August 12, 2020

Marlene Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington DC 20554

Re: Notice of *Ex Parte* Presentation, CG Docket No. 02-278, Petition of Assurance IQ, LLC

Dear Ms. Dortch:

This *ex parte* Notice relates to a meeting held on August 11 between representatives from various consumer groups with staff of the Bureau on Consumer and Governmental Affairs, along with Tim Sostrin, an attorney representing a consumer in a case pending against Assurance IQ, LLC. The Bureau staff in attendance were Aaron Garza, Mika Savir, Karen Schroeder, and Mark Stone. The consumer representatives in attendance, in addition to myself, were Linda Sherry from Consumer Action, Susan Grant from Consumer Federation of America, and George Slover from Consumer Reports.

During the meeting, Mr. Sostrin presented a PowerPoint (which is included in the *ex parte* he has filed with the Commission relating to this meeting). Mr. Sostrin's *ex parte* is attached to this filing as well. Additionally, we discussed the points made in our comments opposing the Petition for Declaratory Ruling.[1]

If there are any questions, please contact Margot Saunders at the National Consumer Law Center (NCLC), msaunders@nclc.org (202 452 6252, extension 104).

This disclosure is made pursuant to 47 C.F.R. § 1.1206.

Thank you very much.

---

[1]Comments of the National Consumer Law Center and Consumer Action, Consumer Reports, National Association of Consumer Advocates, and Public Knowledge, in opposition to the Petition for Declaratory Ruling filed by Assurance IQ, LLC, filed on June 22, 2020, *available here* https://ecfsapi.fcc.gov/file/10622280311488/Consumer%20Comments%20on%20Assurance%20Petition.pdf

Sincerely,

Margot Saunders
Senior Counsel
National Consumer Law Center
1001 Connecticut Ave, NW
Washington, D.C. 20036
msaunders@nclc.org
www.nclc.org

KEOGH LAW LTD.

August 12, 2020

VIA Electronic Filing

Marlene H. Dortch, Secretary
Federal Communications Commission
Office of the Secretary
445 12th Street, SW
Washington, DC 20554

Re: Notice of Written *Ex Parte* Presentation, Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278

Dear Secretary Dortch:

Pursuant to Section 1.1206 of the Federal Communication Commission's ("FCC") rules, the undersigned counsel provides ex parte notice concerning an August 11, 2020 meeting on the Petition for Expedited Declaratory Ruling filed by Assurance IQ, LLC.[1] During that meeting, Timothy J. Sostrin of Keogh Law, Ltd. who is one of the attorney's representing James Shelton in a lawsuit filed against the petitioner,[2] Margot Saunders of the National Consumer Law Center, Linda Sherry from Consumer Action, Susan Grant from Consumer Federation of America, and George Slover from Consumer Reports met with Bureau staff Aaron Garza, Mika Savir, Karen Schroeder, and Mark Stone.

In the meeting, we discussed the topics and issues raised in Mr. Shelton's comments filed in opposition to the petition, [3] as well as the topics and issues raised in the National Consumer Law Center's comments filed in opposition to the petition.[4]

---

[1] *Petition for Expedited Declaratory Ruling Regarding the Application of 47 U.S.C. § 227(b)(1) of the Telephone Consumer Protection Act*, CG Docket No. 02-278 (May 12, 2020)

[2] *James Everett Shelton et al. v. Lumico Life Insurance Company and Assurance IQ, Inc.*, Civ. Action File No. 7:19-cv-6494, United States District Court for the Southern District of New York, filed July 12, 2019.

[3] https://ecfsapi.fcc.gov/file/10622624728686/98973.PDF; https://ecfsapi.fcc.gov/file/107071574027591/shelton%20reply%20comments%20to%20assurance's%20petition%20(final).PDF

[4] https://ecfsapi.fcc.gov/file/10622280311488/Consumer%20Comments%20on%20Assurance%20Petition.pdf

