Fraud reklamowy.

Whitepaper.

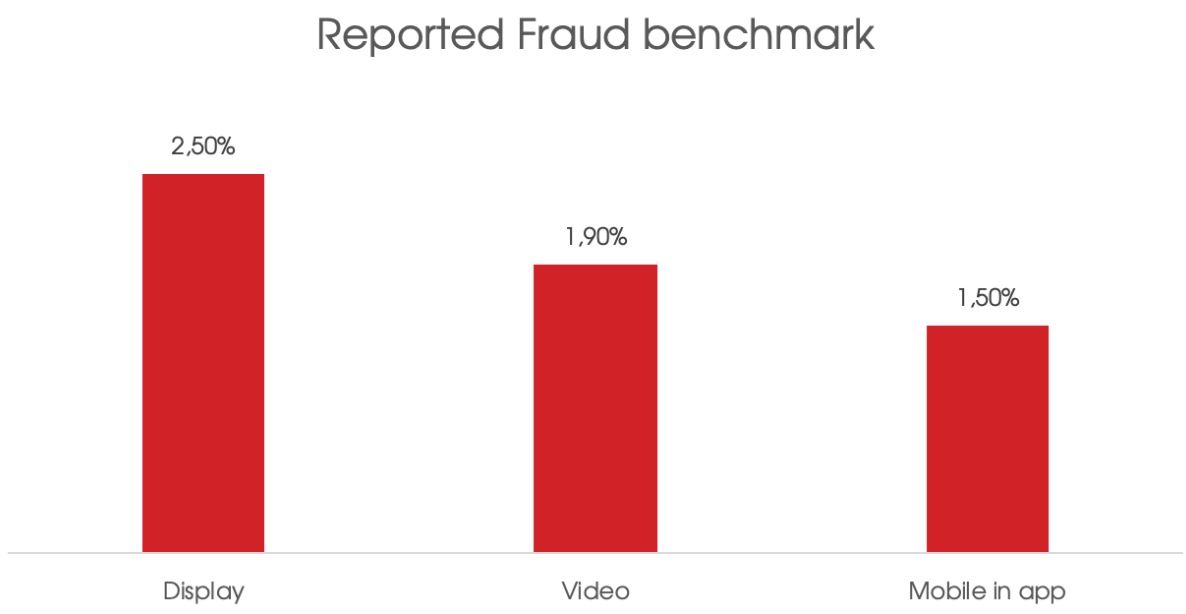
LIPIEC 2020

Spis treści

Wstęp

Etyka powinna być podstawą każdej działalności biznesowej. W branży reklamowej uczciwość jest szczególnie ceniona i pożądana. Zawsze jednak znajdzie się ktoś, kto zechce zarobić na oszustwie, zwłaszcza jeśli można w prosty sposób pomnożyć dochody reklamowe. Choć oczywiście działania takie są niezgodne z prawem i ogólnie przyjętymi normami, takie zjawiska występują. Potocznie w reklamie internetowej nazywamy je **fraudem** (z ang. *fraud* – oszustwo).

Tak jak bywa w większości działań niezgodnych z prawem, skala zjawiska jest dość trudno mierzalna. Na rynku pojawia się wiele raportów i danych. Obecnie najbardziej wiarygodne wydają się te pochodzące od liderów rynku narzędzi do pomiaru fraudów. Dane od tych podmiotów (m.in. Meetrics, IAS, DoubleVerify, MOAT) agregowane są w raporcie Digital Media Benchmark. Według zestawienia za czwarty kwartał 2019[1] roku w Polsce odnotowano fraudy na poziomie 2,1%. Oznacza to, że 2,1% odsłon reklamowych emitowanych w polskim internecie było fraudem.



Odsetek wyświetleń zaraportowanych jako podejrzane (IVT, Invalid Trffic). Zagregowane dane dla Polski, Q4 2019, pochodzące od narzędzi adloox, DoubleVerify, IAS, Meetrics, MOAT.

