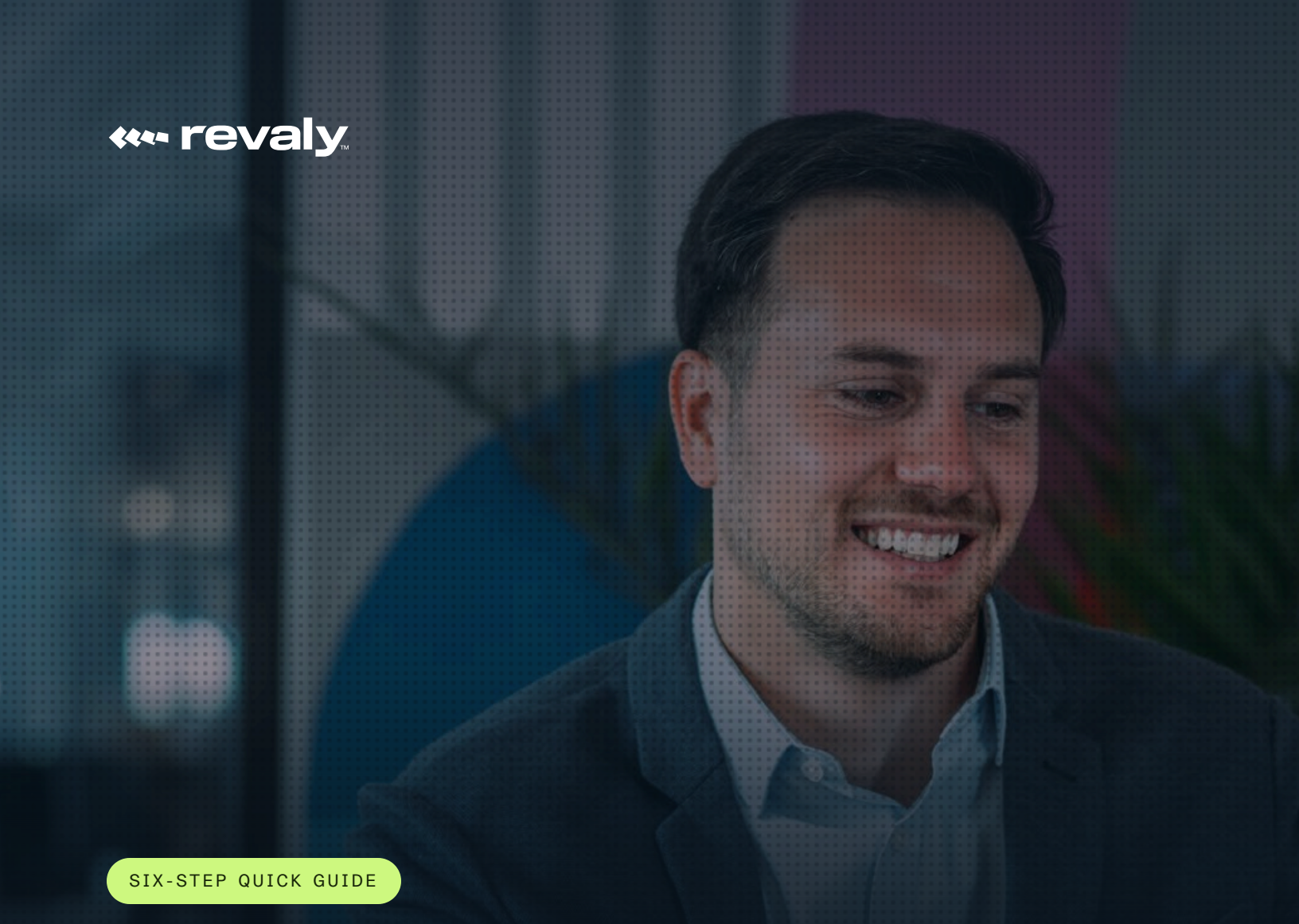


revaly™

SIX-STEP QUICK GUIDE

How to recover soft declines in subscription billing

A practical guide for preventing avoidable payment failures, recovering more soft declines, and reducing involuntary churn.

- Approvals aren't luck. They're engineered.

The scale of the problem

A LARGE SHARE OF LOST SUBSCRIPTION REVENUE STARTS WITH A FAILED PAYMENT.

