reach them from **Fyscal ARCX → Transaction Monitoring** in the sidebar. See Typology list.
Function	In Create Variables, the calculation: **Count**, **Count Distinct**, **Sum**, **Average**, **Minimum** or **Maximum**. Numeric fields offer all six; text and ID fields offer only Count, Count Distinct, Minimum and Maximum. See Building blocks.
Fuzzy, Phonetic	The two sub-fields of **Name** in Screening Configuration, each with its own weightage (Fuzzy 80% and Phonetic 20% in the configuration shown). See Screening Configuration.
GoTRACS	The AMLC reporting format the STR wizard follows ("GoTRACS-compliant STR filing for AMLC"). Codes after STR field names, such as H-3 or D-SD-2, are the GoTRACS field references shown on screen. See File an STR.

Term	Definition
Greater Than Equal (>=)	The condition operator most rules in this guide use: the variable is equal to or above the threshold, for example ≥ 10 receivers. See Create Typology form.
Group by	The field a variable is calculated per: `sender_entity_id` gives one result per sender, `receiver_entity_id` one per receiver. See Create a variable.
Hibernated	Alerts shown when the **Show Hibernated** checkbox on All Alerts is ticked. Alert bands carry an **Auto Hibernate** setting. See Alerts list.
Hierarchy	A template in Team Management that defines an organisational structure as levels of roles with members. The AML hierarchy has the levels AML Admin, AML Team Lead, AML Supervisor and AML Analyst. Status: Active, Inactive or Removed. See Team Management: the hierarchy list.
High value	A large total moved in a period. Rule 3 adds up what a sender sent in the last 30 days; High Value (HV01) is also a typology type. See Rule 3 · High value.
High-risk country	A country (jurisdiction) an institution's policy treats as higher risk for money laundering or terrorist financing. Proposal P1 looks for payments to such countries. See Proposed typologies.
In, Not In	Operators that compare a field with a list of values. Type each value and press Enter. See Building blocks.
Ingestion	Loading data files into the platform: customer, account and transaction files in Batch Ingestion, and watchlist files in Watchlist Ingestion. Each job shows its total, ingested and skipped rows. See Batch Ingestion.
Instrument	The card or account a payment is paid from, held in the field `sender_instrument_id`. Rule 12 counts the different instruments a sender used in 7 days. See Rule 12 · Many instruments.
Internal Watchlist	A watchlist source alongside LSEG. You add subjects to it, or remove them, by uploading a CSV file in Watchlist Ingestion. See Upload an Internal Watchlist file.
Is Null, Is Not Null	Operators in the operator lists that test whether a value is empty. In a typology condition they are not saved with the rule, so do not rely on them. To test for "no transactions", see Building blocks.
KYC	Know Your Customer: checking who a customer is and understanding the business they expect to do. Customer 360 shows a **KYC Level** in the customer list (for example Kyc 0, Kyc 1) and **KYC** on the Customer Profile (for example L2). See The Customer Profile.
Large single transaction	One very large payment. Rule 7 takes the sender's largest single amount in the last day; Large Transaction (LT-01) is also a typology type. See Rule 7 · Large single transaction.
Layering	The stage of money laundering that moves funds through many transactions or accounts to hide where they came from. Layering is also a typology type; proposal P2 (pass-through account) looks for it. See Proposed typologies.
Live Alerts, Shadow Alerts	Columns of the Transaction Monitoring Run History: the alerts raised in a run by Published rules (Live) and by Shadow rules. See Schedules: Run History.
Look-back	Another name for a variable's window: the period counted back from the trigger time T. See Building blocks.
LSEG	A watchlist source. LSEG files appear in Watchlist Ingestion in pairs named **watchlist_delta_…** and **watchlist_deleted_…**. See Watchlist Ingestion.
Maker	The user who raises a Maker Checker request, for example by submitting an **Activate Typology** request with a **Reason**. An activity sets the **Maker Permission**. The maker can **Withdraw** their own pending ticket, with a remark, but has no approve or decline buttons. See Tickets and View a ticket.
Maker Checker Approval	The sidebar item that holds the activities that need approval (**Configs**) and the approval requests raised against them (**Tickets**). See Maker Checker Approval.
Manual Screening	The Name Screening page where you enter one person's or company's details and screen them on demand. See Manual Screening.
Match Score	A row of the Matches panel on a Name Screening alert or case. Each watchlist candidate shows its score band and percentage (for example LOW 87.94%), and each field its own **Weightage** and **Score**. See Customer, accounts and matches.

