MIDWESTCLOUD Computing

CASE STUDY

# RFG Logistics, Inc. | AI-Powered Brand Protection & Driver Safety

RFG Logistics partnered with Midwest Cloud Computing to stop sophisticated domain spoofing attacks. MCC delivered a real-time, AI-driven detection and takedown system that safeguarded drivers, protected freight, and preserved revenue and trust.

**CLIENT**: RFG Logistics, Inc.

RFG

**INDUSTRY**: Logistics / Freight Transportation

**LOCATION**: Omaha, Nebraska

**SERVICES**: Transporting feed and organic goods, organic handling, carrier management, and trailer leasing

## ABOUT RFG LOGISTICS, INC.

RFG Logistics is a fast-growing regional freight and logistics company. With a large fleet of both corporate and independent drivers, operations depend on precise, secure digital communications for load assignments. When cybercriminals began impersonating the RFG brand online, drivers risked arriving at incorrect or unsafe locations, high-value freight was misdelivered, and trust in the company's dispatching process started to erode. RFG needed a solution that protected their people, freight, and reputation before damage occurred.

## THE CHALLENGE

RFG's growth and digital operations made them a target for increasingly sophisticated impersonation attacks:

- Cybercriminals registered lookalike domains (e.g., RF6Logistics.com, RF-GLogistics.com) to trick drivers into following fraudulent work orders.
- Drivers were sent to unsafe or incorrect pickup/drop-off sites, creating safety risks.
- Misdelivered or stolen loads caused direct revenue loss.
- Independent drivers lost trust in the dispatch process, leading to operational delays and churn.
- Dispatch staff spent hours validating every work order to prevent fraud.

The company needed a proactive, reliable solution—one that didn't just react to attacks after they occurred.

## THE MIDWEST CLOUD COMPUTING SOLUTION

Midwest Cloud Computing approached RFG's challenge with a practical, problem-first mindset. Rather than layering another generic security product on top of existing systems, we dug into how these impersonation attacks were actually disrupting drivers, dispatch, and freight movement, and built a solution shaped around those real-world needs.

**Discovery:**
We met with RFG's IT and operations teams to understand exactly how spoofed domains were being used to mislead drivers and redirect loads. By mapping the attackers' patterns, we identified where RFG needed proactive protection instead of reactive cleanup.

**Custom AI Development:**
Our team built an AI-powered monitoring system that continuously scans the internet for newly registered domains that resemble RFG's brand. It uses phonetic, visual, and character-similarity models to detect lookalike domains, even subtle variations like swapping "6" for "G," inserting hyphens or underscores, or using homoglyph characters.

**Proactive Threat Defense:**
Every suspicious domain is automatically analyzed for DNS settings, mail servers, hosting sources, and content indicators. When the system confirms malicious intent, it immediately starts takedown requests with registrars and hosting providers, often shutting down threats before attackers can use them.

**Real-Time Visibility:**
RFG now has a clean, internal dashboard that shows new threats as they appear. Optional alerts give dispatch teams early warning when a communication attempt matches a known spoofing pattern, helping them validate real work orders faster and keep drivers safe.

**Why MCC's Approach Works:**
We didn't just deliver a tool, we delivered ownership. MCC built the platform, handles ongoing tuning, manages takedowns, and ensures the system evolves as attackers get more creative. The result is a solution that protects drivers, freight, revenue, and the RFG brand every single day.

## THE RESULT

Thanks to our solution:

- **97% Reduction in Successful Spoofing Attempts** – Fraudulent domains are detected and removed almost instantly.
- **Improved Driver Safety** – Drivers are no longer sent to unsafe or wrong locations.
- **Protected Loads & Revenue** – Freight is delivered accurately, theft opportunities are eliminated.
- **Rebuilt Trust with Drivers** – Clear, secure assignments restore confidence and reduce churn.
- **Lower Operational Overhead** – Dispatch teams spend far less time validating work orders.
- **Stronger Brand Integrity** – Customers, brokers, and drivers experience consistent and secure RFG branding.

With MCC's AI-driven solution, RFG Logistics now has a proactive defense system that evolves as cybercriminals evolve—protecting people, freight, and profits every day.

## WHAT RFG LOGISTICS, INC. SAYS ABOUT MIDWEST CLOUD COMPUTING

"Before MCC stepped in, we were fighting ghost domains and fraudulent work orders. Our drivers were confused, our loads were at risk, and we were losing money. MCC's AI solution didn't just stop the attacks—it restored control and protected our people."

— IT DIRECTOR, RFG LOGISTICS, INC.

MIDWESTCLOUD Computing

(888) 483-8116

midcloudcomputing.com