[1] *Digital Media Benchmark, Q4 2019, World Federation of Advertisers.*

Niniejszy Whitepaper ma na celu omówienie tematyki fraudów, wprowadzenie polskiej definicji, kategoryzacji oraz wskazanie narzędzi umożliwiających monitoring i prewencję antyfraudową. Jest też przyczynkiem do dalszej dyskusji wokół oszustw w internecie. Jesteśmy świadomi z występowania innych działań nieetycznych w reklamie internetowej, które powodują naruszenie prawa np. w stosunku do konsumenta.

W tym dokumencie skupiamy się na oszustwie, którego główną ofiarą stają się reklamodawcy, co pośrednio wpływa również na pozostałych uczestników rynku reklamy internetowej.

Fraud reklamowy

Ad Fraud - wszystkie celowe działania związane z emisją reklam (reklamy display, reklamy wideo, reklamy w aplikacjach, reklamy efektywnościowej - performance'owej i content marketing) w miejscu (serwisie internetowym/aplikacji), lub do grupy docelowej innej niż ustalone w warunkach kontraktowych. Działanie takie generuje bezpośrednio stratę finansową dla reklamodawcy (także dla wydawcy) lub utratę możliwości zarobkowej.

Oszustwa reklamowe są często określane potocznie jako nieprawidłowy ruch (Invalid Traffic, IVT), przy czym takie określenie jest niewyczerpujące w kontekście rozwoju rynku (zwiększona rola aplikacji mobilnych, wiele formatów reklamowych, formy rozliczeniowe itd.).

Nieprawidłowy ruch to szeroki termin opisujący aktywność online, która nie zawsze pochodzi od rzeczywistego użytkownika, dlatego emisja reklamy w tym wypadku nie stanowią realnej wartości dla reklamodawcy.

Kategoryzacja fraudu

Oszustwa reklamowe zachodzić mogą na wszystkich etapach cyfrowego łańcucha dostaw - od poziomu adserwera i ustawień emisji, przez odbiorców reklam i ich urządzenia, aż po strony reklamodawców.

Choć ostateczny cel oszustwa jest praktycznie zawsze ten sam - uzyskanie wynagrodzenia za działania reklamowe, które albo w ogóle się nie odbyły, albo odbyły się na innych warunkach, niż oczekiwał reklamodawca. Oszuści stosują szeroki wachlarz różnych metod zarówno zautomatyzowanych (poprzez stosowanie botów reklamowych), jak i manualnych, aby cel ten realizować.

Istnieje wiele metod działania oszustów, a ich pomysłowość zdaje się nie mieć granic. Z tego powodu, zapewne nigdy nie powstanie pełen, zamknięty katalog oszustw reklamowych.

Warto przy tym pamiętać, że część przypadków może być równie dobrze efektem ludzkiego błędu przy ustawianiu kampanii, co intencjonalnej próby wprowadzenia reklamodawcy w błąd, zatem ostateczna kwalifikacja danego zdarzenia musi brać pod uwagę jego kontekst, a w szczególności celowość działania. Choć z punktu widzenia reklamodawcy efekty są w praktyce identyczne, to poważniejsze potraktowanie tematu, także ewentualnie pod kątem sankcji na gruncie prawnym, wymaga od wszystkich zainteresowanych stron iście detektywistycznej pracy z zebranymi danymi i dobrego zrozumienia mechaniki działania oszustw.

Oszustwa reklamowe można sklasyfikować ze względu na płaszczyznę ich występowania:

- Poziom 1: Ustawienia emisji
    - Emisja na innych powierzchniach niż w zleceniu
    - Manipulacja placementami
    - Manipulacja statystykami
- Poziom 2: Odbiorca i/lub jego urządzenie
    - Oszustwa co do oferty
    - Recycling leadów
    - Ruch motywowany
    - Nieświadome interakcje
- Poziom 3: Strona docelowa
    - Fałszywe konwersje
    - Fałszowanie zaangażowania na stronie
    - Nadużycia związane ze zwrotami na stronie

Poziom 1: Ustawienia emisji

Oszustwa związane z ustawieniami emisji dotyczą najbardziej podstawowego elementu reklamy internetowej: serwowania reklam użytkownikom i ich monitorowania. Na tym poziomie możliwe jest sfałszowanie wielu kluczowych elementów, od adresów stron, na których reklama się wyświetla, przez emisję reklam w sposób niewidoczny dla realnego użytkownika, aż po ekstremalne sytuacje, w których do emisji w ogóle nie dochodzi.

