Bloomberg BNA

Privacy and Security Law Report®

Lead Generation

Lead generation and data aggregation firms have amassed databases rich in content including detailed consumer and behavioral information. Regulators have recognized the important role lead generators play in matching service providers with consumers, but are cracking down on practices that they deem deceptive or unfair. The authors detail four main lessons from the recent flurry of enforcement activity.

'Lead Generation' Business Under Regulatory Glare for Privacy Violations



By Benjamin Fishman, Craig A. Newman and Geoffrey Potter

Lead generation and data aggregation companies that focus on collecting consumer data for marketing purposes have done surprisingly well in the last few years. And in doing so, they have amassed databases rich in content, including detailed consumer and behavioral information. One leading data broker boasted of a database that includes ''[d]emographics, life-stage segmentation, brand affinities and purchase tendencies for nearly every adult consumer in the U.S.'' Now, though, these companies are facing increased scrutiny by federal and state regulators.

Benjamin Fishman is an associate at Patterson Belknap Webb & Tyler LLP in New York.

Craig A. Newman is a partner at Patterson Belknap Webb & Tyler LLP in New York and chairs the firm's Privacy and Data Security Practice.

Geoffrey Potter is a partner at Patterson Belknap Webb & Tyler LLP in New York.

In a May 2014 report entitled ''Data Brokers: A Call for Transparency and Accountability,'' the Federal Trade Commission (FTC) noted that ''[d]ata brokers acquire a vast array of detailed and specific information about consumers; analyze it to make inferences about consumers, some of which may be considered sensitive; and share the information with clients in a range of industries'' (13 PVLR 947, 6/2/14). Such data might be acquired from consumer purchase data, social media posts, internet search queries and government census data, among other sources.

The data collected varies by industry and sector but typically includes consumer contact information, e-mail, telephone and demographic data. Other data might be based on consumers' political affiliation, ethnicity or even dieting habits.

Regulators have recognized the important role lead generators play in matching service providers with consumers. FTC Bureau of Consumer Protection Director

 ISSN 1538-3423

Jessica Rich said in opening remarks to an October 2015 forum on lead generation, ''lead generation is a well-established industry that has served an important role in the marketplace for many decades. . . . Consumers can spend hours, days or even weeks, searching for the goods or services that meet their needs, at their price. Advertisers and businesses constantly are searching for new and better ways to reach these consumers. Lead generators serve the important function of connecting the two. That's a good thing.''

But at the same time, regulators are cracking down on practices that they deem deceptive or unfair. In February 2016, the FTC announced that it had reached a $5.7 million settlement in *FTC v. Sitesearch Corp.*, an action brought under Section 5 of the FTC Act (15 PVLR 378, 2/22/16). Section 5 permits the FTC to bring civil actions for ''unfair or deceptive acts or practices in or affecting commerce'' where such acts ''cause substantial injury to consumers'' that consumers cannot reasonably avoid, and where such injury is not outweighed by ''countervailing benefits to consumers or competition.'' *See* 15 U.S.C. § § 45(a) & 45(n).

The *Sitesearch* complaint alleged that the defendants—a group of lead aggregators and their principals—sold personal information of hundreds of thousands of consumers, including social security and bank account numbers, to buyers that had ''no legitimate need'' for it. The defendants purchased the data from payday lending websites that had culled it from online loan applications submitted by cash-strapped consumers. The FTC's complaint alleged that ''[a]t least one'' of defendants' customers used the purchased data to scam consumers by making unauthorized withdrawals from their bank accounts, and that the defendants knew or had reason to know that this had happened. But the defendants' other customers are described as ''spammers and telemarketers,'' and all of these customer—the fraudsters as well as the telemarketers—are referred to in the complaint as ''non-lenders'' with ''no legitimate need'' for the data they purchased. The defendants' sale of private consumer data to customers with ''no legitimate need'' for the data is the basis for the Section 5 count.

The health-care sector, too, has been a focus for FTC scrutiny.

In a similar action filed by the Consumer Financial Protection Bureau (CFPB) in December 2015, *CFPB v. D and D Marketing, d/b/a T3Leads*, the CFPB charged that T3Leads, a lead aggregator, and its principals, violated the Consumer Financial Protection Act (CFPA) of 2010. Similar to Section 5 of the FTC Act, the CFPA prohibits ''unfair'' acts injuring consumers, where such injury cannot reasonably be avoided and where the harm is not outweighed by countervailing benefits to consumers or competition. *See* 12 U.S.C. § 5531(c)(1). The CFPA also prohibits ''abusive'' acts that ''take[] unreasonable advantage of . . . a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service.'' *See id.* § 5531(d)(2)(A).