In addition, Mr. Sostrin presented the following power point presentation to provide (1) an explanation of the lead generation and affiliate marketing ecosystems and how they are supposed to function for those in the industry; (2) examples of Publisher web pages that contain consent forms that purport to authorize numerous entities to place telemarketing calls unrelated to the services advertised on those websites; (3) a demonstrative example of lead data that is typically sold in the industry; (4) excerpts from a complaint explaining how lead data often passes through numerous lead aggregators before it ends up in the hands of a telemarketer, who is in no position to evaluate the integrity of the data; (5) an explanation of how lead generators can commit fraud by manipulating the data they sell; (6) allegations made by a telemarketer against a lead generator that the lead generator fabricated the lead data it sold to the telemarketer; (7) an explanation of how affiliate marketers can commit "form fraud" by going to publisher websites and entering a consumer's contact information without that consumer's knowledge or consent; (8) an overview of the various software solutions sold on the market to detect and stop form fraud by affiliate marketers; (9) media reports concerning form fraud by affiliate marketers; (10) a hypothetical scenario intended to establish that Assurance's proposed "reasonable basis" rule is unworkable because it fails to describe what is prohibited by law and leaves victims of fraud with the unreasonable burden to opt out of calls from hundreds of entities; and (11) proposed solutions for telemarketers who seek to rely on consent form data.

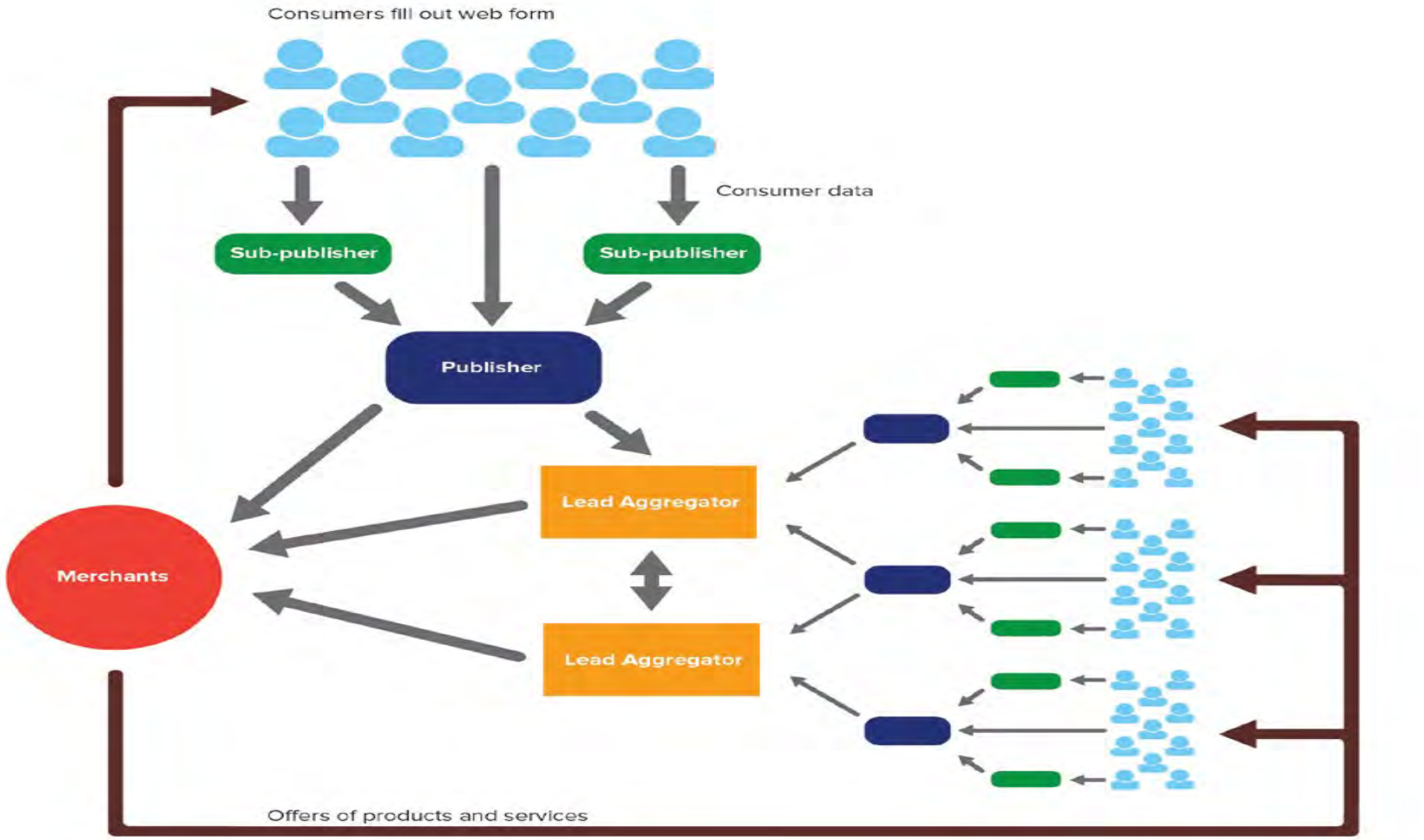
Sincerely,

Timothy J. Sostrin
KEOGH LAW LTD
55 W Monroe St, Ste. 3390
Chicago, IL 60603
(312) 726-1092 / (312) 726-1093 –fax
keith@keoghlaw.com
tsostrin@keoghlaw.com