Term	Definition
Matches	The area of a Name Screening alert that compares the customer with each watchlist candidate, field by field, with the weightage and score of each field. See Customer, accounts and matches.
Merchant category code	A code for a merchant's type of business, held in the transaction field `merchant_category_code`. Proposal P7 looks for payments to categories your policy treats as high risk. See Proposed typologies.
Minimum, Maximum	Variable functions: the smallest or largest value of a field in the window. Rule 7 uses Maximum of amount to find the largest single payment. See Rule 7 · Large single transaction.
Money mule	A person whose account is used to receive and pass on criminal money, knowingly or not. Fan-in, many devices on one account, and one device used by many customers are typical signs. See Rule 6 · Fan-in.
Name Screening	Checking customer names against watchlists of sanctioned parties, PEPs and other names of concern. In Fyscal ARCX, the module that runs batch, delta and manual screening and sets alert bands and weightages. See Name Screening.
Operator	The comparison in a filter or condition. Number fields offer Equal, Not Equal, Greater Than, Greater Than Equal, Less Than, Less Than Equal, Between, Not Between, In and Not In; text fields also offer Contains, Starts With, Ends With, Is Null and Is Not Null. See Building blocks.
Party role	The letter shown against each sender and receiver in an STR: **S** Subject of Suspicion, **B** Beneficiary, **C** Counterparty, **T** Transactor, **O** Other participant. See Step 4: Transaction.
Pass-through account	An account where money received is sent on almost in full within a short time, a sign of layering. Proposal P2 describes a rule for it. See Proposed typologies.
Paused	A chip beside a typology's status on its page: the rule is not currently running, and the page offers **Resume**. See Typology list.
PEP	Politically exposed person. Customers carry a **PEP Flag**; watchlist records carry a **PEP Status**. See The Customer Profile and Watchlist Search.
Positive control	A check used in this guide when a dry run returns 0 alerts: lower the threshold so that any matching record would alert, confirm that alerts appear, then restore the real threshold. It shows whether 0 means "no such pattern" or "the rule cannot read the data". See Test a typology with Dry Run.
Potential Match	A disposition value, chosen in the same places as True Match and False Match. In general use it means the evidence is not enough to confirm or rule out the match. See Dispose alerts and close a case.
Predicate crime	A crime that produces the money being laundered, such as fraud, drug trafficking or corruption. STR step 3 lists **Predicate crimes — PC1-PC36**. See Step 3: Reason for suspicion.
Published, Published Mode	Used in three places. A typology status: the rule was activated in **Published Mode**, "Alert from this rule will flow into Alert Manager." In Agentic Workflows, publishing a prompt creates a new version, and saving a model configuration "publishes a new configuration and retires the current one". In Batch Ingestion, **Published** is one of the ten job statuses, which the screen does not describe. See Typology list, Edit and publish a prompt and Batch Ingestion.
Rationale code	The coded reason for a disposition, chosen from a dropdown in the Dispose Alert dialog, for example "Identification number of the user is the same as the watchlist". It is required, together with **Rationale Details** of at least 10 characters. See Dispose alerts and close a case.
Reason for suspicion codes	The codes chosen in step 3 of an STR: Suspicious circumstances **SC1–SC6**, Predicate crimes **PC1–PC36** and Transnational organized crime **MC1**. See Step 3: Reason for suspicion.
Records Scanned	In a Dry Run result and in a rule's run history, the number of records the run read. 0 means there was no transaction data in the window: check data ingestion for that period before judging the rule. See Schedule Details.
Red flag	A sign that activity may be suspicious and worth a closer look. Each Typology Library rule opens with the red flag it looks for. See Rule index.
Risk Level, RISK	The customer's risk rating. The customer list shows **Risk Level** as a coloured tag; the Customer Profile and the case customer card show **RISK** as a tier with a number in brackets, for example HIGH (77). See The Customer Profile.
Risk-based approach	Setting controls in proportion to risk: more checks and lower thresholds for higher-risk customers, products and countries. The Typology Library's thresholds are starting values to set from your own risk assessment.

