# The Robinhood Trading Agent Setup

## Rules-First Automation for a Dedicated Account

By Orinami Daodu

---

# Read This First — Risk Disclaimer

Trading stocks and ETFs involves risk, including the possible loss of some or all of the money you put in. Prices move. Orders do not always fill at the price you expect. A stop order limits losses in normal conditions; it does not guarantee an exit price, and it does not protect you from every kind of move.

This guide is an educational setup manual. It explains how to connect an AI agent to a Robinhood account and how to fence that connection in with written rules. It is **not financial advice**. It is not a recommendation to buy or sell anything. No setup, rule set, automation, or strategy in this book guarantees a profit — anyone who tells you otherwise is selling you something other than the truth.

The automation described here runs exactly the size you fund it with, and no bigger. That is deliberate. **Never fund a trading agent — or any trading account — with money you cannot afford to lose entirely.** Start with an amount small enough that losing it would be a lesson, not a problem.

If you are not comfortable with every sentence on this page, close the book and do not build this. The setup will still be here when you are.

---

# Introduction: What "an Agent That Trades" Actually Means

Most people hear "AI trading bot" and picture a machine printing money while its owner sleeps on a beach. That picture is fiction, and this book will not sell it to you.

Here is what the setup in this book actually is: an AI assistant — in my case, Muse — connected to Robinhood's Agentic Trading through Robinhood's own MCP server. The

agent can read my accounts, look at positions, check quotes, and, because I deliberately enabled it, place orders on **one small, dedicated account** that exists for exactly this purpose.

The "works while you sleep" part is real, but it is narrower than the fantasy. It means three specific things:

1. **Scheduled checks.** The agent reviews the account on a rhythm I set — positions, stops, drawdown — whether or not I remember to open the app.
2. **A 24-hour entry window.** Entries can be placed as limit orders outside regular market hours, so a plan made on Sunday evening does not have to wait for me to be awake, free, and at my phone at 9:31 a.m. on Monday.
3. **Resting stop orders.** Every position carries its exit with it. If a position falls to its stop during the trading day, it sells — I do not have to be watching, deciding, or overcoming the urge to "give it one more day."

That is the whole trick. Not prediction. Not genius stock picks. **Automation of discipline**: the boring, rule-following parts of trading that humans are bad at because we get busy, emotional, or greedy.

And the foundation under all of it is this: **the rules were written before the agent was allowed to place a single order.** Cash only. Small positions. Few positions. An exit attached to every entry. A drawdown line that stops everything. If you take one idea from this book, take that one. The technology is the easy part. The rules are the product.

My own deployment is deliberately unimpressive: a learning account funded with $496, holding two small ETF positions, each with a resting protective stop. That is not a failure of ambition. That is the correct size for proving a system before you trust it with more — and this book will keep telling you to stay at that size longer than feels exciting.

---

# Chapter 1: The Architecture

Before you connect anything, understand what you are connecting. There are three pieces.

## Piece one: the agent

The agent is an AI assistant — Muse, in my setup — that can use tools. Given the right connection, it can look up account information, read positions, fetch quotes, and place or cancel orders. On its own, an agent knows nothing about your accounts and can touch nothing. Everything it can do flows through the connection you grant it, and — this matters — only through the operations you allow.

## Piece two: Robinhood's Agentic Trading MCP server

Robinhood offers Agentic Trading through an MCP server (at agent.robinhood.com). MCP is a standard way for AI agents to connect to outside services. You link your agent to Robinhood with an OAuth sign-in flow, the same kind of "sign in and approve access" flow you have used for other apps. One practical detail that surprises people: **the connection flow has to be completed on a desktop browser.** Budget for that; do not start this on your phone at midnight.