Lead Generation Fraud

- The Lead Generation and Affiliate Marketing Ecosystems
- Lead Data
- Fraud by lead aggregators (manufactured consent data)
- Fraud by affiliate marketers (fraudulent form fills)
- Reasonable Basis Test is Unworkable
- Solutions

The Lead Generation Marketplace (how it is supposed to work)



Publisher Web Pages – Consent for Telemarketing Calls from Numerous Entities

- Click4Riches
- petfreebiepromos
- Assurance
- the-solar-project

Lead Data Looks Like This

First	Last	Phone	Address	URL	Ip Address	Date time
Martin	Joyce	312-312-22[redacted]	202 main street Chicago, Illinois	homesafecomsign-up	24.148.57.23	6/10/2020 9:00
James	Lawrence	653-821-15[redacted]	111 Ridge Road Carson City, NV	supersecurebizdeal	28.166.58.44	6/8/2020 14:00
Mickey	Mouse	555-867-53[redacted]	44 Magic Kingdom Way Orlando, FL	homesafecomsign-up	24.148.57.23	6/10/2020 9:00

Callers are in No Position to Evaluate the Integrity of the Data

- Complaint alleges: "This [July 21, 2016] call was placed as part of an advertising campaign that Nationwide set up through advertising company Universal McCann and QuinStreet. QuinStreet, in turn, has indicated that the July 21, 2016 call to Ken Johansen came through several further layers of third-party lead generators—i.e., QuinStreet received the lead by way of Avenge Digital, which received the lead through Astoria, which received the lead through Direct Web Advertising, which received the lead through Philippines-based Abundantgeeks—and was ultimately derived through a purported "opt-in" obtained through BestCheapIns.com. Dianne Rice Redding v. Nationwide Mutual Insurance Co., 16-cv-3634, Do. 79, at ¶¶ 125-26 (March 8, 2019).

Callers are in No Position to Evaluate the Integrity of the Data (continued)

- Complaint alleges: "These March 2015 calls to Ken Johansen were made by McGlothin Insurance and Co. ("McGlothin"), a Nationwide-exclusive insurance agency based in Columbus, Ohio, which obtained Ken Johansen's information by purchasing it as a "lead" from lead generator LeadAmp. LeadAmp, in turn, claims that it obtained Ken Johansen's lead information from another third-party lead generator, Precise Leads, which, in turn, claims that it obtained Ken Johansen's lead information from yet another thirdparty lead generator, TBMR. TBMR's owner has since confirmed that it never had any relationship with Nationwide, and that TBMR is not in possession of any evidence indicating that Ken Johansen's contact information was obtained via the website Nationwide associates with the purported lead." Dianne Rice Redding v. Nationwide Mutual Insurance Co., 16-cv-3634, Do. 79, at ¶¶ 103-04 (March 8, 2019).

Lead Generator Fraud

- Sometimes, aggregators fabricate the data
- Reuse lists
- Change urls, times, etc.
- Hard for the Purchaser to know