Subscription businesses often read churn as a verdict on value or price — a customer who decided the product wasn't worth it. In many cases the customer made no such decision: a renewal failed, the account lapsed, and the outcome was still recorded as churn. The customer may not even have known there was a problem until access was interrupted.

That distinction matters because payment-driven churn, commonly referred to as involuntary churn, is often preventable or recoverable. When it's grouped with voluntary churn, teams lose visibility into how much revenue could still be protected and may respond with changes to pricing, product, or retention strategy when the real issue is a failed payment.

INVOLUNTARY CHURN

34%

of total churn is involuntary — the customer was lost to a failed payment, not an active decision to cancel. *(Stripe, The State of Subscription and Billing Management)*

GLOBAL LOSS / YEAR

$129B

in projected global losses from failed subscription payments this year, per industry estimates. *(LexisNexis Risk Solutions, True Cost of Failed Payments)*

RECOVERABLE

80%+

of payment failures are soft declines - recoverable with better data, timing, routing, credentials, or retry logic. *(Checkout.com)*

WHERE TO START

The first step is to separate payment-driven churn from voluntary churn, then identify which failures can be prevented, which can be recovered through better payment logic, and which require customer action.

The next six steps walk through how to classify declines, diagnose their cause, improve first-attempt approvals, tailor retries, use customer outreach more intelligently, and measure the revenue impact accurately.

Separate soft declines from hard declines

DIFFERENT DECLINE TYPES REQUIRE DIFFERENT RESPONSES.

A decline code tells you that a payment failed, but not always why it failed or what should happen next. Some failures can recover through better timing, routing, or transaction data. Others require the customer to update their payment method. Separating the two helps teams focus retries where they can still work and move customers to an update flow when they cannot.

RULE OF THUMB

Soft declines usually require a change to the payment process.
Hard declines usually require a change to the payment method.

RECOVERABLE

Soft declines

- Insufficient funds
- Issuer unavailable
- Do-not-honor
- Generic decline
- Processor timeout

Often temporary: the issuer was unavailable, the timing was poor, credentials were stale, or the request lacked the data to look trustworthy.

MAY RECOVER THROUGH

Different retry timing, routing, credentials, and issuer signals can give a declined payment a better chance of approval.

CUSTOMER ACTION NEEDED

Hard declines

- Stolen card
- Closed account
- Invalid card number
- Suspected fraud
- Permanently blocked

The current payment method can no longer complete the transaction. The customer generally needs to update their details or provide another method.

WHY NOT RETRY

Repeated retries are unlikely to change the outcome and can add fees or draw scrutiny from card networks and issuers.

KEY TAKEAWAY

Classifying the decline correctly determines whether the next step should be a retry, a change to the transaction, or customer action.

Diagnose the root cause

THE DECLINE CODE IS ONLY ONE PART OF THE PICTURE.

The same decline code can appear across transactions with very different causes — issuer risk, incomplete data, stale credentials, poor timing, or a temporary balance issue. Responding to the code alone applies one action to failures that need different fixes; look instead for patterns across issuers, processors, card types, segments, billing dates, and previous attempts.

LOOK FOR PATTERNS BY

Issuer · Card type · Decline reason · Processor · Region · Billing date · Amount · Customer tenure · Retry attempt · Time of day

ISSUER FRICTION

If many declines come from the same bank, region, processor, or card type, the customer may not be the issue. The payment may be failing because of how the transaction is being recognized, formatted, or routed.

DO – Compare approval patterns across issuers, processors, regions, and routes; then adjust the format or path before retrying.

CARD LIFECYCLE

Cards expire, get reissued, or receive updated details while the merchant keeps billing the old credential. If declines are tied to expired cards, reissued cards, or older stored payment methods, the issue may be stale payment data rather than customer intent.

DO – Use tokenization, account updater, and simple update flows before the next attempt.

TIMING & AMOUNT

Some payments fail because they are attempted at the wrong time. If declines cluster around billing dates, pay cycles, or certain transaction amounts, the issue may be timing rather than the customer's willingness to pay.

DO – Time the next attempt to cash availability, billing date, and prior customer behavior.

