Defending a Data Breach Investigation by the Federal Trade Commission

Kevin L. Coy and Robert R. Belair

Your company has experienced a data breach, and the Federal Trade Commission ("FTC") notifies you that it is initiating a non-public investigation. How the company responds can significantly affect the course of the investigation and whether the FTC ultimately brings an enforcement action.

At the outset, the company likely will receive notice from the FTC of its investigation and a request for information and documents. This request can come in the form of an "access letter," requesting that the company voluntarily provide the requested information, or, more frequently, in the form of a Civil Investigative Demand ("CID"), the FTC's version of an administrative subpoena. The "request" typically will ask the company to preserve relevant records, so it is important to put a litigation hold in place, like the company would for a general litigation matter.

The access letter or CID will include the name of one or more FTC staff attorneys ("the Staff"), who will be the company's point of contact regarding the investigation and the lead investigators for the matter, and a timeline for both responding and discussing any concerns about the access letter or CID. As a general rule, we find it helpful to work through the Staff responsible for the investigation rather than attempting to work around them. There may be exceptions, but in our experience there often is little to be gained by attempting an end run around the Staff responsible for the case and immediately taking the matter "up the line" to more senior FTC officials. Reaching out to more senior FTC officials and the Commissioners themselves can be helpful, but we have found that to be a tactic best deployed later in the process.

If the CID or access letter is overly burdensome, negotiate with the Staff in an effort to narrow their requests and/or request additional time to produce the information that they are requesting. (There also is a brief window to seek to quash a CID in court, although we have found compromises with the Staff are frequently attainable. Plus, the FTC has broad investigative authority, so it is exceedingly difficult to quash a CID.) In the case of a data breach investigation, the cause of the breach, consumer harm, and the reasonableness of the company's information security program are key considerations, and most requests likely will focus on these aspects. Unless an organization has a prior history with the FTC, however, the Staff may not understand how it maintains its records or what information is or is not readily available. We have had success negotiating with the Staff to reduce the burden on clients in responding to FTC information and document requests through education about such matters.

The Staff also may seek oral testimony (the FTC's version of depositions) from company personnel. We have negotiated with the Staff regarding who will be called to give oral testimony and related logistics. We also have worked with witnesses to help them prepare for their oral testimony and represented them while the FTC has taken their oral testimony. In some FTC investigations, we have found it helpful to bring clients in to meet with the Staff outside the formal oral testimony process in an effort to address potential Staff questions and promote closure of the investigation without an enforcement action.

Many FTC inquiries are closed by the Staff without action once the investigation phase is completed. We have found it helpful to submit an informal "brief" or "white paper" making the case for closing the investigation. If, however, the Staff believe that a non-frivolous violation of law has occurred, they may propose that the target company enter into a settlement agreement to resolve

the issue. A proposed settlement may take the form of an administrative order or a stipulated order to be entered by a federal district court. The Staff's recommendation is not dispositive, so, after attempting to resolve the matter with front-line Staff, we frequently have reached out to more senior FTC officials and ultimately to the Commissioners themselves—both to advocate closure of an investigation without an enforcement action and to negotiate over particular terms of a settlement agreement.

If the company decides to try to settle the matter, settlements often follow the template that the FTC has used in prior information security/data breach cases. While the FTC Staff often resists changes to their settlement template, modifications are possible and should be considered carefully. Also, do not forget the complaint. In the event of a settlement, the FTC's complaint and accompanying press release will frame any settlement order. Although difficult to accomplish, we have sought to negotiate these with the Staff to ensure that they are accurate and more favorably set the stage against which any settlement will be viewed.

In addition to the operational terms of the settlement—which, in data security cases, customarily include a mandatory information security program, 20 years of biennial, independent third-party assessments of that information security program, and various recordkeeping and reporting requirements—there is the question of whether there will be a monetary penalty. Whether the FTC can seek a civil penalty will depend on which statute(s) the FTC can use as a basis for its action.

If the company cannot come to an agreement regarding the disposition of a matter, litigation is always an option. Litigation (either administrative or judicial) as a result of FTC data breach investigations, however, has been rare. To date, it has only happened twice (as compared to over 50 settlements without litigation and many more closed without any action). Wyndham Hotels initially declined to settle with the FTC after a data breach investigation and challenged the FTC's authority to bring data security cases under Section 5 of the Federal Trade Commission Act (the "FTC Act"). Wyndham ultimately reached a settlement with the FTC in December 2015 after an adverse ruling from the Third Circuit in August of that year, upholding the FTC's authority to regulate data security under Section 5 of the FTC Act. In the second case, LabMD has been vigorously fighting an administrative enforcement action brought by the FTC Staff against the company following a data breach involving health information. LabMD won before an administrative law judge ("ALJ"), but in a Decision and Order published on July 29, 2016, the Commission reversed the ALJ and found that LabMD engaged in unfair practices in violation of Section 5 of the FTC Act as a result of inadequate data security practices.

Authors and Contributors

Kevin L. Coy
Partner, DC Office
202.677.4034
kevin.coy@agg.com

Robert R. Belair
Partner, DC Office
202.677.4040
robert.belair@agg.com

not *if*, but *how*.®

About Arnall Golden Gregory LLP

Arnall Golden Gregory, a law firm with more than 150 attorneys in Atlanta and Washington, DC, employs a "business sensibility" approach, developing a deep understanding of each client's industry and situation in order to find a customized, cost-sensitive solution, and then continuing to help them stay one step ahead. Selected for The National Law Journal's prestigious 2013 Midsize Hot List, the firm offers corporate, litigation and regulatory services for numerous industries, including healthcare, life sciences, global logistics and transportation, real estate, food distribution, financial services, franchising, consumer products and services, information services, energy and manufacturing. AGG subscribes to the belief "not if, but how.®" Visit www.agg.com.

Atlanta Office
171 17th Street, NW
Suite 2100
Atlanta, GA 30363

Washington, DC Office
1775 Pennsylvania Avenue, NW
Suite 1000
Washington, DC 20006

To subscribe to future alerts, insights and newsletters: **http://www.agg.com/subscribe/**