MEMCYCO

Industry Impact Case Study

Financial Institutions

Client 1: 60M
global customers

Client 2: 30M
credit accounts

Client 3: Top 10
in North America

The above figures represent part of the burden of responsibility these three distinguished Memcyco clients hold over customers, partners and, of course their own reputations.

When it comes to safeguarding customer assets, even if you get it right 99.99% of the time, it's the 0.01% that makes headlines people remember you for. As they say, trust takes a long time to gain, but only a split second to lose.

With account-takeover scams (ATO) accelerating to full throttle in recent years, and website impersonation more accessible than ever, that split second of ATO meltdown can come without warning, or the luxury of foresight and visibility.

AT A GLANCE

1. **Major international bank**
   targeted by ATO attacks
2. **Top EMEA credit card issuer**
   experiencing CC fraud
3. **North American top-10 bank**
   hit with credential stuffing attacks

SPOILERS

Memcyco's Customer ATO and Fraud Protection solution instantly impacted sharp reductions in ATO-related incidents, netting all three clients sizeable savings on customer refunds and incident handling costs, with rapid upticks in CSAT scores, also bolstering cybersecurity frameworks and risk-engine predictive capacity.

Customer ATO and Fraud Protection

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

When these three financial institutions approached us about our flagship Customer ATO and Fraud Protection solution, foresight and visibility is exactly what Memcyco delivered. In practical terms, that means **real-time detection and response to ATO scams** emanating from the most sophisticated website impersonation techniques.

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

The Challenges

Client 1: 60M CUSTOMERS

PERSONAL BANKING & CORPORATE FINANCE

Presence across 50 countries, with a vast network of physical branches and a robust digital banking platform.

THEIR CHALLENGE

CREDENTIAL HARVESTING

The bank had been plagued by a flurry of rogue websites had been impersonating their own, causing runaway customer reimbursement and incident-response expenses.

Client 2: 30 MILLION CREDIT ACCOUNTS

TOP TIER CREDIT CARD ISSUER

Known for innovative financial products, partnering with a plethora of retail and commercial businesses throughout EMEA.

THEIR CHALLENGE

CREEPING CREDIT CARD FRAUD

Customer cards details were being stolen via fake phishing websites, impacting operational efficiency and customer trust in a highly competitive EMEA market.

Client 3: TOP 10 BANK IN NOTH AMERICA

CONSUMER & COMMERCIAL BAKING

Operating across all U.S. states and Canadian territories. Known for its consumer and commercial banking divisions, with standout presence in digital banking.

THEIR CHALLENGE

CREDENTIAL STUFFING ATTACKS

Unknown to them, the bank had been the target of persistent credential stuffing attacks, with many resulting in successful ATO, equating to dire consequences on cost structure and customer satisfaction indicators.

Memcyco ROI: Crunching the Numbers

Quantifiable savings covering two of the three FI clients discussed

INTERNATIONAL BANK

CREDENTIAL HARVESTING

12,000 ATO cases / year

X

~ USD 1,500 in cost-to-remedy per case

=

~ USD 18M / year in refunds and incident handling

56% of ATO cases eliminated

~ USD 10 million saved p / y

EMEA CREDIT CARD ISSUER

CREDENTIAL STUFFING ATTACKS

Memcyco detects 600 credit card incidents / month

X

EUR 2,000 per case

=

~ EUR 1.2 million saved p/m

~ EUR 14.4 million saved p / y

ALL THANKS TO

Real-time website impersonation detection and instant Red Alerts auto-warning users whenever they attempt to access fake sites impersonating yours. The moment they click the link, you'll know about it, and so will they.

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.

Decoy Credentials

Swap real customer credentials intercepted by fraudsters, with marked 'Decoy Credentials', trackable whenever fraudsters attempt to use them for ATO.