MEMCYCO

CASE STUDY

How Memcyco helped a top card issuer counteract a sharp rise in credit card fraud

About the client

- Competitive presence throughout EMEA
- Known for innovative financial products
- Servicing 30M credit accounts

Why they approached Memcyco

The client needed a quick and proactive way to eliminate a rise in phishing-related scams responsible for harvesting customer cards details using highly accomplished digital impersonation techniques.

The business challenges

The card issuer's team could only gain partial and late attack visibility, following complaints from customers. Their in-place solution was able to scan for and take down the fake sites responsible but couldn't protect customers while scams were still live – or tell the issuer which customers were being exposed and impacted.

€ 1.2M p/m in remediation costs: Each of the 600 or so monthly card fraud incidents cost the bank around EUR €2000 to investigate and remediate.

Late (and partial) attack visibility: The bank learned about attacks only when customers actively decided to complain – or shamed the bank on social media.

Loss of Digital Trust, and related churn: Once defrauded, even reimbursed customers were closing accounts, fearful of repeat incidents.

Incalculable damage to brand equity: Some impacted customers were sharing negative experiences online, discouraging others from doing business with the bank.

Post-takedown fraud risk: Despite offending websites being taken down, the threat persisted – of further, related attacks launched from other domains, or through using stolen card details sold to other bad actors on the darknet.

MEMCYCO'S APPROACH

Real-time Digital Risk Protection from Credit Card Fraud

After a quick and simple installation of Memcyco's real-time AI-based technology, the issuer's teams could instantly detect and counter digital impersonation and credit card harvesting attacks in ways previously not possible.

DETECTION

- ✓ Offending sites are now detected instantly, as the attack starts
- ✓ Impacted customers are immediately identified
- ✓ Previously unobtainable attack device data is now available

PROTECTION

- ✓ Red Alerts pop up on customer screens when entering fake sites, advising them not to move forward
- ✓ Exposed card data was swapped for marked decoy data, protecting customers who provided data despite alert

RESPONSE

- ✓ Customers can keep working with their cards even if they fell victim to the attack
- ✓ Attackers are blocked from using customer cards
- ✓ Risk engine data is enriched via an API

Outcomes

Once Memcyco's agentless solution was quickly installed, the client's team could instantly detect the malicious sites as the fake URLs were being registered, and as they went live, without the delay and risk of intermittent scanning.

They could also effortlessly protect every customer who clicked a link to an offending site or entered their card data without realizing they were being scammed.

- ✓ **Incidents reduced by over 50%**
- ✓ **Millions saved in related costs**
- ✓ **Decreased customer churn**
- ✓ **Less risk of negative PR**
- ✓ **Better control of brand equity**
- ✓ **MTTD of zero (instant detection)**
- ✓ **Improved risk engine predictions**
- ✓ **Lighter caseload management**
- ✓ **Lower SOC workload**
- ✓ **Stronger compliance posture**

Cost savings calculation

600 card fraud incidents annually

X

~ €2000 in remediation costs per case

=

~ €1.2M per month in refunds and incident handling

Memcyco saving the bank approximately

€1.2 million p/m