EMISJA NA INNYCH POWIERZCHNIACH NIŻ W ZLECENIU

- Podszywanie się (ang. *domain spoofing*): występująca w zakupie programatycznym technika, w której oszust, podszywający się pod prawdziwego wydawcę znanego portalu, w rzeczywistości sprzedaje emisję na stronach o niskiej jakości, często specjalnie w tym celu zhackowanych.

- Emisja w niedozwolonych kanałach: występująca najczęściej w kampaniach performance marketingowych i biddable media, metoda oszustwa polegająca na emisji reklam nie na powierzchni deklarowanej przez wydawcę, tylko w kanałach bardziej efektywnych niż standardowy display (np. wyszukiwarki) lub takich, których użycie wymaga szczególnej uwagi i ścisłej współpracy z reklamodawcą (np. wykorzystanie call center). W przypadku reklamy w wyszukiwarkach, wydawca kanibalizuje standardową kampanię w wyszukiwarce prowadzoną przez reklamodawcę, zmniejszając jej potencjał lub zwiększając koszty. Nieumiejętne wykorzystanie call center może prowadzić do problemów natury prawnej i wizerunkowej dla marki.

- Kupowanie ruchu / audience'u (ang. *traffic / audience sourcing*): jeśli wydawca nie jest w stanie zapewnić odpowiedniego poziomu ruchu na swojej stronie, może go kupić od innych podmiotów - zazwyczaj będzie on niższej jakości (mniej zaangażowani użytkownicy, często pozyskani przez sprzedawcę ruchu w sposób niekoniecznie legalny lub trafiając na stronę wydawcy nie do końca świadomie) niż oryginalny, ale reklamodawca zapłaci za niego pełną cenę.

- Ruch botowy (ang. *non-human traffic, traffic bot*): wydawca zamiast emitować reklamę do prawdziwych użytkowników, wyświetla ją specjalnie do tego napisanym botom internetowym.

- Fałszywi followersi/fani (ang. *fake followers*): w przypadku marketingu influencerskiego wartość powierzchni reklamowej ocenia się głównie poprzez porównanie liczby fanów - co jest mało miarodajne i nie rekomendowane.

Jednak aby zwiększyć swoją atrakcyjność w ocenie reklamodawcy, nieuczciwi influencerzy potrafią kupować u rozmaitych pośredników polubienia ich profilu w danym medium przez specjalnie stworzone do tego boty lub użytkowników - w obu przypadkach realna wartość takiego fana jest znikoma.

MANIPULACJA PLACEMENTAMI

- Multiplikacja impresji (ang. *inflating impressions*): wydawca zwiększa liczbę wyświetleń reklamy lub skraca kontakt użytkownika z reklamą, np. poprzez nieuzgodnione z klientem użycie rotatorów, które zmieniają bannery co kilka czy kilkanaście sekund.

- Emisja niewidoczna: wydawca w jednym slocie reklamowym umieszcza więcej niż jedną reklamę, nakładając kolejne kreacje na siebie, jedna pod drugą (*ad stacking*); użytkownik widzi tylko tę, która jest na wierzchu, podczas gdy w rzeczywistości jego przeglądarka dokonała wyświetlenia nawet kilkuset reklam. Alternatywnie wydawca może otwierać reklamę w nowym, ale zminimalizowanym i pojawiającym w tle, oknie przeglądarki, przez co jest ona niewidoczna dla użytkownika (*pop-under* jako przeciwieństwo *pop-upów*, pojawiających się na pierwszym planie).

