MEMCYCO

Industry Impact Case Study

# Retail and e-commerce

| Client 1 | Client 2 | Client 3 | Client 4 |
|---|---|---|---|
| ~20 million customers | ~ USD 10 billion revenue | ~ EUR 3 billion revenue | ~ USD 6 billion revenue |

All four Memcyco customers are public companies with sizable revenues and a large customer base. Losing revenue and alienating customers, all because of website impersonation scams, is definitely something they can't afford.

The four companies put in place solutions based on scanning the web for lookalike domains and then proceeding to taking them down. However, these solutions left their customers unprotected for long periods of time. Also, the four companies had no visibility as to the timing and magnitude of impersonation attacks.

Additional security measures, like customer education and an MFA policy, didn't help much. The companies were in dire need of protection and visibility. And so, they came to Memcyco...

## CUSTOMERS

1. **International supermarket chain** targeted by gift card scams
2. **Global luxury goods provider** battling sites that sell counterfeits
3. **Large European fashion company** struggling with counterfeiting as well
4. **Major Asian manufacturer of CPG** hit by  a “spy” performing price scraping for the competition

## BOTTOM LINE

Memcyco’s Website Impersonation Protection solution instantly lowered the number of scams, significantly decreasing revenue losses and cutting down expenses on customer refunds and incident handling. In addition, Memcyco’s solution also increased customer satisfaction and helped keep brand reputation untarnished.

## Memcyco’s Website Impersonation Protection Solution

### Detect, Protect & Respond to Attempts-in-Progress

When these four retailers approached Memcyco about its flagship Website Impersonation Protection solution, visibility and protection is exactly what Memcyco delivered. In practical terms, that means **real-time detection and response** to scams emanating from the most sophisticated website impersonation techniques.

**It took little more than a few line of code to plug financial leaks worth millions.**

memcyco.com | info@memcyco.com

# The Challenges

## Client 1: ~20 MILLION CUSTOMERS

### INTERNATIONAL SUPERMARKET CHAIN

Presence across 50 countries, with a vast network of physical branches and a robust e-commerce platform.

THEIR CHALLENGE

### GIFT CARD SCAMS

**The retailer had been attacked by a number of malicious websites offering fake vouchers, creating a need to reimburse disgruntled customers – and leading to significant expenses related to incident handling.**

## Client 2: ~ USD 10 BILLION REVENUE

### GLOBAL LUXURY GOODS PROVIDER

Known for centuries-long reputation of excellence, with more than a thousand stores worldwide.

THEIR CHALLENGE

### COUNTERFEIT GOODS SITES

**The company had to fight a number of fake websites offering counterfeit luxury goods, leading to erosion in brand equity.**

## Client 3: ~ EUR 3 BILLION REVENUE

### LARGE EUROPEAN FASHION COMPANY

Boasts a network of branches in all major European cities, as well as a significant internet presence with dozens of highly localized e-commerce websites.

THEIR CHALLENGE

### COUNTERFEIT GOODS SITES

**The company, which sells low ticket apparel, suffers from hundreds of sites selling fake versions of its clothes, leading to significant revenue losses.**

## Client 4: ~ USD 6 BILLION REVENUE

### MAJOR ASIAN MANUFACTURER OF CPG

Operates 15 high-volume manufacturing plants in Asia and sells to thousands of retailers globally.

THEIR CHALLENGE

### PRICE SCRAPING

**Competitors had been targeting the business with price intelligence gathering, causing indirect revenue loss.**

# Memcyco ROI: Crunching the Numbers

Quantifiable savings covering two of the four clients discussed

## INTERNATIONAL SUPERMARKET CHAIN

### GIFT CARD SCAMS

**150,000 fake gift cards purchased / year**

X

**~ USD 100 in cost-to-remedy per case (reimbursement + handling)**

=

**~ USD 15M in expenses**

**33% of cases eliminated**

## ~ USD 5 million

**saved per year**

## LARGE EUROPEAN FASHION COMPANY

### COUNTERFEIT GOODS SITES

**Memcyco detects 500 fake sites per year, warns customers against buying from them, and takes them down**

X

**USD 15,000 estimated revenue loss per fake site per year**

## ~ USD 7.5 million

**saved per year**

## ALL THANKS TO

**Real-time website impersonation detection** and instant Red Alerts auto-warning users whenever they attempt to access such fake sites. The moment they click the link, both business and customers will be warned.

**Full attack forensics**

Including attack source and timing, plus which customers fell into the trap. Forensic data also enriches and fine-tunes risk engine predictions.

**SEO poisoning protection**

When hackers promote their impersonating sites, achieve a Google ranking higher than the real site, and thereby lure customers to the fake site, Memcyco applies a counter-poisoning technique to downgrade fake site ranking