wiley

NEWSLETTER

FTC Agreement Adds to the Accretive Health Enforcement Saga

January 2014

On New Year's Eve, the Federal Trade Commission (FTC) announced a consent order settlement with Accretive Health, Inc., purporting to address the latter's failure "to employ reasonable and appropriate measures to protect personal information against unauthorized access." This matter is potentially significant and troubling for multiple reasons. Specifically, the FTC suggests a broad requirement for businesses in general to adopt complex data security programs, even in the absence of any security claim, under the commission's "unfairness" power. There is also reason to believe the enforcement initiative was motivated, at least in part, by the FTC's dislike of certain Accretive Health debt collection practices that also motivated enforcement by the Minnesota Attorney General (AG) in 2012.

Enforcement Background

As characterized by the FTC, Accretive Health is a business that enters "service agreements with hospital systems" to provide "revenue cycle" services including "registration, transcription, coding and medical documentation, billing, denial management, strategic pricing, and collection of past due accounts." It does so through "technology, operating methodology, and by placing some revenue cycle managers into the hospital systems' existing processes to augment its revenue cycle operations."

Enforcement arose from a July 2011 incident in Minneapolis, in which "an Accretive Health laptop containing over 600 files with more than 20 million pieces of information related to 23,000 patients was left in the locked passenger compartment of the employee's car and stolen." The FTC does not claim that any of the personal information is known to have been used by the thief or that any harm to any

Authors

Bruce L. McDonald
Senior Counsel
202.719.7014
bmcdonald@wiley.law

individual is traceable to the information theft.

The FTC's subsequent investigation identified several failures to "provide reasonable and appropriate security for consumers' personal information" that "taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access." Those alleged failures were (1) transporting laptops "in a manner that made them vulnerable to theft," (2) failure to restrict access to personal information "based on an employee's need for the information," (3) failure "to ensure" employees removed information "for which they no longer had a business need," and (4) using "consumers' personal information in training sessions" and "failing to ensure the information was removed from employees' computers following the training." Although the public FTC materials do not discuss these matters, presumably the Commission reasoned that the amount of information on the stolen laptop would have been less if the latter three "failures" had not occurred and the laptop would not have been so "vulnerable" to theft if it had not been in the "passenger compartment" of the vehicle where it could be seen by persons outside.

The Ordered Requirements

As a remedy, the proposed consent order will require Accretive Health, for 20 years, to maintain "a comprehensive information security program" containing "administrative, technical, and physical controls." It must designate employees "to coordinate and be accountable" for the program, identify "material internal and external risks," design and implement "reasonable safeguards to control the risks," regularly test and monitor "the effectiveness of the safeguards' key controls, systems and procedures," select capable "service providers" and require them "by contract" to "implement and maintain appropriate safeguards," and evaluate and adjust its information security program in light of the results of monitoring and testing, among other steps.

Thus, Accretive Health must maintain an elaborate security program and require that its service providers who receive personal information from it also maintain appropriate data security programs. Additionally, Accretive Health must initially and biennially thereafter obtain "an assessment and report from a qualified, objective, independent third party" certifying that it has a security program in place that provides the required protection and that it is "operating with sufficient effectiveness to provide reasonable assurance" that "the security, confidentiality, and integrity of sensitive consumer information has been protected." Furthermore, it must maintain specified types of records for specified periods and make a compliance report to the Commission.

HIPAA Not Mentioned

Our health care industry readers will recognize that Accretive Health has been a "business associate" of hospitals regulated under the Health Insurance Portability and Accountability Act (HIPAA) and presumably has been a party to business associate agreements that imposed a duty to maintain personal health information under "reasonable and appropriate" safeguards. Since September 2013, such business associates have been obliged to comply directly with the HIPAA Security Rule. Among the requirements imposed by the Health Information Technology for Economic and Clinical Health (HITECH) law is that subcontractors of business

associates must also maintain compliant data security programs (which appears to be reflected in the FTC order's "service providers" requirement noted above). What is striking is that none of the FTC materials accompanying the FTC's December 31 announcement contain any mention of HIPAA at all. For example, there is no indication that compliance with the HIPAA Security Rule will be deemed to establish compliance under the order. Rather, the complaint and associated materials are phrased to suggest that the FTC may and, in some instances, will enforce parallel data security requirements on entities regulated under HIPAA.

Interestingly, while the FTC complaint's allegations about the 2011 breach included that the laptop contained "sensitive" "health information" including "diagnostic information," the consent order's elaborate definition of "Personal information" does not expressly include such information. It does include 10 specified categories of information "from or about an individual" (name, address, email address, etc.). However, it then goes on to add "any information that is combined with any of those" identifiers. Thus, health information combined with the individual's name arguably would be covered by the order.

No Deception Claim

Typically, the FTC's data security enforcement initiatives have seized upon some representation about data security contained in the respondent's website or other promotional materials, and then claimed the fact of a breach means the representation was "deceptive" and, therefore, violative of Section 5 of the FTC Act. *See e. g.*, "The FTC Imposes Data Security Obligations on a Cord Blood Bank" (February 2013 *Privacy In Focus*) ("CBR takes steps to ensure that your information is treated securely"). Here, by contrast, the FTC makes no claim of deception. Rather, the complaint simply asserts that the alleged security failures "were and are an unfair act or practice in violation of Section 5(a)" of the FTC Act.

Thus, the case can in the future be cited by the FTC as precedent for a claim that any business has a duty under federal law to implement and maintain a data security program of the type it then deems appropriate.

Potential Other Motive

When Accretive Health was sued by the Minnesota Attorney General for alleged HIPAA violations leading to the 2011 laptop theft, there was concern that the suit might actually have been motivated by political opposition to Accretive Health's debt collection practices. *See* "Case Filed by Minnesota Raises Significant HIPAA Enforcement Issues" (April 2012 *Privacy In Focus*).

Minnesota thereafter forced a settlement under which Accretive Health agreed to stop doing business in Minnesota. The AG's press release focused not on data security but, instead, debt collection practices. According to the AG, "A hospital emergency room is a place of medical trauma and emotional suffering for patients and their families. It should be a solemn place, not a place for a financial shakedown of patients. It is good to close the door on this disturbing chapter in Minnesota health care." The release went on to assert that under the federal Emergency Medical Treatment and Active Labor Act, a hospital is supposed to examine a patient and, if an emergency exists, treat and stabilize the patient before seeking money," but noted that the Attorney General's office "does not have authority to enforce the federal law." Thus, the AG had used the leverage created by HIPAA enforcement jurisdiction to secure another goal.

Here also, some have wondered whether the theft of a laptop from an employee's locked car itself merited an attack by the FTC and imposition of two decades of burdensome regulation. The formal settlement documents (Complaint, Agreement Containing Consent Order, Commission Analysis) say nothing about matters other than data security. However, the FTC's press release notes cryptically that while the "staff is declining to recommend a Fair Debt Collection Practices Act case against Accretive at this time, the practice of attempting to collect payment for prior debts from consumers while they are seeking treatment in an emergency room or other medical facility raises serious concerns." This makes clear, in the context of the Minnesota action, that the FTC was pressuring Accretive Health on both fronts.

Thus, this FTC action, as postured by its press release, may well be seen as support for what the AG did and suggests that the FTC itself is prepared to inflate the importance of security incidents and use them to punish businesses engaged in practices it finds concerning.