

Stabilize Before You Scale

...

Alec Zaslav · Product Take-Home · May 2026

What I Was Handed

The Situation

Two AI products

- An Agentic Telecom Platform replacing human agents for outbound calls, SMS and email
- An AI Compliance System reviewing every collections interaction for a banking context

Four enterprise clients deploying at once

- Agentic Telecom Platform for Clients 1, 2 and 3.
- AI Compliance System for Clients 2 and 4. Client 2 is the biggest.

The Minutia

Engineering says requirements are unclear.

Sales promised full automation.

The CTO says it is not production ready.

Client 4 says it is still manual-heavy.

Usage up, complaints up, conversions down.

The Rules

Seven days to complete. 15 slides maximum. No clarifying questions. Every assumption stated. Every decision defended live.

What I was asked, and where it is answered

What is actually broken	4
Strategy for both products	5 to 7
PRD and jobs to be done	8
Technical requirements	8
System diagram	9
Three-month roadmap with trade-offs	10
Midway twist and the updated plan	11
Managing four clients	12
Crisis email to an unhappy client	13
Collaboration model	14
Metrics	15
Execution structure	16

Who We're Building For

Operations Manager

Drives daily collections performance

Needs the agent closing accounts, not just touching them

Owns recovery targets and feels it when conversions don't move

Lives in the gap between what the system does and what it delivers

Compliance Officer

Owns legal and regulatory risk

Needs every outbound interaction to be audit-ready and defensible

Relies on the Compliance System being bulletproof

An FDCPA violation isn't a slowdown, it's legal exposure

Executive Sponsor

Signs the checks, owns the outcomes

Needs ROI to show up in recovery numbers, not just activity metrics

The business case lives or dies on both products working together

Quietly deciding whether this bet was worth making

Every decision in this deck is made with all three in the room.

What's Actually Broken

*Operations
Manager*



No one ever defined what the agent needed to do.
The agent makes contact but fails at the close.

*Compliance
Officer*



Each client has different requirements, but the system isn't configured yet to enforce them consistently. Manual gaps remain.

*Executive
Sponsor*



Sales sold a finished product. Engineering shipped a starting point. The gap is still unowned.

Usage is up. Conversions are down. The product is active but not delivering.

Prioritize Compliance, Then Telecom

This isn't a choice between two products, it's a sequencing decision.

Here's why the order matters:

The Compliance System comes first

The Agentic Telecom Platform cannot operate legally or effectively without it. Every outbound interaction must be FDCPA compliant. An unstable compliance layer doesn't slow it down, it makes it a legal liability.

The Agentic Telecom Platform is the priority product

Deployed at three of four clients with the broadest exposure. Usage is climbing but conversions aren't following. Once compliance is stable, this is where we accelerate.

Slow on the surface, stable underneath. That's the trade-off.

Agentic Telecom Platform Strategy

The promise was full automation. The reality is a system that contacts but doesn't close. The strategy is closing that gap by making the agent work consistently and showing clients the work.

Three strategic pillars:

Reliability over Features

Stop adding capability until what exists works consistently. Clients need to trust the agent is working, not just running.

Compliance as a Feature

Build compliance signals into the agent's output. Interactions show clients what's checked. Show them the work.

Visibility before Velocity

Instrument before optimizing. Clients see call summaries and decision logs. Observability is the path to autonomy.

Trust is earned in transparency, not capability.

AI Compliance System Strategy

The system is built to review compliance proactively. The reality is gaps still exist and clients are feeling them. The strategy is closing those gaps before they become violations.

Three strategic pillars:

Configuration First

Each client has distinct requirements. Enforce different rules per client without a custom build each time. Configuration scales. Custom builds don't.

Block before Flag

Stop violations before they happen, not after. The system blocks contact attempts that exceed regulatory limits in real time. Prevention beats review.

Audit Trail as Artifact

Every interaction generates a record the Compliance Officer can defend to a regulator. The audit trail isn't a byproduct of the system.