MANIPULACJA STATYSTYKAMI

- Impresje / ruch z data center (ang. *data center traffic*): w przypadku tego oszustwa emisja reklamy nie jest prowadzona do użytkowników, lecz odbywa się na wynajętych serwerach pełniących rolę emulatorów prawdziwych urządzeń. Od wykorzystania botów technika ta różni się tym, że emisja jest prowadzona w całkowicie sztucznym środowisku.

- Fałszowanie atrybucji mobilnej metodą siłową (ang. *passing falsified devices ID*) - polega na przekazywaniu wygenerowanych sztucznie ID urządzeń mobilnych do systemów trackingowych z założeniem, że jeśli na danym urządzeniu jest zainstalowana jedna z promowanych mediowo aplikacji, danemu wydawcy zostanie przypisana jej instalacja, a przez to - odpowiednie wynagrodzenie.

- Fałszowanie konwersji - "wpychanie" ciastek (ang. *cookie stuffing/cookie dropping*) - oszustwo polega na implementacji plików cookie (najczęściej od wielu różnych reklamodawców) w przeglądarce docelowego użytkownika. Działanie ma na celu przypisanie atrybucji do danego wydawcy i związane z tym oszustwa w zakresie rozliczeń prowizyjnych (CPS).

Poziom 2: Odbiorca i/lub jego urządzenie

Oszustwa tego typu zakładają wykorzystanie całego szeregu technik, których wspólnym mianownikiem jest to, że wykorzystują one albo rozmaite luki bezpieczeństwa systemów IT lub urządzeń, z których korzystają odbiorcy, albo naiwność samych odbiorców. Ich źródłem jest zatem sam użytkownik lub jego urządzenie - nawet jeśli jego właściciel jest nieświadomy swego uczestnictwa w procederze.

- Oszustwa co do oferty: niezgodne z rzeczywistością przedstawienie oferty reklamodawcy, mające na celu zachęcenie użytkownika do wykonania akcji, za którą wydawca jest wynagradzany. Wydawca przygotowuje własne wersje materiałów reklamowych, prezentujące ofertę różną od dostępnej w rzeczywistości, ale przez to zwiększającą szansę na pozyskanie użytkownika: może być to przedstawienie krótkiej jazdy testowej jako wypożyczenia samochodu na kilka dni czy komunikowanie standardowych zniżek dostępnych w e-sklepie jako kuponu rabatowego przeznaczonego wyłącznie dla danego użytkownika - w każdym z tych przypadków reklamodawca próbuje zachęcić użytkownika nieistniejącą korzyścią do kliknięcia w reklamę lub pozostawienia swoich danych osobowych.

- Recycling leadów (ang. *recycled leads*): może przybrać wiele form, ale najczęściej polega na wykorzystywaniu danych osobowych zebranych na specjalnie do tego stworzonej stronie wydawcy i wysyłaniu ich równocześnie do wielu reklamodawców w celu zwiększenia szansy na konwersję u któregokolwiek z nich lub licząc na to, że lead zostanie poprawnie zweryfikowany u więcej niż jednego reklamodawcy. Część wydawców afiliacyjnych działa w ten sposób całkowicie jawnie i - o ile reklamodawcy się godzą na taki sposób pozyskiwania leadów w ich kampaniach - nie można nazywać tego oszustwem, bo użytkownik wie, do jakich podmiotów trafią jego dane.

- Ruch motywowany (ang. *incentivized traffic*): wydawca oferuje użytkownikom jakiś rodzaj korzyści w zamian za obejrzenie reklamy lub wykonanie czynności na stronie reklamodawcy albo w aplikacji mobilnej. Takimi zachętami mogą być zarówno dobra wirtualne (np. punkty lub przedmioty w grach), jak i środki pieniężne, oferowane mniej lub bardziej bezpośrednio (programy cashbackowe). Podobnie jak w przypadku recyclingu leadów, ruch motywowany sam w sobie nie musi być oszustwem - staje się nim dopiero wtedy, gdy jest stosowany bez wiedzy reklamodawcy.