CASE STUDY

ADAPTIVE HEALTH

+15% increase in payment recovery

Adaptive Health increased retained revenue from recovered payments — after separating decline reasons and applying a different action to each category.

KEY TAKEAWAY

Effective recovery depends on identifying the cause of the failure and changing the conditions around the next attempt.

Improve first-attempt approvals

THE STRONGEST RECOVERY IS A PAYMENT THAT SUCCEEDS THE FIRST TIME.

First-attempt approvals are the cleanest way to protect renewal revenue. When a payment goes through the first time, the customer never sees a warning, loses access, questions the charge, or has to update their card. Some failures will still need recovery, but the strongest payment strategy reduces avoidable failures before they happen. Many factors influence whether a payment is approved on the first try, from how credentials are stored to how transactions are routed and recognized. The three below are practical places to start.

Network tokenization

Tokenization swaps the stored card number for a secure token that updates as credentials change so legitimate renewals continue without asking the customer to re-enter anything.

WHY – Keeping credentials current reduces expired-card declines, resulting in cleaner authorization data and fewer customer interruptions.

Smart routing

The same payment can perform better through one processor than another, depending on the issuer, region, and card type. Smart routing uses those patterns to choose the path most likely to result in approval.

WHY – Small gains compound across a large volume of recurring transactions with no change to product, price, or experience.

Clear statement descriptors

A recognizable charge helps the customer connect the transaction to the subscription they bought, reducing disputes, support requests, confusion, and fraud concerns.

WHY – Recognizable charges are easier to trust and less likely to create friction after approval.

KEY TAKEAWAY

Improving first-attempt approvals protects revenue before the customer experiences a failed payment or needs to take action.

Match retry logic to the failure

A RETRY WORKS BEST WHEN THE NEXT ATTEMPT IS MEANINGFULLY DIFFERENT.

Many businesses retry every failed payment on a fixed schedule — the next day, a few days later, once more the following week. It's easy to operate, but it ignores the cause. An issuer that was briefly unavailable may recover within hours; an insufficient-funds decline may do better after a payday; a generic decline may need different data or routing first.

GENERIC RETRY

Same schedule for every failure; ignores reason, issuer, history, amount, processor, and likelihood of recovery.

Repeated attempts on payments that can't succeed; mistimed retries on ones that could.

REASON-SPECIFIC RETRY

Adjusts timing, routing, data, and number of attempts to the cause of the failure.

The next attempt is designed around what's most likely to work, not a calendar.

DESIGN THE NEXT ATTEMPT AROUND THE DECLINE REASON

Insufficient funds
Retry after a likely payday, when the customer is more likely to have funds available.

Issuer unavailable
Retry within a few hours; these often resolve quickly.

Generic / do-not-honor
Change timing, data, or routing before retrying.

Card lifecycle issue
Refresh credentials first — stale details keep failing.

REASON-SPECIFIC RETRIES CAN RECOVER

45–70%

of soft declines — often well above a generic fixed schedule, without adding any acquisition cost. (Revaly internal analysis)

KEY TAKEAWAY

Retry performance improves when timing, routing, and transaction treatment reflect the reason the payment failed.

Move beyond traditional dunning

REACH OUT BASED ON WHETHER THE CUSTOMER NEEDS TO ACT.

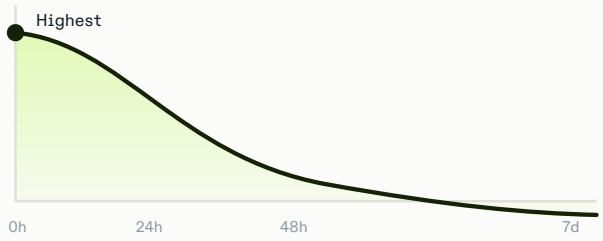
Traditional dunning emails the same sequence after every failure, timed by days since failure rather than the reason. That creates friction, because many soft declines recover without customer involvement. A stronger approach uses payment signals to decide between silent recovery and outreach.

USE SILENT RECOVERY WHEN

The issue is likely temporary · issuer/processor was unavailable · a better-timed retry may resolve it · credentials can refresh automatically · another attempt is pending

USE CUSTOMER OUTREACH WHEN

The card is closed, invalid, or unavailable · billing details need updating · retries are exhausted · the account nears interruption · another method is required



RECOVERY RATE BY TIME SINCE FAILURE

Recovery is highest soon after the failure and declines over time. Begin quickly, with backend action and communication coordinated around the cause.