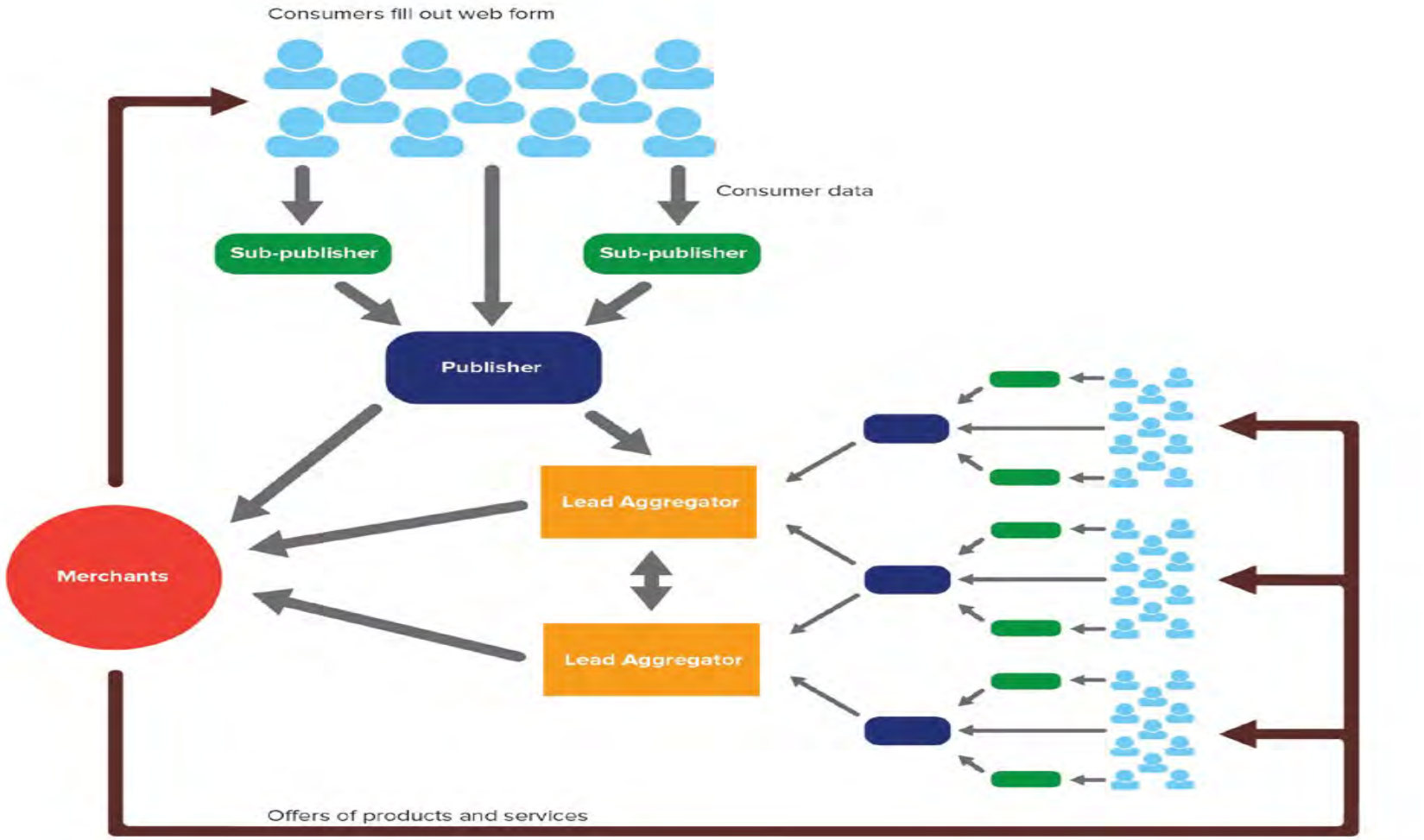
Telemarketer Sues Aggregator for Fabricating Data

- Dicksen v. Direct Energy LP, 18-cv-182 (N.D. Ohio May 7, 2020)
  - Direct Energy alleges that "TMC sent Direct Energy an Excel spreadsheet of data and a website screenshot that TMC represented was evidence of Plaintiff's purported opted-in. Recently, in the course of discovery, Direct Energy learned that TMC's documentation was faked and its representations false. TMC employees manufactured the "Dickson opt-in" and fraudulently passed it off to Direct Energy claiming that it was legitimate—it was not."
  - Direct Energy alleges that "the Excel spreadsheet TMC provided listing the Dickson personal information did not originate from any master spreadsheet, central records repository, database, or "system" . . . Rather, the "Dickson opt-in" originated from TMC employee Joe Yates, who apparently created the Excel spreadsheet and then circulated it to other TMC employees to ensure that the "date lines up with the call date(s) before sending [to Direct Energy]."