## Piece three: the one tradable account

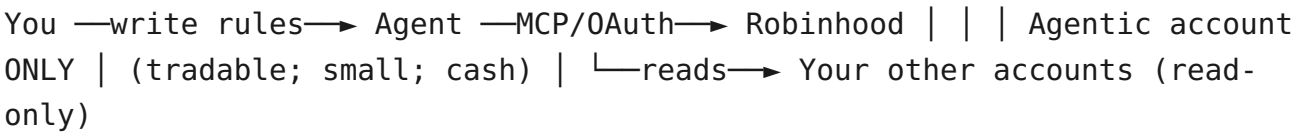
This is the most important architectural fact in the book, so it gets its own paragraph:

**Exactly one of your Robinhood accounts is tradable by the agent: the dedicated Agentic account. Robinhood enforces this on their side, not yours.**

The agent can read your other accounts — your main brokerage, your retirement accounts — which is genuinely useful for reviews and net-worth checks. But it cannot place orders on them. Order tools reject them. It also cannot move money between accounts. Your retirement account is not one bad prompt away from being day-traded, because the platform itself will not allow it.

That enforced separation is what makes this setup sane. You are not handing an AI the keys to your financial life. You are handing it a small, fenced yard, built by the broker, and then fencing it further with your own rules.

## The shape of the whole system




Everything in the chapters ahead hangs off this shape: one small tradable account, rules written by you, an agent that operates inside both fences.

---

# Chapter 2: Account Setup

Do this chapter before you touch the connection. Order matters.

## Use the dedicated Agentic account

Robinhood's agentic setup designates a dedicated account for agent trading. Use it, and only it, for this system. Do not try to make your main account the trading account — the platform will not let the agent trade it anyway, and that restriction is a feature. Your main account, your IRA, your long-term holdings: they stay read-only to the agent, permanently.

## Cash, not margin

Run the Agentic account as a **cash account**. No margin, no borrowing, no exceptions, and this rule is not negotiable within this system. Margin multiplies mistakes, adds interest costs, and creates the possibility of losing more than you deposited. An automated system should never be able to spend money that is not there. If your dedicated account is set up with margin, switch it to cash before funding it.

## Fund it small — smaller than that

Fund the account with a learning amount. Mine is $496. Yours should be whatever number you can lose completely without it changing your month, your mood, or your opinion of the whole project. For most people starting out, that is a few hundred dollars.

Small funding does three jobs:

- It caps the total possible damage from any bug, bad fill, or misunderstanding while you learn how the system behaves.
- It forces the rules to do the work, because the position sizes are so small that no single trade matters.
- It makes the drawdown halt (Chapter 4) a cheap alarm instead of an expensive one.

You can always add money later, after the system has run clean for months. Raising the stakes is a one-way door you should walk through slowly.

## Leave the rest of your accounts alone

Do not consolidate anything into the Agentic account. Do not move positions into it "so the agent can manage them." The agent's job is to run a small, rule-bound experiment. Your real portfolio's job is to be left alone.

---

# Chapter 3: Connect and Verify

Now connect the agent — in read-only mode first. The principle for this whole chapter: **prove you can see everything before you allow the agent to do anything.**

## Step 1: Complete the OAuth flow on desktop

Start the connection from your agent's connector or setup flow for Robinhood Trading and complete the OAuth sign-in on a desktop browser. You will sign in to Robinhood and approve the connection. If a step fails or looks wrong, stop and restart rather than pushing through — a half-completed authorization helps no one.

## Step 2: Read the account list

With the connection live, have the agent list your accounts. You are looking for two facts:

1. **Which account is flagged as agent-tradable.** Confirm it is the dedicated Agentic account and no other. This flag is set on Robinhood's side. If what you see does not match that expectation, stop here and sort it out before going further.
2. **That your other accounts appear as readable but not tradable.** This is the fence from Chapter 1, and you should see it with your own eyes rather than take this book's word for it.

## Step 3: Read the portfolio and positions

Have the agent pull the Agentic account's portfolio and positions. On a fresh account this should show your small funding amount as cash and no positions. Read the numbers back against what the Robinhood app shows you. They should match exactly. This read-back habit — the agent reports, you verify against the source — is the single most valuable routine in this book, and it starts now.

## Step 4: Check the trade-approval setting

Robinhood has a trade-approval setting for the Agentic account. With approvals **on**, every order the agent wants to place waits for your tap in Robinhood before it goes through. With approvals **off**, the agent's orders execute on their own.

Read the current setting and write down what it is. You will make a deliberate choice about it in Chapter 4 — but whatever you choose, choose it on purpose. My guidance for your first months: **leave approvals on** while you watch how the agent behaves. Approvals off is a graduation, not a starting point.