- Nieświadome interakcje (zazwyczaj na zhackowanych urządzeniach): szeroka kategoria oszustw, których cechą wspólną jest to, że oszust wykorzystując luki bezpieczeństwa na urządzeniu użytkownika, dokonuje emisji reklam, często bez wiedzy użytkownika. Przykłady:
    - Insercja reklam na strony - oszuści, wykorzystując np. wtyczki do przeglądarek, mogą emitować dodatkowe reklamy na stronach lub wręcz podmieniać wszystkie reklamy, w tym także w wyszukiwarkach takich jak Google, na takie, które przynoszą im dochód.
    - Zombienety - sieci przejętych przez oszustów urządzeń, które w tle, podczas standardowej pracy użytkownika, wyświetlają reklamy, często w sposób kompletnie dla użytkownika niewidoczny (np. w tle działania aplikacji na telefonie).

Poziom 3: Strona docelowa

Oszuści reklamowi wykorzystują również wszelkie luki bezpieczeństwa na stronach oraz w monitoringu interakcji użytkowników ze stronami, najczęściej w celu zafałszowania statystyk jakościowych lub przypisania sobie konwersji, która w innym przypadku zostałaby zatrybuowana do innego podmiotu. W ten obszar wchodzą również wszelkiego rodzaju oszustwa w kampaniach leadowych związane z wypełnianiem formularzy.

- Fałszywe konwersje
    - Nieprawidłowe leady - wykorzystanie w kampaniach leadowych danych osobowych niezainteresowanych ofertą, szczególnie przy braku dalszej weryfikacji jakości takich leadów przez call center. Oszustwo to może przybierać formę zarówno wykorzystania danych pozyskanych w sposób całkowicie nielegalny (np. kupionych od hackera), jak i - podobnie jak w przypadku recyclingu leadów - wykorzystania informacji pozyskanych przez wydawcę na swojej stronie w kontekście konkretnego produktu (np. kredytu) w kampaniach prowadzonych dla innych branż (np. ubezpieczeniach czy telekomunikacji), którymi użytkownik nie był zainteresowany w momencie powierzania swoich danych.
    - Nielegalne transakcje - wykorzystanie np. skradzionych kart kredytowych do generowania sprzedaży w sklepach lub usługach online. Reklamodawca płaci więc prowizję wydawcy za transakcje,

które najprawdopodobniej i tak zostaną za jakiś czas anulowane, a być może zostanie także zmuszony oddać pieniądze posiadaczowi karty.

- Fałszowanie zaangażowania na stronie
    - Zaawansowane boty - boty mogą być wykorzystywane nie tylko do fałszowania odsłon reklam - są w stanie realizować nawet bardzo zaawansowane scenariusze poruszania się po stronie reklamodawcy, łącznie z generowaniem fałszywych interakcji z nią (np. pobieranie cenników czy gazetek, korzystanie z wyszukiwarki punktów, sklepów czy dealerów itp.). Choć bot taki może realizować nawet najbardziej zaawansowane KPI mediowe, nie ma możliwości, aby przełożył się na realizację celów biznesowych klienta, więc jakość takiego ruchu jest praktycznie zerowa.
    - Nieprawidłowe podpięcie systemów mierzących interakcje na stronie - szczególnie direct i organic.
- Nadużycia związane ze zwrotami produktów: wydawca wykorzystuje możliwość odstąpienia od zawartej na odległość umowy sprzedaży po tym, jak otrzymał już pieniądze od reklamodawcy za wygenerowanie sprzedaży.

Przeciwdziałanie i rozpoznawanie fraudów

Identyfikacja ad fraudów to nieustanny wyścig z potencjalnymi `fraudsterami', wykorzystującymi zaawansowane technologie i systemy w celu generowania dużego strumienia przychodów z budżetów reklamowych.