In its complaint, the CFPB alleged that T3 sold personal data purchased from websites that solicited applications for payday and installment loans. T3 sold the data to various customers, including lenders, other lead aggregators, and marketers. The CFPB charged that T3 and its principals violated the CFPA because, in buying and selling this data, they ''failed to vet or monitor'' either the sellers or purchasers of the data, thereby ''expos[ing] consumers to the risk of having their information purchased by illegal actors.'' Specifically, the complaint charges that the defendants should have known that the websites which generated the leads made false or misleading statements to potential borrowers. The complaint also alleged that the defendants should have known that many of their customers were likely to charge above-average interest rates (contrary to the promises made on the lead-generating websites).

Finally, the CFPB charged that defendants should have known that there was a ''risk'' that some customers would engage in illegal conduct, such as abusive debt collection practices and fraud, because such conduct is common in the payday and installment lending industry. As head of the CFPB Richard Cordray said in a CFPB press release: ''This is a reminder to the middlemen who traffic in personal information: if you ignore warning signs that those buying this data are violating the law, you risk the consequences for the harm you are doing to people.''

In April 2016, the CFPB, based on the same facts, filed separate complaints against the two founders of one of the defendant companies, alleging ''substantial assistance'' in the alleged violations of the CFPA.

Also in April 2016, the FTC announced that it had settled its first Section 5 enforcement action against an education lead generator, Gigats.com. In its complaint, the FTC alleged that the company and its principal gathered online job announcements and summarized them on its website, which made it appear that the site would accept applications for the positions. But in fact, Gigats had no authority to accept the job applications and was simply gathering the would-be job applicants' personal data—including education and employment status—in order to market for-profit schools, which were paying Gigats between $22 and $125 for each lead. The settlement order included a $90 million penalty, almost all of which is suspended based on the defendants' inability to pay. The order also prohibits defendants from making misrepresentations like those described in the complaint.

In a press release accompanying the Gigats settlement, the FTC warned: ''Members of the lead generation industry should take this as one more reminder of the need for transparency. Be upfront with consumers about what you're up to and don't use deception to elicit personal information.''

State attorneys general have not stayed on the sidelines.

The health-care sector, too, has been a focus for FTC scrutiny. In February 2015, the Commission filed complaints against PaymentsMD and its Chief Executive Officer, charging that they violated Section 5 of the FTC

  PVLR ISSN 1538-3423

Act. The FTC alleged that the defendants failed to adequately inform customers of the PaymentsMD health billing portal that it was attempting to collect the customers' health data (including prescriptions, procedures, medical diagnoses, and lab tests) from third-party insurers, pharmacies, and labs. According to the complaint, PaymentsMD was attempting to collect that data in order to create a comprehensive individual health record that would be marketed back to those same customers. (As it turned out, almost none of the third parties PaymentsMD contacted provided any of the requested information.) In a press release, the FTC's Rich said: ''Using deceptive tactics to gain consumers' 'permission' to collect their full health history is contrary to the most basic privacy principles.''

While the PaymentsMD case involved aggregating individuals' health information from third parties in order to sell a product back to those same individuals, it is easy to imagine the FTC targeting, on the same basis, a company selling individuals' health information, without their consent, to third-party marketers. Indeed, the PaymentsMD settlement orders specifically prohibit PaymentsMD and its CEO from misrepresenting to consumers not only the extent to which they will *seek* private health information from third parties (as was at issue in the matter), but also the extent to which they will *share* such information with third parties. In a March 2016 statement to a congressional subcommittee, the FTC's Rich made clear that the agency views Section 5 of the FTCA as providing broad authority to the agency to pursue ''both Health Insurance Portability and Accountability Act (HIPAA) and non-HIPAA covered entities'' that engage in ''unfair or deceptive'' practices involving health data, including ''unauthorized disclosure.''

State attorneys general have not stayed on the sidelines. For instance, in complaints filed in December 2015 and April 2016, the West Virginia Attorney General charged three pharmacies with participating in a single scheme to violate state consumer protection laws by misusing consumers' health-care data, which the defendants obtained through online ''forms, surveys and other questionnaires.'' The complaints allege that the defendants, including the pharmacies' individual principals, used this information to generate forms directing doctors' offices to transfer the consumers' prescriptions to the defendant pharmacies. In May 2016, a West Virginia circuit court denied the defendants' motions to dismiss those charges.

The early lessons from this flurry of enforcement activity are four-fold:

- Government agencies are increasingly focused on policing this industry. While the CFPB's jurisdiction is limited to the financial sector, the FTC and state attorneys general will likely continue to bring enforcement actions involving lead generation in a variety of industries.
- As the *Sitesearch*action shows, the FTC will bring enforcement actions not only where leads are purchased from or sold to actors that clearly violate the law, but also where the conduct of lead generators or end-users is ''illegitimate,'' or where there is a material ''risk'' that the generators or users of leads will violate the law.
- The enforcement actions thus far have targeted not only companies, but their individual principals, so regulators are holding those in leadership positions accountable.
- Finally, for companies that buy or sell sensitive consumer data, and their principals, regulators will likely continue to focus on whether the consumers whose data is being bought or sold have been fairly apprised of how their data might be used, and whether the data is likely to be used to ''legitimate'' ends.