## Step 5: Do not enable order tools yet

If your agent setup lets you control which operations are allowed, keep order placement blocked until Chapter 4 is finished — your rules written, your funding in place, your verification done. An agent that can look but cannot yet trade is the correct intermediate state, and there is no prize for skipping it.

# Chapter 4: Write Your Rules Before Any Order

This is the chapter the whole book exists for. Everything else is plumbing.

An agent without written rules is just a faster way to make unwritten decisions. Your rules convert the agent from a novelty into a system: they define what it may buy, how much, how often, how it exits, and when it must stop entirely. Write them down — actually down, in a document — before the first order is possible.

Below is the exact rule set my setup runs on. After it, there is a worksheet to write your own version. Do not copy my numbers blindly; copy the shape and set numbers that fit your account size and your temperament.

## The rules this setup runs on

1. **Cash account only.** No margin, no borrowed money, ever.
2. **Liquid stocks and broad ETFs only.** Things that trade heavily and can be exited easily. No penny stocks, no thin names, no options, no crypto in this system. Boring is a requirement, not a limitation.
3. **About $125 maximum per position.** Position size is capped in dollars, so one idea can only ever be worth a small, known amount of the account.
4. **Maximum 3 positions at once.** Few positions means every position gets watched, and a bad week cannot hide inside a crowd.
5. **An exit goes in with every entry.** Every buy carries a protective stop roughly 6% below the entry price, placed at the same time. A position without an exit is not a trade in this system; it is a hope, and hopes are not allowed.
6. **A 15% account drawdown halts all trading.** If the account falls 15% from its high-water mark, the agent stops — no new entries, full stop — until I review what happened and restart it manually. The halt is the system admitting it might be wrong.
7. **Maximum 3 trades per week.** A frequency cap kills overtrading, which is where small accounts go to die.

8. **Every fill is reported and reviewed.** The agent reports each execution — what, when, at what price — and I review fills against the rules. An unreported trade is a broken system, even if it made money.

## Why each rule earns its place

Notice what the rules collectively do: they make the worst case boring. Cash-only plus a $125 cap plus a stop means a single position going wrong costs a few dollars. Three positions maximum means all three going wrong at once costs a few more. The drawdown halt means a genuinely bad stretch stops the machine instead of compounding. The weekly trade cap means the system cannot churn your account into fees and noise. None of these rules make you money. All of them keep you in the game long enough for discipline to matter.

## Approvals on or off — an honest account

I run with trade approvals **off**: the agent executes within the rules without waiting for my tap. I want to be plain with you about why that is acceptable in this specific setup and when it would not be:

- The account is small and cash-only, so the maximum possible harm is capped by the account itself.
- Every rule above was written and tested before delegation, and every fill is reported to me.
- The drawdown halt and the kill switch (Chapter 7) mean I can end the experiment in one action.

If any of those three things is not true for you — bigger account, unwritten rules, no reporting habit — **leave approvals on.** Approvals on is not a lesser mode; it is the right mode for most people, indefinitely. The agent still does the monitoring, the math, the scheduling, and the paperwork. You keep the final tap.

## Worksheet: write your rules

Fill this in before enabling any order tool. If a line is blank, you are not ready.

- My tradable account is the dedicated Agentic account: ☐ verified in Chapter 3

- Account type: ☐ cash (margin: not used in this system)
- Amount funded: $_____ (an amount I can afford to lose entirely)
- Allowed instruments: ☐ liquid stocks ☐ broad ETFs (nothing else)
- Maximum per position: $_____
- Maximum positions at once: _____
- Protective stop on every entry: _____% below entry
- Account drawdown halt: _____% from high-water mark → all trading stops
- Maximum trades per week: _____
- Trade approvals: ☐ ON (agent proposes, I tap) ☐ OFF (only with rules + reporting in place)
- Fill reports go to me: ☐ after every fill ☐ daily summary
- My kill switch is: _____ (write the exact steps)

Sign it, date it, and keep it where you will actually reread it. When you are tempted to loosen a rule mid-drawdown — the exact moment rules matter most — the document is what you argue with, not your mood.