Term	Definition
Rule Analysis	The tab on a Transaction Monitoring alert that shows the rule triggered, its window and frequency, the number of breaches and each breached condition. See Transaction Monitoring evidence tabs.
Sanctions	Legal restrictions on dealing with named people, organisations, vessels or countries. Sanctioned parties appear on watchlists and are what name screening looks for. See Watchlist Search.
Save as Draft	Saves a new typology with the status **Draft**, on the page after the conditions. It needs a schedule, and the page then becomes **Update Typology**. See Part 6: Save as draft.
Schedule	When a recurring job runs, shown as **Current Frequency**, **Next Run** and **Last Run** on Batch Ingestion, Batch Screening and Delta Screening. A schedule change takes effect after the next scheduled run. In Transaction Monitoring, a schedule has a name, an **Execution Interval**, a start time and an optional end time, and one schedule can drive several rules. See Change the ingestion schedule and Schedules: Schedule List.
Screening Configuration	The Name Screening page that holds the weightages of the screening fields (Name, Address, Citizenship, Gender, DOB) and their sub-fields. See Screening Configuration.
SEGMENT	A tag on the Customer Profile and the case customer card that gives the customer's segment, for example Retail. See The Customer Profile.
Shadow, Shadow Mode	A typology status and **Activation Mode**. In **Shadow Mode**, "Alert generated against live data will be shown in rule detail page": the rule runs on live data and its alerts appear on the rule's page rather than flowing into Alert Manager. In the Activate Typology ticket, **Data Difference** shows Activation Mode changing from - to **shadow**. See Typology list and Request Shadow activation.
Skipped Rows	The rows of a Batch Ingestion file that were not loaded. When above 0, the number is a link that downloads the error rows CSV. See Batch Ingestion.
SLA	Service level agreement. Alerts show an **SLA Deadline** (**On Track** or **Breached**); each alert band sets an SLA Deadline in days, hours and minutes; each Maker Checker activity sets an SLA in hours. See Alerts list.
Smurfing	Many very small payments, often made by several people, that together move a large amount. Rule 8 counts a sender's transactions under ₱1,000 in the last day. See Rule 8 · Smurfing.
Spike	A sudden rise against a customer's own history. Rule 9 compares the sender's 7-day total with their 90-day total. See Rule 9 · Spike against own history.
Static, Dynamic	On a filter row, Static compares the field with a value you type; Dynamic compares it with another field. In a condition the choice is **Static Value** or **Variable**. See Building blocks.
Status (case)	One of eight values: **Not Started**, **Under Investigation**, **Pending Review**, **Escalated**, **STR Draft**, **STR Created**, **Closed**, **Reopened**. Alerts use the same values except STR Draft and STR Created. See Case statuses and dispositions.
STR	Suspicious Transaction Report. Prepared from a case in Case Manager with the six-step STR wizard, "GoTRACS-compliant STR filing for AMLC". Cases with an STR show the status **STR Draft** or **STR Created**, and a filed report is listed, read-only, in Regulatory Reports. See File an STR and The STR register.
STR Type	The type of report chosen in step 2 of an STR: **STRR** (Regular STR), **STRA** (Per Account), **STRHP** (High Priority), **STRHU** (Highly unusual) or **STRBR** (Bulk Report). See Step 2: Report Type.
Structuring	Splitting money into several amounts that each stay below a level that would draw attention. Rule 1 counts a sender's transactions in a band just below an amount you review. See Rule 1 · Structuring.
Subject of Suspicion	The person or organisation whose activity the STR is about. In an STR, party role **S**. See Step 4: Transaction.
Subject parties	Step 5 of an STR: the parties auto-derived from the selected transactions, each with a party role and identity details. See Step 5: Subject parties.
Sum	A variable **Function** for numeric fields: the total of the field over the window, for example the amount a sender sent in 30 days (Rule 3). See Create a variable.
Suppression Window	A setting on a typology: a number (default 0) and a unit such as Hour or Day, for example 7 Day. An information icon (ⓘ) next to the label holds the field's help text. See Create Typology form.