Dlatego namierzanie i walka z oszustwami reklamowymi wymaga zastosowania zaawansowanych technologii umożliwiających weryfikację poszczególnych obszarów i parametrów składających się na finalną ocenę monitorowanej formy reklamowej. Dlatego systemy anty ad-fraudowe stosują rozwiązania systemowe z obszaru sztucznej inteligencji, sieci neuronowych oraz fingerprintingu.

Skuteczna walka z ad fraudami i monitoring potencjalnych nadużyć powinna odbywać się po obu stronach eko-systemu reklamowego: po stronie wydawcy dostarczającego ruch oraz reklamodawcy, do którego ten traffic jest generowany.

Poniżej przedstawiamy szereg elementarnych działań, które te strony mogą i powinny podejmować w celu rozpoznawania i przeciwdziałania oszustwom reklamowym.

Wydawca

1. Jasno określ swoje zasoby (ang. *inventory*), które sprzedajesz oraz jasne procedury operacyjne dla działów traffic.
2. Przestrzegaj zasad określonych przez Coalition for Better Ads.
3. Wdróż narzędzia i procedury regularnego przeglądu Twojego inventory oraz wykrywania anomalii.
4. Sprawdzaj swoje zasoby pod względem bezpieczeństwa na przykład poprzez cykliczne audyty. Wdróż zasady zasady zabezpieczenia swoich aplikacji i serwisów zgodnie ze dobrymi praktykami opisanymi w OWASP.
5. Zaimplementuj rozwiązanie techniczne umożliwiające blokowanie ruchu z komputerów zainfekowanych urządzeń i tych, które historycznie generowały podejrzany ruch.
6. Określ jasno zasady reklamacji.
7. Sprawdzaj swój traffic z aktualnymi bot-listami.

Reklamodawcy, agencje, domy mediowe

1. Korzystaj z narzędzi i systemow weryfikujacych dostarczany ruch reklamowy.
2. Zapytaj swojego wydawcę o stosowane zabezpieczenia anty ad fraudowe - poproś o przesłanie Specyfikacji Technicznej (ang. *Description of Methodology*) w zakresie zastosowanych rozwiązań.
3. Analizuj tzw. custom outcomy mierzone przez systemy analityczne (np. Google Analytics), po których widać, że wygenerowany ruch jest nienaturalny. Jest to widoczne np. przy benchmarku z innymi kanałami. Porównując wskaźniki obrazujące efektywność kanałów wyraźnie widać różnicę w przypadku jednego lub większej liczby współczynników. Przykładowo mogą to być:
    - Bounce rate,
    - Czas na stronie,

- Liczba Page Views (PV),
- Conversion Rate,
- Click Through Rate (CTR),
- Koszt pozyskania użytkownika,
- Bardzo niski koszt eCPA/eCPL (np. optymalizacja z CPC pod akcję na stronie, złożenie leada).

4. Używaj narzędzi pozwalających na weryfikację ruchu pod kątem jakości jego źródła. Narzędzia umożliwiają identyfikację ruchu pod kątem np. botów i weryfikują wiele współczynników, m.in:
    - Fingerprint maszyny generującej ruch,
    - Parametry systemowe,
    - Geolokalizacja,
    - Zachowanie on site.
5. Korzystaj z narzędzi pozwalających na weryfikację oszustw polegających na biddowaniu w Google Ads na np. frazy brandowe przez wydawców afiliacyjnych:
    - Aktywne - identyfikują fraud zaraz po jego wystąpieniu. Narzędzia po podłączeniu do konta Google Ads wychwytują click boty oraz inny podejrzany ruch blokując dla niego wyświetlanie reklam;
    - Pasywne - raportują fraud post factum). Narzędzia skanują w określonych iteracjach określoną liczbę fraz i zwracają raport w skład którego wchodzą dane, np.:
        - Frazę, na której pojawiła się konkurencyjna reklama,
        - Pozycję, na której pojawiła się reklama,
        - Tekst reklamy,
        - URL użyty w reklamie,
        - URL docelowy,
        - URL domeny reklamodawcy,
        - Liczbę wyświetleń reklamy.