---

# Chapter 5: Order Mechanics

Rules say what the agent may do. Mechanics are how orders actually behave, and a few of these behaviors surprise people. Learn them here rather than with your money.

## Limit orders vs. market orders

A **market order** says "buy now, at whatever the current price is." A **limit order** says "buy at this price or better — and if the price never gets there, do not buy." This system uses limit orders for entries. The reasons are practical: a limit order cannot chase a spike, cannot pay a silly price in a fast open, and expresses your plan as a number instead of a mood.

The tradeoff is real and you must accept it upfront: **a limit order can sit unfilled.** The price may never touch your limit, and the trade simply does not happen. That is not the system failing. That is the system declining a trade at the wrong price. Patience is a feature; several of my own planned entries never filled, and the correct response was to let them go, not to raise the limit in a hurry.

## Protective stops — and their real limit

Every entry in this system is paired with a protective stop order roughly 6% below the entry price, set to remain in place (a good-til-cancelled style resting order) so the exit exists even when nobody is watching. If the position trades down to the stop during the session, it sells.

Now the limitation, stated as plainly as it deserves: **protective stops execute during regular market hours.** Overnight and pre-market moves do not trigger them. A position can gap down overnight and open well below your stop; the stop will then execute at the open, at the available price — which is worse than the stop price. A stop is a seatbelt, not a force field. This is one more reason position sizes stay small and the account stays a learning size.

## The 24 Hour Market window

Robinhood's 24 Hour Market lets eligible stocks and ETFs trade outside regular hours, and in this setup entries can be placed as **limit orders — whole shares only — during that extended window.** This is where the "while you sleep" phrase honestly comes from: a plan written in the evening can be working overnight instead of waiting for you to be free at the open.

Use the window with both eyes open:

- **Limit orders only.** In thin overnight trading, a market order is an invitation to a bad fill. The limit is your protection.
- **Whole shares.** No fractional orders in this window — size your entries accordingly (another reason the dollar caps in Chapter 4 are modest).
- **Liquidity is thinner.** Prices overnight can be jumpier and spreads wider. A limit that looks close at 11 p.m. may be far away by morning. Unfilled overnight orders are normal; let them expire rather than chasing.
- **Stops still keep regular hours.** Your exit protection does not extend into the night even though your entries can. Never let the 24-hour entry window talk you into a position size that assumed round-the-clock protection.

## Order hygiene

- One plan, one order. If an entry order is resting, do not stack a second one "just in case."
- When a fill comes in, confirm the paired stop exists. Every time. No exceptions because the app "probably did it."
- Review resting orders weekly and cancel stale ones deliberately, in your review — not impulsively, mid-week.

---

# Chapter 6: The Monitoring Rhythm

An automated system you never look at is not automated; it is abandoned. The rhythm below is the minimum attention this setup needs, and it is designed to be small enough that you will actually keep it.

## Scheduled position checks

Have the agent check the account on a schedule — in my setup, these run without me asking each time. Each check covers:

- Current positions and their prices versus entry
- Confirmation that every position still has its protective stop in place
- Account value versus the high-water mark (drawdown check against the 15% halt)
- Any fills since the last check
- Any resting orders, and their age

If the drawdown line is crossed, the check's job is to report the halt, not to negotiate with it.

## Fill reports

Every fill gets reported: instrument, side, quantity, price, time. Not a weekly bundle — a report per fill, while it is still news. Your job on receiving one is a ten-second audit: Is this inside my rules? Size right? Stop attached? If the answer to any of those is no, that is a system problem to fix before the next trade, not a shrug.

## The weekly review

Once a week — mine takes about fifteen minutes — sit down with the week's record:

1. List every trade. Check each against the written rules.
2. Check the drawdown number and how close the account is to the halt.
3. Look at resting orders and stops. Cancel or adjust deliberately, in the review, on the record.
4. Write one sentence about what the system did and one about what you will change — or "nothing." The sentence matters more than the analysis; it proves a human is steering.

## What the agent reports, and what you decide

Keep this division clean forever: the agent monitors, calculates, reports, and executes the written rules. **You** change the rules, change the funding, restart after a halt, and decide whether the experiment continues. The moment those lines blur — the agent suggesting its own rule changes and applying them — you no longer have a system. You have a stranger with your password.

