FINANCE · AP AUTOMATION · STATUS FOR BRIAN

Automate AP

Where the project stands, what's done, and what's left to hit the 80% automation goal.

Project Automate AP (Finance board) **Lead** Camille, with Will on merch & controls **Updated** June 20, 2026

TL;DR

- The foundation is built and battle-tested: invoices auto-route from inbox to tracked cards, and all **9 of 9 fraud red-team tests pass**. A real phishing attempt on June 4 was caught and nobody clicked it.
- **Payment stays a manual human click in Chase, by design.** That's the fraud firewall, not a missing feature. The bot never moves money.
- Live today: vendor notifications, draft-only reply emails, and a daily report of every invoice's path plus the on-time-payment rate.
- To reach 80%, three things remain: run it **unattended** (off Camille's laptop), add **PDF + Salesforce auto-matching**, and finish **buying-team rollout** + lock an SLA scoreboard.
- The original May 29 target was met for intake + security. The deeper automation (Phase 2) was deliberately gated on security and is now unblocked.

9/9 Fraud red-team tests passing	**6** Main milestones done
4 Milestones remaining	**Manual** Payment rail, by design

01 The objective

What success looks like for this project.

Automate **80% of the accounts payable process**. The number-one priority: pay every vendor **on time by the due date**, and notify the team and the vendor when a payment is made.

Two ground rules were set at kickoff and still hold:

- **Rules first, AI second**
  Anything that doesn't exactly match approved conditions fails safely and goes to manual review. No guessing.
- **Security is a primary focus, not an afterthought**
  The bot handles intake, screening, tracking, and notifications. A human always presses Send on the actual payment.

02 Main milestones

The real building blocks toward 80%, minor admin steps left out.

DONE Built, tested, and live today.

- ✓ **Invoice intake is live**
  Vendor invoices from the accounting inboxes auto-route into tracked Basecamp cards, with a 40+ vendor whitelist and routing by vendor type.
- ✓ **Security hardened — 9 of 9 red-team tests passing**
  Nine fraud controls are live in code: lookalike-domain detection, hidden-text / prompt-injection stripping, bank-change kill-switch, authorized-approver checks, submitter-is-not-approver, new-payee gate + amount caps, bank-baseline mismatch, a tamper-evident audit log, and sender-identity checking (added after a real phishing email on June 4). Flagged mail goes to a quarantine lane.
- ✓ **Draft-only vendor replies**
  The bot drafts the vendor email on the right thread; a person clicks Send. Nothing goes out automatically.

Notifications when a bill is paid

The person who submitted the invoice is automatically notified the moment it's marked paid, so no one has to chase status.

Payment history + metrics report

A daily report shows each invoice's full path (requested → approved by whom → paid date), the on-time-payment rate, a by-brand breakdown, and any late-payment callouts.

QuickBooks integration set up for Camille

Accounting-system connection in place for the bookkeeping side.

REMAINING What's left to cross the 80% line.

1. **Run it unattended**

   Move the tool off Camille's laptop onto a scheduled service after a few weeks of audit-log data. Today it only runs when her machine is open. This is the biggest gap between "built" and "fully automated."

2. **Deeper auto-matching (Phase 2)**

   Read the invoice amount and bank details straight from PDF attachments (today an amount can show as "to be determined" until the buying-team sheet catches up), and add a Salesforce 3-way match — invoice vs. purchase order vs. goods received — for merch vendors before payment, with freight and duty handled as their own line per Will.

3. **Buying-team rollout**

   Present to and onboard the buying team (Maryanne and Alex from Merch) so their invoices flow through the same pipeline. This is Anthony's step.

4. **Lock the scoreboard**

   Set the SLA target (average days to pay after approval) and the exact definition of "on time" so there's one agreed metric everyone watches. The reporting mechanism already exists; the target and the "what counts as 80%" definition still need to be set.

Note: none of the remaining work adds payment risk. It extends an already-secured pipeline. Money movement stays a manual human action throughout.

03 Summary takeaway

WHAT IT TAKES TO FINISH

The hard part is done. **Intake and fraud defense are live and proven** — 9 of 9 red-team tests pass and a real phishing attempt was blocked — and **payment stays a deliberate human click** so the system can never be tricked into moving money.

To cross the 80% line, the work left is **operational, not foundational**: get it running unattended off Camille's laptop, add PDF + Salesforce auto-matching so amounts and POs verify themselves instead of going to manual, finish the buying-team rollout, and lock an SLA scoreboard so "on time" is actually measured.

Each of these extends what's already secured. **No new risk, just more reach.**