CRM End-to-End Audit Report

Remotive Logistics SalesHub
Audit Date: January 9, 2026
Auditor: Claude Code
Scope: Batches 1-3 + Reply Portal

Executive Summary

Section	Status	Critical Issues
1. Permissions & Visibility	**PASS**	Minor: 403/404 inconsistency
2. Assignment Rules	**PARTIAL**	Bulk reassign missing proper logging
3. Time Fields	**PARTIAL**	`responseTime` field never populated
4. CRM Settings Enforcement	**FAIL**	Settings stored but NOT enforced
5. Filters & Saved Views	**PASS**	Fully functional
6. CustomerInterest	**PARTIAL**	No permission checks on API
7. Reply Portal & Messages	**PASS**	Minor: No rate limiting
8. Audit Log & Settings Page	**PARTIAL**	High-risk actions not logged

Total Estimated Fix Effort: 13.25 hours

1. Permissions & Visibility

Status: PASS (with minor issue)

Check	Status	Location
Salesperson sees only `assignedToId = self`	PASS	`app/api/crm/customers/route.ts:204-220`
Manager sees team customers only	PASS	OR clause: assignedToId IN team OR managerId = self
Owner/Director/CRM Admin sees all	PASS	No filter applied
Returns 404 for unauthorized customer detail	PASS	`app/api/crm/customers/[id]/route.ts:300-327`
Thread visibility respects permissions	PASS	`app/api/crm/threads/route.ts:38-51`

Implementation Details

Customer List Endpoint (`/api/crm/customers` GET):

- Salesperson: `where.assignedToId = currentUser.id`
- Manager: `OR [{ assignedToId IN teamMemberIds }, { managerId = currentUser.id }]`
- Owner/Director/CRM Admin: No filter (sees all)

Customer Detail Endpoint (`/api/crm/customers/[id]` GET):

- Returns 404 if unauthorized (security-through-obscurity)
- Same role-based logic as list endpoint

Thread Endpoints (`/api/crm/threads`):

- Returns 403 for unauthorized (inconsistent with customer endpoints)

Minor Issue

Thread endpoints return 403 while customer endpoints return 404 for unauthorized access. Recommend standardizing to 404 for security-through-obscurity.

Fix Effort: 30 minutes

2. Assignment Rules (Batch 1)

Status: PARTIAL

Check	Status	Location
repCode → assign rep + manager	PASS	`route.ts:420-445`

repCode → method="repCode"	PASS	`assignmentMethod: "repCode"` set
No repCode → canAdminCRM intake	PASS	`route.ts:447-460`
No repCode → method="intake"	PASS	`assignmentMethod: "intake"` set
Owner/Director can reassign any	PASS	No restrictions
Manager team-only reassign	PASS	`route.ts:67-79`
Salesperson blocked from reassign	PASS	Returns 403
Assignment history via `assignment_change` activity	PASS	`route.ts:187-242`

Auto-Assignment Flow

With RepCode:

1. Look up UserProfile by repCode
2. Assign `assignedToId = rep.userId`
3. Assign `salesRepName = rep's name`
4. Assign `managerId = rep.managerId` (auto-inherit)
5. Set `assignmentMethod = "repCode"`

Without RepCode (Intake):

1. Find first active CRM Admin (`canAdminCRM=true`, `isActive=true`)
2. Order by `createdAt ASC` (oldest first - deterministic)
3. Assign to CRM Admin
4. Set `assignmentMethod = "intake"`

Assignment History Logging

Single customer reassignment creates `assignment_change` activity with rich JSON:

```
{
  "fromAssignedToId": "old-user-id",
  "toAssignedToId": "new-user-id",
  "fromAssignedToName": "Old Rep Name",
  "toAssignedToName": "New Rep Name",
  "fromManagerId": "old-manager-id",
  "toManagerId": "new-manager-id",
  "changedBy": "user@email.com",
  "changedByRole": "manager",
  "reason": "reassignReason from request body",
  "method": "manual"
}
```

Gaps Found

Issue	File	Effort
Bulk reassign creates `type: "note"` instead of `assignment_change`	`bulk-actions/reassign/route.ts:72-86`	1 hour
Bulk reassign doesn't set `assignmentMethod: "bulk_reassign"`	Same file	15 min
Bulk reassign doesn't update `managerId`	Same file	30 min