Certyfikacje

Na rynku istnieje kilka podmiotów, które zajmują się wydawaniem certyfikatów poświadczających jakość pomiarów, a także stosowanie się określonych mechanizmów i definicji.

O ile posiadanie jakiejkolwiek certyfikacji nie jest niezbędne, może stanowić pewną przewagę nad konkurencją. Firma posiadająca certyfikację deklaruje, że stosuje się do jasnych kryteriów, przyjmuje określone definicje i poddaje się niezależnym audytom.

Wśród najpopularniejszych organizacji zajmujących się certyfikacją w zakresie wykrywania i klasyfikacji podejrzanego ruchu, wymienić należy MRC i TAG.

Media Rating Council (MRC)

Media Rating Council (MRC) to amerykańska organizacja non-profit, która wydaje akredytacje w zakresie badań i pomiaru mediów. Celem działań organizacji jest m.in. określenie minimalnych kryteriów i procedur pomiarów, a także weryfikacja skuteczności i etyczności narzędzi pomiarowych.

Akredytacją (globalną bądź lokalną) MRC mogą być objęte narzędzia do pomiaru różnego typu mediów: cyfrowych, out-of-home, drukowanych, radiowych, TV oraz produktów wieloplatformowych. Cykliczne audyty prowadzone są przez zewnętrzne podmioty audytujące, takie jak Ernst & Young.

Standaryzacji i akredytacji MRC podlega wiele wskaźników i obszarów. Wśród nich wymienić można: wyświetlenia (impressions) w zakresie zliczania i widoczności (viewability), kliki, ogólny i wyrafinowany ruch podejrzany (general & sophisticated invalid traffic).

Aktualną listę certyfikowanych i będących w procesie weryfikacji firm można znaleźć na stronie Media Rating Council.

Trustworthy Accountability Group (TAG)

Trustworthy Accountability Group, stworzona przez American Association of Advertising Agencies (4A's), Association of National Advertisers (ANA) oraz Interactive Advertising Bureau (IAB), swój certyfikat przeciwdziałający Fraudom ogłosiła w 2016 roku.

O stempel "Certified Against Fraud" (CAF) mogą wystąpić podmioty z całego świata/działające globalnie, ale tylko te, które uprzednio przeszły ogólną weryfikację TAG.

Poprzez wyznaczanie i rekomendowanie standardów, a przede wszystkim zachęcanie firm do działania według nich, Program CAF wspiera redukcję poziomu podejrzanego ruchu w przestrzeni reklamy cyfrowej. Obecnie ponad 125 firm posiada stemple przeciwdziałania fraudom, piractwu i złośliwemu oprogramowaniu, wśród nich np. Google, eBay, carat, IPG Mediabrands, GroupM i The Washington Post.

Jednym z wymogów programu CAF jest zgodność z wytycznymi MRC (Media Rating Council) w zakresie wykrywania i filtrowania podejrzanego ruchu GIVT (General Invalid Traffic).

Lista firm ze stemplem CAF dostępna jest na stronie TAG.

Stemple przysługujące firmom zweryfikowanym przez TAG w poszczególnych obszarach.

Podsumowanie

Fraud reklamowy jest tematem skomplikowanym i wymagającym ciągłej edukacji na wielu płaszczyznach. Ponadto jest to obszar, który ze względu na swą specyfikę i dynamizm, trudno ustandaryzować. Niemniej jednak, jest to zjawisko na tyle ważne dla branży reklamy online, a także dla samych użytkowników internetu, że konieczne jest podejmowanie kolejnych kroków w kierunku ograniczania i zwalczania wszelkich oszustw reklamowych.

W skład **Grupy Zadaniowej ds. Fraudów** przy **IAB Polska** wchodzą przedstawiciele firm:
ABT Shield
Agora
GroupM
Interia
Mediacom
Meetrics
Nielsen
Polska Press
Ringier Axel Springer
TrafficWatchdog