The audit trail is the product.

From Strategy to Spec

Each follows the same handoff: written, reviewed with engineering, translated into tracked tickets.

Agentic Telecom Platform

JTBD: Recover debt without human intervention

Outbound contact across SMS, email, and calls
when account goes delinquent

Authentication and negotiation handled end to end
without agent involvement

Seamless handoff to human agent when escalation
threshold is met

AI Compliance System

JTBD: Every interaction is defensible before it goes out

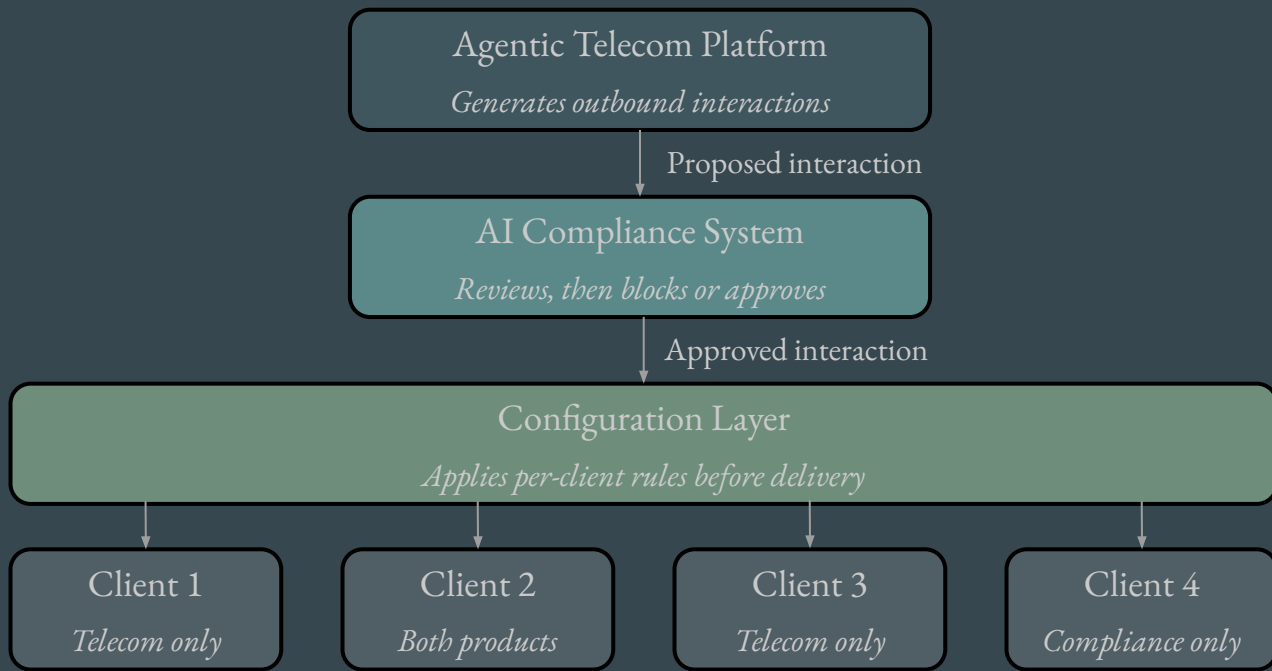
Flag interactions violating client-specific rules before
sending out to end users

Auto-generate audit trail for every interaction across
every channel

Block contact attempts exceeding regulatory limits by
client, location, or asset type

Requirements don't lie. Vague ones do.

How It All Holds Together



One platform. Four configurations. No custom builds.

The 90-Day Plan

Month 1

Stabilize

Lock compliance configuration per client before anything else moves

Close manual gaps in the Compliance System

No new feature development until foundation is solid, conversions may remain flat in the meantime

Month 2

Validate

Activate the ATP against the stable compliance foundation

Roll out client by client starting with lowest risk, slower than parallel, less to recover if something breaks

Track conversion metrics closely against pre-rollout baseline

Month 3

Accelerate

Address Client 4's manual-heavy experience directly

Expand AI Agent scope where Month 2 data confirms readiness

Reassess roadmap against validation results, prioritize next features from evidence

Trading short-term velocity for long-term stability. That's the right call.

