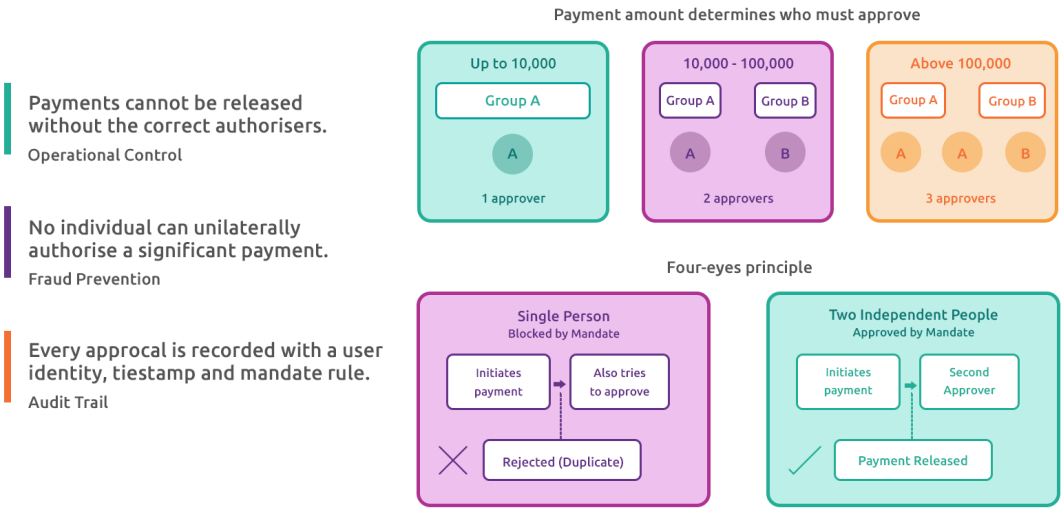
How Banking Mandates Protect Your Treasury from Unauthorised Payments



In treasury operations, the question is never whether controls are needed — it is whether the controls you have are actually enforced. A payment authorisation policy written in a procedure manual and circulated by email is a start. But a policy that lives only in a document can be ignored, forgotten, or bypassed under the pressure of an end-of-day settlement deadline.

A Banking Mandate takes that policy off the page and puts it inside the payment system itself. It defines, in precise and enforceable terms, who must approve a payment — and the system simply will not let the payment move forward until those requirements are met.

Here is how that changes the risk picture for a treasury team.

PROPORTIONAL CONTROLS FOR PROPORTIONAL RISK

Not all payments carry the same risk. Paying a small operational expense is a different act from wiring a seven-figure settlement. Treating them identically —

demanding the same number of approvers for every transaction regardless of size — either creates unnecessary friction for low-value routine payments or, worse, leads to approvals being rubber-stamped because the process is felt to be excessive.

A Banking Mandate solves this by tying the authorisation requirement directly to the payment amount. A typical structure might look like this:

> Up to 10,000: Any one authoriser from Group A
> 10,001 to 100,000: One from Group A and one from Group B
> Above 100,000: Two from Group A and one from Group B

As payment value rises, so does the number and seniority of approvers required. The thresholds are set by the business and enforced automatically — no one has to remember to escalate a large payment for extra sign-off. The system checks the amount, looks up the relevant tier, and enforces the correct combination. It is always consistent, regardless of who is at their desk that day.

THE END OF THE "ONE-PERSON PAYMENT"

One of the most persistent fraud vectors in treasury is the ability of a single person to both initiate and authorise a payment. Even where internal policy prohibits this, a manual process — email approval chains, spreadsheet sign-offs, paper authorisation forms — is difficult to audit in real time and easy to circumvent under pressure.

With a Banking Mandate in place, the payment workflow enforces four-eyes principle structurally. A payment cannot be sent unless the required combination of approvers from the required groups have each independently recorded their approval. The person who set up the payment configuration cannot be the only approver if the mandate requires a second signatory from a different group.

Nor can the same individual approve twice. The system records each approver by their user identity and blocks duplicate approvals. Group membership is set by administrators — it cannot be self-assigned.

SIGNING COMBINATIONS REFLECT HOW YOUR BUSINESS ACTUALLY WORKS

Real treasury teams are not homogeneous. A typical setup might have a group of

payment administrators who handle the preparation work and a separate group of senior treasury officers who hold authorisation authority. The mandate can require one from each group for mid-range amounts, or two senior officers for high-value transactions.

The OR logic in signing combinations adds further flexibility. A tier might accept “two from Group A, OR one from Group A and one from Group B”. This means the control adapts to staffing reality — if only one Group A officer is available on a given day, the payment can still proceed provided a Group B co-signatory is present. The control is not so rigid that it brings operations to a halt, but it is not so loose that it can be circumvented by a single individual.

The important point is that the flexibility is designed in and approved in advance. It is not improvised at the point of payment.

AN UNAPPROVED MANDATE HAS NO EFFECT

One design feature worth noting: a mandate only takes effect once it has been explicitly approved by an authorised user. A newly created or recently modified mandate sits in a “Not Approved” state and is ignored by the payment workflow entirely.

This is a deliberate second-gate control. It means that a rogue or erroneous change to a mandate — whether a well-intentioned misconfiguration or a malicious amendment — cannot immediately affect live payments. A second pair of eyes must review and approve the mandate before the new rules apply.

Every change to a mandate is logged with the user identity and timestamp. The full history of every amendment is retrievable at any time.

GAPS AND ERRORS ARE CAUGHT BEFORE THEY CAN DO DAMAGE

Configuring a mandate with gaps in amount coverage — a band from 0 to 10,000 and the next from 10,002 upwards, with nothing at 10,001 — is a common human error in a manual process. That gap might pass unnoticed until a payment of exactly that amount is submitted and the system cannot determine which signing rule applies.

The mandate configuration validates contiguity before saving. A gap will be flagged immediately, and the mandate cannot be saved until it is corrected. The

same applies to overlapping bands, rules that reference groups which have not been defined, and missing member assignments. The system enforces coherence at the point of setup, not at the point of payment.

WHAT THIS MEANS FOR TREASURY RISK

The practical effect of a well-configured Banking Mandate is a reduction in three distinct categories of treasury risk:

> Operational risk — payments cannot be released without the correct authorisers. Procedural lapses, forgotten escalations, and deadline pressure cannot override the control.
>
> Fraud risk — no individual can unilaterally authorise a significant payment. Even if a user's credentials are compromised, the attacker must also control a second independent authoriser in the required group. Separation of duties is structural, not procedural.
>
> Compliance risk — every approval is recorded with a user identity, timestamp, and the mandate rule that governed it. Auditors can verify that every payment was authorised correctly. There is no reliance on paper trails or email threads.

A mandate is, in essence, a formalisation of the treasury governance policy that your board has approved — expressed in a form the system can actually check. Getting it right is not complex. But the discipline of setting it up accurately, reviewing it regularly, and ensuring membership reflects current staffing is what makes the control real rather than theoretical.