---

# Chapter 7: Failure Modes and the Kill Switch

Systems fail. The question is whether they fail small, loudly, and under your control. These are the failure modes I have either lived or planned for.

## The connection token expires

Real one, from my own run: the agent's connection to Robinhood stopped working because the authorization token expired, and the fix was to reconnect — run the OAuth flow again and re-verify the account list afterward (Chapter 3, quickly). Nothing traded during the outage, which is the correct failure direction: when in doubt, this system does nothing. Expect to reconnect occasionally. After any reconnect, re-confirm which account is tradable before anything else.

## Dust positions

Small accounts breed dust: tiny leftover amounts — a fraction of a share from a partial fill, a position worth a couple of dollars that is too small to fit the rules but still sitting there. Dust is not dangerous, but it is noise, and noise hides signal in a three-position system. Sweep it occasionally, during a weekly review, on purpose: sell or consolidate the leftovers so the account you see is the account you actually run.

## The unfilled order that tempts you

Covered in Chapter 5, repeated here because it is the most common emotional failure: a limit order sits, the price runs away, and you feel the trade "got away." It did not get away. It was never yours at your price. The system's answer is to let it expire and re-plan at the next review. Chasing is how rule-based accounts become mood-based accounts.

## The drawdown halt triggers

This is the system working, not failing. When the halt triggers: no new entries, existing stops stay in place, and the agent reports. Your job is a real review — were the rules followed? Was the loss normal variance inside small positions, or is something actually wrong (a broken stop, a rule quietly not applied, an instrument that does not belong)? Restart only after that review, in writing, even if the writing is one line: "Rules were followed; losses within design; restarting."

## The kill switch

You must be able to stop everything, fast, without the agent's cooperation. Know these before the first trade:

1. **Turn trade approvals on** in Robinhood — instantly, every proposed order now needs your tap, and you simply stop tapping.
2. **Revoke the agent's connection** — disconnect the OAuth authorization so the agent cannot reach the account at all.
3. **Cancel resting orders** you do not want live, and decide on open positions deliberately: stops in place means you can walk away and let the exits work; closing positions yourself is also fine. The point is that it is your decision, made calmly.

Write your exact kill-switch steps in the Chapter 4 worksheet. A kill switch you have to figure out during a problem is not a kill switch.

## The failure you must not automate away

The last failure mode is you: loosening rules after a loss ("the stop was too tight"), enlarging positions after a win ("the system works, let's go bigger"), or quietly disabling the halt. The written rules and the weekly sentence exist to catch this. If you find yourself arguing with your own worksheet, the worksheet wins. That was the deal you made with yourself when you were calm.

---

# Closing Checklist

Before the agent places its first order, every box below should be checked.

**Setup** - ☐ I have read the risk disclaimer and I am funding this with money I can afford to lose. - ☐ The dedicated Agentic account is the only account the agent can trade — verified by reading the account list. - ☐ The account is cash-only. Margin is off and stays off. - ☐ The account is funded small, at learning size.

**Connection** - ☐ OAuth connection completed on desktop. - ☐ Read-only verification done: accounts, portfolio, and positions read back against the Robinhood app. - ☐ Trade-approval setting checked and recorded. - ☐ Order tools stayed disabled until my rules were written.

**Rules** - ☐ My rules are written and signed: instruments, $ cap per position, max positions, stop %, drawdown halt %, max trades per week. - ☐ Approvals on/off chosen deliberately, for a reason I can say out loud. - ☐ Every entry will carry its protective stop at placement. - ☐ Fill reporting is set up, and I know what a fill report should contain.

**Operations** - ☐ Scheduled position checks are running. - ☐ My weekly review is on my calendar, and I know its four steps. - ☐ I understand: limit orders can go unfilled; stops execute in regular hours only; overnight entries are limit-only, whole shares. - ☐ My kill-switch steps are written in the worksheet, and I could execute them today.

If every box is checked, you do not have a money machine. You have something better and much rarer: a small, honest system that follows your rules while you sleep, reports

what it did, and stops when you tell it to. Run it small, run it long, and let the boring discipline do whatever compounding is going to get done.

— Oris