The Plan Meets Reality

*Engineering
capacity drops*



Protect Month 1 entirely. Delay Month 2 validation by a couple weeks. Reduce Month 3 scope. Sequencing holds, timeline stretches.

*Client 2
expands scope*



Acknowledge formally, scope it together, defer to Month 3 or beyond. Client 2's expansion gets a dedicated planning conversation, not a queue slot. The sequencing holds, even for our biggest client.

*Competitor
launches*



What's broken internally doesn't change. What changes is client patience. Stay focused on stabilization, accelerate communication, and let execution be the differentiator.

The plan changes. The priorities don't.

Every Client, Accounted For

Supporting artifacts:

- Status tracker

- Weekly digest

- Escalation log

All four tracked in a living document, updated weekly. Red triggers leadership review.

Tier 1: Strategic

Client 2

Weekly check-ins across both products, highest internal visibility

Scope changes require formal review before entering roadmap

Dedicated point of contact for escalations at all times

Tier 2: Standard

Clients 1 and 3

Biweekly check-ins, single product deployment, lower risk profile

Updates shared async unless an escalation threshold is crossed

Milestone progress tracked and reported on shared cadence

Tier 3: Active Recovery

Client 4

Dedicated recovery cadence with direct communication

Progress tracked weekly against compliance milestones

Exit when manual gaps close and status stays green for two weeks

Different clients. Different needs. One system to manage them all.

Responding to the Crisis

Hey [Client POC Name],

Thank you for being direct. You're right. The experience you're having today is not what I committed to, and I take ownership of that gap.

I'm mapping the manual dependencies in your current setup and prioritizing closing them on the active roadmap. You'll see meaningful progress within a couple weeks. I'll be your direct point of contact throughout, with weekly updates on exactly where things stand.

I'd like to connect this week to walk you through the plan in detail. I have availability Tuesday and Wednesday afternoon, let me know which works better for you, or if another time this week is easier.

I'm committed to getting this right for you.

Best,

Alec Zaslav

Own it. Fix it. Don't hide behind process.

The Operating System

- Channels* → PM reviews all outbound before it goes out
Internally: #product-agent, #product-compliance, #engineering
Client comms in dedicated external threads, completely separate
- Rituals* → Weekly standup, biweekly retro, monthly roadmap review. Internal standup feeds client updates same day. Short, structured, decisions documented by EOD.
- Escalation* → PM owns below red threshold. Engineering lead for technical blockers. Leadership when a client relationship or milestone is at risk, same criteria as the client tracker.

Clear channels. Clear ownership. Everyone knows the plan.

What Gets Measured

Operations Manager

Recovery performance

North Star: conversion rate above pre-deployment baseline

Conversion rate

Contact-to-conversation rate

Appropriate escalation rate

Compliance Officer

Compliance health

North Star: zero FDCPA violations

FDCPA violation rate

Audit trail completion rate

Pre-send block rate by client

Executive Sponsor

Business outcomes

North Star: cost per recovered account trending down

Overall recovery volume

Cost per recovered account

Time to first conversion per client

If it's not measured, it's not managed.

How The Work Gets Done

One Jira board per product. Epics map to roadmap phases. Every ticket tagged to a client.

Epics

One per product per month.

Aligned directly to roadmap phases: Stabilize, Validate, Accelerate.

Stories

One per client-feature combination.

Four client tags (C1, C2, C3, C4) plus two product tags (ATP, ACS)

Tasks

Individual engineering tickets, QA items, and client configuration work.

Compliance label required on any ticket touching the Compliance System

If it's not in Jira, it doesn't exist.