Once customer outreach is needed, how the message is communicated can make the difference between a recovered payment and a lost customer. These three practices help reduce friction and improve completion.

TIP 1

Lead with the consequence

Your access ends in 3 days" gives the customer a reason to act. "Your payment failed" only describes the problem.

TIP 2

Make updating easy

Make the payment-update flow direct and secure, with no forced login or unnecessary re-entry. Every extra step adds friction and increases drop-off.

TIP 3

Coordinate with retries

Don't ask customers to act while a retry is still pending.

KEY TAKEAWAY

Customer outreach works best when it is triggered by a genuine need for customer action and coordinated with the recovery process.

Measure recovery accurately

MORE THAN A SINGLE RECOVERY RATE.

Decline rate shows how many payments failed — not what was preventable, recovered, or lost. A useful framework separates prevention, recovery, customer action, and downstream retention across six metrics.

1 First-attempt approval rate

How much legitimate revenue clears before recovery is needed — the clearest measure of prevention.

2 Soft decline recovery rate

How effectively recoverable failures are saved. Segment by reason, issuer, attempt, and method.

3 Involuntary churn rate

Customer loss caused by payment failure, not intent — a payment problem, not a value problem.

4 Revenue recovered by reason

Which reasons, issuers, and strategies drive the most value — where to focus next.

5 At-risk accounts retained

Recovery saves the transaction; retention shows the relationship continued.

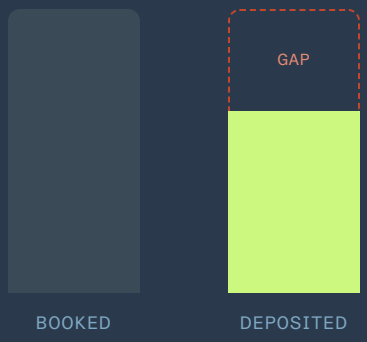
6 Customer-assisted recovery

How much came from customer action — a high rate may mean too many failures reached the customer.

THE SANITY CHECK

Compare booked revenue with actual deposits

The difference between what you billed and what settled is a rough estimate of the revenue still recoverable.



KEY TAKEAWAY

Payment performance should be measured across approvals, recovery, customer action, retention, and revenue.

Payment performance falls between teams

Failed-payment recovery usually touches several functions. Each owns part of the process, but the full payment journey often has no single owner.

01
Billing
owns the retry logic

02
Fraud
owns the risk rules

03
Retention
owns the churn number

04
Finance
sees the revenue gap

05
Support
handles complaints & exceptions

Billing manages retries. Retention sends dunning emails. Support helps customers update details. Finance reports the revenue that wasn't collected. Fraud manages rules that affect approval. When these functions operate separately, teams miss the patterns connecting issuer behavior, credentials, routing, timing, outreach, and retention.

A more effective operating model brings these areas together and uses the same payment signals throughout the process. That means connecting the work that happens before a payment fails, the decisions made after a decline, and the way the outcome is measured across the business.

> Each team owns part of the process, but the full payment journey often has no single owner. That's the gap.

ONE CONNECTED PROCESS

Five moves, working from the same signals.

01

Prevent

Improve how legitimate payments are presented before the first authorization attempt.

02

Diagnose

Determine whether the failure came from issuer friction, outdated credentials, timing, routing, or a permanent payment-method issue.

03

Recover

Select the retry timing and path that best fits the reason for the decline.

04

Reach out

Contact the customer when their action is required, and coordinate the message with any remaining recovery attempts.

05

Measure

Track first-attempt approvals, recovered revenue, retained accounts, involuntary churn, customer-assisted saves, and overall revenue impact.

RECOVER MORE OF THE REVENUE YOU'VE ALREADY EARNED

Revaly brings payment signals, issuer intelligence, credential management, retry logic, and customer outreach into one connected process — helping subscription businesses prevent more avoidable declines, recover more legitimate payments, reduce involuntary churn, and protect customers who expected their subscription to continue.

Talk to us about payment performance.

Discover what we can do for your organization.

Get started →