Term	Definition
Team Management	The Case Manager Config page that lists the hierarchy templates and opens the hierarchy builder. See Team Management: the hierarchy list.
THAN MULTIPLIER	In a condition that compares with another **Variable**, the factor applied to that variable: 0.5 means "at least half of it" (Rule 9). See Create Typology form.
Threshold	The value a condition compares a variable with, for example ≥ 10 receivers. Set it from your own risk assessment and check it with a Dry Run. See Tuning and false positives.
Ticket	A request raised for a Maker Checker activity and waiting for approval, identified by a Request ID (the ticket details show a longer ID beginning **AMLTM_**). A ticket starts as **Pending**; the Status filter lists eight statuses. See Tickets and Ticket statuses.
Time Window	The period a variable covers, set as a unit (Hours, Days, Weeks, Months or Years) and a range "Analyze Transaction from X to Y … ago". The range can end before now: 100 to 1 Days covers the 100 days up to yesterday. See Building blocks.
Transaction Monitoring	Checking customers' transactions for patterns that may be suspicious. In Fyscal ARCX, the module that holds the typologies, variables and schedules and raises alerts with IDs starting **ALT-TMS**. See Transaction Monitoring.
Transactor	The person who carries out a transaction, who may differ from the account holder. In an STR, party role **T**. See Step 4: Transaction.
Transnational organized crime	Serious crime planned or carried out across borders by organised groups. STR step 3 lists it as code **MC1**. See Step 3: Reason for suspicion.
Trigger time (T)	The time a rule's run starts. Variable windows are counted back from it; the form reads "This variable will be triggered time 00:00:00 on day T." See Building blocks.
True Match	A disposition value, chosen in the same places as False Match and Potential Match. In this guide, a case that is **Closed** with the disposition True Match shows **File STR**. See File an STR.
Tuning	Adjusting a rule's thresholds, windows, filters and Suppression Window so that it raises useful alerts. Run a Dry Run after each change. See Tuning and false positives.
Typology	A known pattern of money-laundering or terrorist-financing behaviour. In Fyscal ARCX, a Transaction Monitoring rule that looks for one, with an ID starting **TMR-**. It holds one or more conditions on variables, a typology type, a suppression window and a schedule, and has the status **Draft**, **Shadow** or **Published**. New typologies are saved as Draft and are activated through a Maker Checker request. The Typology Library gives tested examples. See Typology list and Typology Library.
Typology type	The category chosen for a typology on the Create Typology form, for example Structuring (TP100), Velocity (V-01) or Anomaly (TP103). The list shows **No category** when none was chosen. See Building blocks.
UID	A unique identifier. Watchlist records have a UID (for example 3601955), and so do Maker Checker activities (codes beginning **ACT_**). See Watchlist Search.
UTC	Coordinated Universal Time. Schedule run times in the Change Screening Schedule and Change Ingestion Schedule dialogs are given in UTC. See Delta Screening.
Variable	A named calculation with an ID starting **VAR-**, such as the number of transactions a sender made in the last 7 days. It is set by a **Field**, a **Function** (for example Count or Sum), a **Group by** field, a **Time Window** and optional **Filters**. Typology conditions test variables, and one variable can be used by many typologies. When a customer has no records in the window, the value is empty, not 0. See Variables list and Building blocks.
Velocity	Many transactions in a short time. Rule 2 counts a sender's transactions in the last day; Velocity (V-01) is also a typology type. See Rule 2 · Velocity.
Watchlist	The records that names are screened against, from the sources **LSEG** and **Internal Watchlist**. Each record has a UID, name, PEP status, country, category and date of birth. See Watchlist Search.
Watchlist Ingestion	The Data Ingestion page that lists each watchlist file loaded into the platform, with its source, status and rows processed. See Watchlist Ingestion.
Weightage	The share a screening field or sub-field carries, set in Screening Configuration. The field weightages add up to 100%. Manual Screening shows the weightage next to each field. See Screening Configuration.

Term	Definition
Withdraw	The action in the maker's view of their own Pending ticket that withdraws the request; **Remarks** is required. See View a ticket.

> **Note**
> The screens do not define the three dispositions. For their usual meaning in AML work, see the AML context in Case statuses and dispositions; follow your institution's own definitions.