Total Fix Effort: 1.75 hours

---

3. Time Fields Accuracy

Status: PARTIAL

Field	Status	Details
`createdAt`	PASS	Prisma `@default(now())` - always correct
`lastContactedAt`	PASS	Starts null, updates on contact activity
`lastActivityAt`	PASS	Updates on all activity types
`responseTime`	**FAIL**	**Never populated in database**

lastContactedAt Update Triggers

1. **Activity creation** (call, email, meeting): `activities/route.ts:97-102`
2. **Quick email action**: `quick-actions/email/route.ts:74-80`
3. **Quick SMS action**: `quick-actions/sms/route.ts:90-96`
4. **Message thread reply**: `threads/[id]/route.ts:275-280`

Critical Gap: responseTime Never Calculated

Schema Definition: `responseTime Int? // Minutes from lead creation to first contact`

Problem: This field is NEVER written to. Zero database writes across entire codebase.

Impact: Dashboard aggregation returns null for `avgResponseTime`.

Required Fix

Add to all `lastContactedAt` update locations:

```
if (!existingCustomer.lastContactedAt) {
  const responseMinutes = Math.floor(
    (new Date().getTime() - existingCustomer.createdAt.getTime()) / 60000
  );
  data.responseTime = Math.max(0, responseMinutes);
}
```

Files to Update:

- `app/api/crm/activities/route.ts:97-102`
- `app/api/crm/quick-actions/email/route.ts:74-80`
- `app/api/crm/quick-actions/sms/route.ts:90-96`
- `app/api/crm/threads/[id]/route.ts:275-280`

Fix Effort: 2 hours

---

4. CRM Settings Enforcement (Phase 2)

Status: FAIL

Settings are STORED in database but NEVER ENFORCED at any API endpoint.

Setting	Stored	Enforced	Expected Behavior
`require_rep_for_contacted`	YES	**NO**	Block status→contacted if no rep
`require_rep_for_qualified`	YES	**NO**	Block status→qualified if no rep
`require_lost_reason`	YES	**NO**	Require lostReason when status→dead
`required_for_qualified`	YES	**NO**	Validate required fields
`required_for_applied`	YES	**NO**	Validate required fields
`required_for_won`	YES	**NO**	Validate required fields
`lock_reassignment`	YES	**NO**	Hardcoded in crm-permissions.ts
`steal_protection`	YES	**NO**	Not checked anywhere

Settings Infrastructure

Database Model: `CRMSetting` with key/value pairs, categories, audit fields

API Endpoints:

- GET `/api/crm/settings` - Fetches all settings, seeds defaults
- PATCH `/api/crm/settings` - Updates settings, creates audit log

UI: Full settings page with tabs for Assignment, SLA, Required Fields, Import

The Problem

The settings system is a UI-only configuration store. No API endpoint reads these settings to enforce business rules.

Example of what should happen:

```
// In /api/crm/customers/[id]/status route
const settings = await getCRMSettings();
if (settings.require_rep_for_contacted && !customer.assignedToId && status === "contacted") {
  return NextResponse.json({ error: "Cannot mark as contacted without assigned rep" }, { status: 400 });
}
```

Required Fixes

Fix	File	Effort
Create settings helper to fetch/check settings	New: `lib/crm-settings-enforcement.ts`	2 hours
Add require_rep checks to status change	`customers/[id]/status/route.ts`	1 hour
Add require_lost_reason enforcement	Same file	30 min
Add required_for_* field validation	Same file	1.5 hours
Wire lock_reassignment to permission system	`lib/crm-permissions.ts`	1 hour

Total Fix Effort: 6 hours

---

5. Filters & Saved Views (Batch 2)

Status: PASS

Check	Status	Details
Advanced filters AND logic	PASS	All filters combined with Prisma implicit AND
URL persistence	PASS	`filtersToSearchParams()` function
Saved views per user	PASS	`userId` field + `isGlobal` flag
Default view auto-load	PASS	From user preferences
Unassigned toggle	PASS	`where.assignedToId = null`
Never contacted toggle	PASS	`where.lastContactedAt = null`
Overdue follow-up toggle	PASS	`where.nextFollowUpDate = { lt: new Date() }`

Filter Categories

- **People & Assignment:** assignedToId, managerId, unassignedOnly
- **Status/Temperature/Priority:** Multi-select with `{ in: array }` syntax
- **Financing:** financingType, rtoApprovalStatus, financeApprovalStatus
- **Location:** state, city, zipcode
- **Trailer:** trailerType, trailerSize, vin, stockNumber
- **Time:** createdAfter/Before, lastContactedAfter/Before
- **Quick Toggles:** unassignedOnly, neverContacted, followUpOverdue

