CASE STUDY

REAL-TIME AD VERIFICATION

How Dentsu's CCI deployed CHEQ to block 760M fraudulent, brand unsafe ad requests in absolute real-time

BACKGROUND

For more than two decades Cyber Communications Inc (CCI), owned by Dentsu Group has been at the forefront of Japan's $8.18 billion online advertising industry. CCI, the leading media company in Japan, works with 500 ad agencies and 1500 websites including Facebook, Twitter, Apple, and Yahoo-Japan.

THE ISSUE

Brand Safety and Ad Fraud Mitigation not enforced in real time

CCI faced a serious challenge that campaigns were affected by fraud, brand safety violations and lack of viewability.

Akio Niizawa, Dentsu CCI's representative director and president said: "In the Japanese market, increasing caution relating to ad fraud, and ensuring the increase in brand safety and viewability are becoming hugely important."

However first-generation ad verification providers used to tackle these challenges were found to be highly ineffective. In the first instance, existing solutions were "post-bid".

This saw verification partners only measuring problems after an ad had been served, with detection reports only issued after-the-fact. In the case of ad fraud, this required a lengthy and complex process seeking to convincing publishers to provide reimbursement for fraudulent impressions while for brand safety violations, the damage was already done. The second type of verification involved "Pre-Bid" involving verification partners scraping ad-inventory and pooling "safe" inventory into a pre-bid segment, then targeting this safe segment, to avoid negative exposure. However, CCI found this hurt scale on campaigns —the non-real time aspect of scraping and indexing, effectively excluded the newest and most popular inventory from the pre-bid segment. This measure also failed to account for the fact that URLs often change, so a page that was previously classified as safe, might not be safe at a later date.

CHEQ

THE CHALLENGE

REAL-TIME BRAND SAFETY AND FRAUD MITIGATION

CCI selected CHEQ, because of the cybersecurity company's ability to block all threats in real-time (in milliseconds) using AI and cybersecurity. For **fraud** CHEQ deploys 700 proprietary parameters, including honey pots (bot traps), advanced OS Fingerprinting and Dynamic Code patching cybersecurity technology and deep learning algorithms applied for the first time to the digital advertising industry. For **brand safety**, the CHEQ AI was trained on millions of documents to understand the nuances of Japanese cultural and brand sensitivities, satisfying the brand safety guidelines of all CCI clients.

"The most common means of blocking bad placements is to rely on past data via a demand-side platform, but the gold standard is a real-time adjustment," says Shigehiro Ando, Ad Platform Business, Division Manager, CCI.

THE CAMPAIGN

CHEQ worked with CCI to implement header tags across tens of publishers in the CCI network, which the software analyzes on an ongoing basis. CHEQ's natural language processing (NLP) was heavily trained in Japanese across tens of millions of documents, learning 39 categories of brand safety in Japanese. The solution is used by brands and publishers to secure brand safety protection, successfully understanding context any content—from alcohol to sexually explicit content, or fine art –in milliseconds. In contrast to blunt keywords-based decisions, CHEQ's AI can recognize a concept however it is phrased or wherever it appears and block brands from appearing next to unsuitable, or toxic content with complete accuracy.

"The most common means of blocking bad placements is to rely on past data via a demand-side platform, but the gold standard is a real-time adjustment."

Shigehiro Ando, Ad Platform Business, Division Manager, CCI

CHEQ

THE RESULTS

CCI used a major marketing research company to track 3,395 consumers who see served ads on publishers sites.
The study compared the experience of consumers seeing ads with CHEQ's AI brand safety and ad fraud-prevention enabled, against sites without this ad verification. The results show that click-through rates increased by up to 250% where CHEQ was in place, and ads served next to safe content, compared to publishers without this protection.
Of these ad requests, 7% were blocked for fraud (183 million impressions) before any ad was served or money paid.

Meanwhile, across 2.4 billion ad requests, nearly one quarter (24%), were blocked on the grounds of brand safety (totaling 576 million ad requests). CHEQ stopped brands from appearing next to potentially disastrous articles, including executions of women for affairs, incest, and animal cruelty.

01 183 million fraud Impressions blocked

02 576 million brand safety impressions blocked

03 Accuracy rate of 95%

04 Unlocking 80% of inventory

05 CTR increased by 250%

CHEQ