Help & Support

Common issues

Issue	What to do
You cannot sign in	Check your email and password, or click **Forgot password?**. See Signing in.
Continue to Password Change is greyed out	Enter both your registered email and your current password. See Changing your password.
Disposition is greyed out on an alert	The alert is **Not Started**. Disposition can be opened once the alert is **Under Investigation** and assigned. See Work an alert.
Add note is greyed out	Type a note in **ADD A NOTE** first. See Timeline and notes.
Proceed to screen is greyed out	The form is empty. Enter at least the **Customer Name**, the only required field. See Manual Screening.
Review Changes is greyed out in Change Screening Schedule	Enter a **Reason** for the change. See Delta Screening.
A schedule change has not taken effect	A schedule change takes effect after the next scheduled run. See Change the ingestion schedule.
A Completed ingestion job shows skipped rows	Click the red **Skipped Rows** number to download the error rows CSV. See Batch Ingestion.
Upload & Add is greyed out	Choose a CSV file first. Only CSV format is supported. See Upload an Internal Watchlist file.
Transaction charts are empty but the table lists transactions	Change the date range above the charts to the period of the transactions. See Transactions tab.
Save as Draft is greyed out on a typology	Choose a schedule whose start time is in the future. See Before you build.
Update seems to do nothing on a typology that has a dry-run result	Look for the **Update Typology** dialog ("Your dry run results would be erased ...") and confirm it. See Test a typology with Dry Run.
Unable to load MCA config, with "insufficient scopes in the provided token"	The message appears in an activity's View window and in the Diff Fields box of Edit. Contact support with the activity name and UID. See Activity actions.

Contact support

- **Email**: hello@fyscaltech.com
- **Phone**: +65 8080 5424
- **Headquarters**: 68 Circular Road #02-01, Singapore 049422
- **India office**: GM IT Park, Sector 142, Noida 201305, India

RELATED IN REFERENCE & SUPPORT

Release Notes

REFERENCE & SUPPORT

13 Release Notes

Changes to Fyscal ARCX and to this guide, newest first. Each entry links to the chapter that describes the change.

2 November 2026

- **Changed: STR Listing is now Regulatory Reports.** The STR Listing page is renamed Regulatory Reports and now has two tabs, STR and CTR, switched at the top right. The STR tab works as before. See The STR register.
- **New: Covered Transaction Reports (CTR).** CTRs are created automatically once a day at 3:00 AM from uploaded transactions above the threshold (in general, more than ₱500,000), each with a filing deadline and a CSV in the AMLC GoTRACS format to download for filing. See The CTR register.

29 October 2026

- **New: Customer Risk Profile (CRP).** Risk Score Configuration and Score Configuration under Customers: choose the customer attributes to score, give each value a score from 0 to 100, weight the attributes up to 100% in total, set the Low, Medium and High score bands, and activate versions from a draft, with a full configuration history. Each customer's score and its breakdown appear on the new Customer Risk Score tab of the Customer Profile. See Customer risk profile.

8 October 2026

- **New: Typology Library.** Fifteen example typologies built in Transaction Monitoring, each with its variables and conditions, a dry-run result and a Shadow activation request, plus how to test a rule with Dry Run and request Shadow activation through Maker Checker Approval. See Typology Library.

7 October 2026

- **New: AML Dashboard.** Six metric tiles (Overdue, Unassigned, Escalated and Pending alerts; Pending and Escalated cases), case and alert distribution by status, disposition, score, type, assignment and age, an STR Filed chart, and a Daily Jobs grid for Batch Screening, Delta Screening, TM Runs and Data Ingestion. See AML Dashboard.
- **New: Maker Checker Approval: Tickets.** Approval requests, such as Activate Typology, are listed as tickets with a request view (Maker Submission and Remarks tabs). The Status filter lists eight statuses: Pending, In Progress, Execution Pending, Approved, Declined, Withdrawn, Expired and Execution Failed. Activity configurations are under Configs. See Tickets.
- **New: Team Management.** Hierarchy templates under Case Manager → Config, with a Template Builder and a Hierarchy Builder. The AML hierarchy has the levels AML Admin, AML Team Lead, AML Supervisor and AML Analyst. See Team Management.
- **New: Pending Review on cases.** A case awaiting review shows a Pending Review panel with Review Decision, Approve and Reject. See Review a case in Pending Review.
- **New: Upload Internal Watchlist.** Add subjects to, or delete them from, the Internal Watchlist by uploading a CSV file from Watchlist Ingestion. See Upload an Internal Watchlist file.
- **New: AI Summary and Agentic Workflows.** Alerts can generate an AI Summary on request. Agentic Workflows has Prompt Config, with prompt revisions, and Model Config, with previous configurations. See Agentic Workflows.
- **New: Typology run history and Schedules.** Schedule Details shows each typology's run history, and Schedules has Run History and Schedule List views. See Schedule Details.
- **New: Watchlist Entity Details.** Opening a Watchlist Search result shows the entity in four tabs: Profile & Identity, Risk & Background, Network & Locations and Source. See Watchlist Entity Details.