Saved Views System

- Personal views: `userId = currentUser.id`
- Global views: `isGlobal = true` (Owner/Director only)
- Default view: `isDefault = true` per user
- Auto-load from user preferences on page mount

No Fixes Required

---

6. CustomerInterest

Status: PARTIAL

Check	Status	Details
Multiple customers per stock/VIN	PASS	No unique constraint, by design
UI creates/reads correctly	PASS	`interested-units.tsx` component
Duplicate prevention	PASS	API checks before create
Visibility respects permissions	**FAIL**	**No permission checks in API**

Critical Security Gap

The `/api/crm/interests` endpoint has NO role-based access control.

Current Implementation:

```
export async function GET(req: NextRequest) {
  const session = await getServerSession(authOptions);
  if (!session?.user?.email) {
    return NextResponse.json({ error: "Unauthorized" }, { status: 401 });
  }
  // NO role checks, NO team membership validation
  // Anyone authenticated can view ANY customer's interests
}
```

What Could Go Wrong:

1. Salesperson A can fetch interests for Salesperson B's customers
2. Team privacy breach across managers
3. Competitive intelligence leak between reps

Required Fix

Add same permission checks as customer detail endpoint to all interest endpoints (GET, POST, DELETE).

Fix Effort: 1.5 hours

---

7. Reply Portal & Messages Inbox

Status: PASS (with minor issues)

Check	Status	Details
Email creates/links thread	PASS	`api/crm/email/route.ts`
Thread logs outbound message	PASS	`direction: "OUTBOUND", channel: "EMAIL"`
Email includes reply portal button	PASS	`replyLink = /reply/${thread.portalToken}`
Customer reply creates inbound message	PASS	`api/reply-portal/[token]/route.ts`
Reply notifies rep	PASS	`notifyCustomerReply()` function
Reply notifies manager	PASS	If managerId exists
Unread tracking in inbox	PASS	`unreadForRep`, `unreadForManager` flags
Thread visibility respects permissions	PASS	Same as customer visibility

Email Sending Flow

1. Authenticated POST to `/api/crm/email`
2. Create/find MessageThread for customer
3. Create Message with `direction: "OUTBOUND", channel: "EMAIL"`
4. Update thread `lastMessageAt`, `lastMessagePreview`
5. Send via Resend with reply portal link
6. Return threadId, replyLink

Customer Reply Flow

1. Customer visits `/reply/[token]`
2. Validate token exists and not expired
3. POST creates Message with `direction: "INBOUND", channel: "PORTAL"`
4. Update thread: `unreadForRep: true`, `unreadForManager: true`
5. Update customer: `lastContactedAt`, `lastActivityAt`
6. Create activity log
7. Notify rep and manager via in-app notifications

Unread Tracking

- `MessageThread.unreadForRep` - Boolean flag for rep's inbox
- `MessageThread.unreadForManager` - Boolean flag for manager oversight
- `Message.readByRepAt` - Timestamp when rep read message
- `Message.readByManagerAt` - Timestamp when manager read message
- Auto-mark as read when viewing thread detail

Minor Issues

Issue	File	Effort
No rate limiting on portal replies	`api/reply-portal/[token]/route.ts`	30 min
Email logged before Resend confirmation	`api/crm/email/route.ts`	1 hour

Total Fix Effort: 1.5 hours

8. Audit Log & CRM Settings Page

Status: PARTIAL

Check	Status	Details
Settings page: Owner can edit	PASS	`canEdit: true`
Settings page: CRM Admin can edit	PASS	`canAdminCRM` check
Settings page: Director view-only	PASS	`canView: true, canEdit: false`
Audit log records settings changes	PASS	`settings/route.ts:265-278`
Audit log filters work	PASS	Date range, action, entity type, entity ID
Audit log CSV export works	PASS	Up to 10k records
Audit log records high-risk actions	**FAIL**	Many actions NOT logged

Settings Page Permissions

```
// From lib/crm-permissions.ts
export function canAccessCRMSettings(context): { canView: boolean; canEdit: boolean } {
  if (context.role === "owner") return { canView: true, canEdit: true };
  if (context.canAdminCRM) return { canView: true, canEdit: true };
  if (context.role === "director") return { canView: true, canEdit: false };
  return { canView: false, canEdit: false };
}
```