Fraudulent Form Fills

- Sometimes, the fraud takes place when contact information is entered at the publisher's website
- somebody enters a consumer's personal information without their knowledge or consent
- Can be a bot, or a human click farm
- Who does this?
  - Affiliate Marketers earn commissions by generating leads

The Lead Generation Marketplace (how it is supposed to work)



Affiliate Marketers Drive Traffic to Publisher's Websites

How Do we Know? - Form Fraud Detection Software

- Fraudlogix – “Affiliate Marketing Suite”
  - Stop fraud before it happens by blocking high-risk traffic at the click level.
- Nura – “Achieve TCPA compliance with an ad fraud solution.”
  - An ad fraud detection solution like Anura can help your organization easily determine whether forms are being filled out by bots, malware, or human click farms. As a result, lead generation marketers get the peace of mind that comes with knowing their lead capture data is accurate and that their methods are in compliance with the TCPA.
- Partnership Cloud, by Impact - “Pay for Leads, Not Dead Ends”
  - Fraud especially targets lead-generation campaigns, collecting high payments for stolen or recycled info. Gain real-time insights into suspicious traffic sources to quickly identify high-risk partners. Block payments for illegitimate lead and conversion events.
- IPQualityScore – “Proactively Prevent Fraud”
  - “IPQS provides complete protection for your sites and apps from fake signups, fraudulent accounts, and invalid lead generation data.” “Some sites may notice up to 17% of their accounts are using stolen user data or completely invalid user information”
  - “IPQS performs the most advanced verification methods while also checking against our database of compromised user information and data associated with recent abuse across the IPQS threat network. Automatically block fraudsters that have engaged in lead generation fraud and fake signups across the internet's most popular sites.”
- e-Hawk – “Block Fake Leads and Fraud Sign-Ups”
  - “To detect and block fake traffic from your affiliate ad campaigns, our affiliate lead fraud and ad fraud solutions have got you covered.”

How do we know? - Media Reports

- WALL STREET JOURNAL, **Fraudulent Web Traffic Continues to Plague Advertisers, Other Businesses,** March 8, 2018
  - "Web traffic is rife with bots and non-human traffic, making it difficult for ad and media businesses to understand who is visiting their sites and why, according to new findings from Adobe. In a recent study, Adobe found that about 28% of website traffic showed strong 'non-human signals,' leading the company to believe that the traffic came from bots or click farms."
- PERFORMANCE MARKETING INSIDER, **Bot Form Fills are Destroying Lead Generation Industry. What can Be Done?**, March 19, 2019
  - "Deceitful affiliates will maximize leads by using bots, malware, or an even more sophisticated method – human fraud farms engaged in filling out forms with real people's information."
- DIGIDAY, **Confessions of a Lead-Gen Specialist,**
  - "I have seen thousands of leads come through in a matter of hours from one source. All were fraud, and none of the leads had ever opted in or had any memory of visiting the site/offer."
  - "Fraud is part of the game, just price it into your model and you will relieve yourself of a lot of stress."

A Reasonable Basis to Believe Test is Unworkable

Scenario. Home security company pays a lead aggregator to provide it with leads who have consented to receive telemarketing calls from home security companies.

- Contract says all leads will be Opt-Ins who provided their information on a web page that expressly authorizes telemarketing calls from the home security company.
- Home security company pays a premium for Opt-In leads
- Aggregator provides lead data in spreadsheet form

Does it have a reasonable basis to believe the people it is calling have consented??

What if the telemarketer researched the aggregator's reputation and couldn't find any complaints about the integrity of its data?

What if the telemarketer reviewed all of the URL's and determined that the consent disclosure is actually complaint with this Commission's rules?

What if it reviewed only a quarter of them?

What if the data set contained a significant number of obviously fake names or addresses, like Mickey Mouse at 123 Main Street, The North Pole? What is a significant number?

What if a significant number of the ip addresses are actually assigned to TOR Exit Routers? What is a significant number?

Reasonable Basis to Believe Test

- Nobody knows how to answer these questions
- Rule would fail to describe what exactly is prohibited by law - should keep bright line test
- Would leave victims of fraud without recourse under TCPA - May have to Opt out of calls from hundreds of entities

Solutions

- Confirm Form Submissions with an email
  - “If the email bounces, is not responded to or is responded to with I didn’t submit anything on your web site the lead should be tossed.” Comments of Joe Shields, at p. 2.
- Or, call leads without using an ATDS or prerecorded message in order to confirm the consent.
- Or, mitigate risk by using one of the many products (Fraudlogix, Anura, etc.) that focus on detecting and blocking fraudulent traffic.
  - should do so at their own risk. Don’t place the burden of fraud onto the victims