Invoice Receiver Permissions Fix

Problem

Invoice receivers were getting **403 FORBIDDEN** errors when trying to:

1. View individual invoice details via the `invoice.getById` endpoint
2. Update invoice status (e.g., mark as paid)
3. View margin information for invoices they receive

The error occurred on:

```
GET /api/trpc/invoice.getById?batch=1&input=...
Response: 403 FORBIDDEN
```

Root Cause

The permission checks in the invoice router (`server/api/routers/invoice.ts`) only verified that the user was the **creator** (`createdBy`) of the invoice, but didn't check if the user was the **receiver** (`receiverId`).

Previous Permission Check

```
if (!isAdmin && invoice.createdBy !== ctx.session.user.id) {
  throw new TRPCError({ code: "FORBIDDEN" })
}
```

This logic only allowed:
- Admins (with `LIST_GLOBAL` permission)
- Invoice creators

But **excluded** invoice receivers entirely.

Solution

Updated three key endpoints to allow both creators AND receivers to access invoices:

1. `getById` Query (Lines 285-288)

Before:

```
// Security: non-admin can only read their own items
if (!isAdmin && invoice.createdBy !== ctx.session.user.id) {
  throw new TRPCError({ code: "FORBIDDEN" })
}
```

After:

```
// Security: non-admin can only read items they created OR received
if (!isAdmin && invoice.createdBy !== ctx.session.user.id && invoice.receiverId !== ctx.session.user.id) {
  throw new TRPCError({ code: "FORBIDDEN" })
}
```

2. `update` Mutation (Lines 435-438)

Before:

```
if (!isAdmin && invoice.createdBy !== ctx.session.user.id) {
  throw new TRPCError({ code: "FORBIDDEN" })
}
```

After:

```
// Security: non-admin can only update items they created OR received
if (!isAdmin && invoice.createdBy !== ctx.session.user.id && invoice.receiverId !== ctx.session.user.id) {
  throw new TRPCError({ code: "FORBIDDEN" })
}
```

3. `getInvoiceMargin` Query (Lines 1396-1399)

Before:

```
if (!isAdmin && invoice.createdBy !== ctx.session.user.id) {
  throw new TRPCError({ code: "FORBIDDEN" })
}
```

After:

```
// Security: non-admin can only view margin for items they created OR received
if (!isAdmin && invoice.createdBy !== ctx.session.user.id && invoice.receiverId !== ctx.session.user.id) {
  throw new TRPCError({ code: "FORBIDDEN" })
}
```

Impact

These changes now allow invoice receivers to:

✅ **View invoice details** - Receivers can now click “View” on an invoice and see the full details

✅ **Update invoice status** - Receivers can mark invoices as paid and perform other status updates

✅ **View margin information** - Receivers can see margin calculations for their invoices

Permission Logic

The new logic follows this pattern:

```
Allow access if:
  - User is an admin (has LIST_GLOBAL or UPDATE_GLOBAL permission)
  OR
  - User is the creator (createdBy === user.id)
  OR
  - User is the receiver (receiverId === user.id)
```

Testing

To verify the fix works:

1. **As a receiver user** (not admin):
   - Navigate to the invoices list
   - You should see invoices where you are the receiver
   - Click “View” on any invoice → Should NOT get 403 error
   - You should be able to see the invoice details
   - You should be able to update the invoice status

2. **As an admin user**:
   - All previous functionality should work as before
   - Can view and update any invoice

3. **As a creator user**:
   - All previous functionality should work as before
   - Can view and update invoices you created

Related Changes

This fix complements the previous fix in the `getMyInvoices` endpoint (lines 118-158) which already included both creators and receivers in the list query:

```
where: {
  tenantId: ctx.tenantId,
  OR: [
    { createdBy: ctx.session.user.id },
    { receiverId: ctx.session.user.id }, // Already included receivers
  ],
}
```

Files Modified

- `server/api/routers/invoice.ts`
- Line 286: Updated `getById` permission check
- Line 436: Updated `update` permission check
- Line 1397: Updated `getInvoiceMargin` permission check

Commit

```
commit c743fa6
Author: DeepAgent
Date: 2025-12-12

Fix: Allow invoice receivers to view and update invoices

- Updated getById query to allow both creators and receivers to access invoices
- Updated update mutation to allow both creators and receivers to update invoices
- Updated getInvoiceMargin query to allow both creators and receivers to view margins
- Fixes 403 FORBIDDEN error when receivers try to view individual invoices
```

Branch

✅ Changes pushed to `expenses-structure` branch