Audit Log Features

- **Filters:** Action type, Entity type, Entity ID, Date range
- **Export:** CSV with up to 10k records
- **UI:** Color-coded badges, icons, JSON diff viewer
- **Indexes:** Optimized for entityType, userId, action, createdAt

What IS Being Logged

1. **CRM Settings Changes** - key, old value, new value, IP, user agent
2. **Audit Log Exports** - count exported, filters applied

What is NOT Being Logged (Gaps)

Action	File	Effort
Customer status changes	`customers/[id]/status/route.ts`	45 min
Customer assignment/reassignment	`bulk-actions/reassign/route.ts`	45 min
User role changes	`admin/users/route.ts`	1 hour
User permission changes	Same file	30 min
Account bans/timeouts	Same file	30 min
Customer deletion	`bulk-actions/delete/route.ts`	30 min

Total Fix Effort: 4 hours

Priority Fix Order

P0 - Critical Security (Do Immediately)

Fix	Impact	Effort
Add permission checks to CustomerInterest API	Prevents data leak between reps	1.5 hours

P1 - High Priority (This Week)

Fix	Impact	Effort
Wire CRM Settings enforcement to status change endpoint	Enables business rule enforcement	3 hours
Add require_rep checks	Ensures rep assignment before progression	Included above
Add require_lost_reason enforcement	Ensures data quality	30 min
Add audit logging to user management	Tracks high-risk admin actions	2 hours

Fix `responseTime` calculation	Enables response time reporting	2 hours

P2 - Medium Priority (This Sprint)

Fix	Impact	Effort
Fix bulk reassign logging	Proper audit trail for bulk ops	2 hours
Add audit logging to customer status changes	Tracks pipeline changes	45 min
Add rate limiting to reply portal	Prevents spam	30 min

P3 - Low Priority (Backlog)

Fix	Impact	Effort
Standardize 403/404 responses	Consistent security model	30 min
Add email send confirmation tracking	Better delivery tracking	1 hour

Total Estimated Effort

Priority	Hours
P0 - Critical	1.5
P1 - High	7.5
P2 - Medium	3.25
P3 - Low	1.5
Total	**13.75 hours**

Quick Wins (Safety Improvements)

Fix	Impact	Effort
Standardize all unauthorized responses to 404	Security consistency	30 min
Add permission checks to `/api/crm/interests`	**Critical security fix**	1.5 hours
Add rate limiting to reply portal	Prevent spam attacks	30 min
Log bulk reassignment to AuditLog	Compliance improvement	45 min

Files Reference

Core Permission System

- `lib/crm-permissions.ts` - Centralized permission checks (441 lines)

Customer Endpoints

- `app/api/crm/customers/route.ts` - List/Create (415 lines)
- `app/api/crm/customers/[id]/route.ts` - Detail/Update (338 lines)
- `app/api/crm/customers/[id]/status/route.ts` - Status change

Bulk Actions

- `app/api/crm/bulk-actions/reassign/route.ts` - Bulk reassignment
- `app/api/crm/bulk-actions/delete/route.ts` - Bulk deletion
- `app/api/crm/bulk-actions/status/route.ts` - Bulk status change
- `app/api/crm/bulk-actions/export/route.ts` - CSV export

Messages & Threads

- `app/api/crm/threads/route.ts` - Thread list/create
- `app/api/crm/threads/[id]/route.ts` - Thread detail/reply
- `app/api/crm/email/route.ts` - Send email with thread
- `app/api/reply-portal/[token]/route.ts` - Public reply portal

Settings & Audit

- `app/api/crm/settings/route.ts` - CRM settings CRUD
- `app/api/admin/audit-log/route.ts` - Audit log API
- `app/[lang]/(dashboard)/(admin)/settings/crm/page.tsx` - Settings UI
- `app/[lang]/(dashboard)/(admin)/audit-log/page.tsx` - Audit log UI

Interests (Needs Fix)

- `app/api/crm/interests/route.ts` - CustomerInterest CRUD (missing permissions)

Database Schema

- `prisma/schema.prisma` - Customer model (lines 247-378), CRMSetting (1421-1432), AuditLog (1434-1458)

Report Generated: January 9, 2026
Next Review: After P0/P1 fixes implemented