CHICAGOLAWBULLETIN.COM

Serving Chicago's legal community for 160 years

THURSDAY, DECEMBER 31, 2015

Chicago Daily Law Bulletin®

Volume 161, No. 255

No harm, no foul? Defining FTC's authority over data security

Given the frequency of high-profile breaches, it's reasonable for companies and consumers to be not only fearful but also realistic (or some would say fatalistic) about data security. It's not a question of if a security lapse will occur, but when.

Even companies with robust security practices can't immunize themselves entirely against breaches. But vulnerability doesn't ultimately mean liability — at least in Federal Trade Commission enforcement actions. While the FTC is eager to exercise its prosecutorial authority under Section 5 of the Federal Trade Commission Act in the data security arena, two recent rulings show that the reach of that authority is still far from certain.

In August, the 3rd U.S. Circuit Court of Appeals affirmed that the FTC could pursue an enforcement action against a global hotel chain for its allegedly deficient security measures.

More recently, however, FTC Chief Administrative Law Judge D. Michael Chappell issued an exhaustively detailed ruling rejecting the commission's complaint against a now-defunct health-care company, finding that the FTC failed to produce credible evidence of the likelihood of any consumer injury and, therefore, could not support its claims.

Together, the two rulings suggest that while the FTC will keep pushing forward with its data security agenda, the FTC act is far from a "strict liability" regime, and the commission's authority is not unrestrained. The two rulings also lend themselves to some more specific takeaways.

Unreasonable data security practices can be "unfair or deceptive" acts giving rise to liability.

While the FTC has pursued scores of companies for cybersecurity breaches over the last several years, these actions almost invariably settle, and the 3rd Circuit's August ruling, affirming the FTC's authority under Section 5, is significant.

As background, the FTC filed suit after hackers broke into the hotel chain's computer systems on three separate occasions, stole customers' personal and financial information and caused millions of dollars in unauthorized charges.

Citing the absence of firewalls, weak passwords, access to the central system by third-party vendors and inadequate measures to detect breaches, the FTC charged that the company's security fell short of both the assurances in its own privacy policy and reasonable consumer expectations.

The U.S. District Court denied a motion to dismiss, and the company brought an interlocutory appeal challenging the FTC's authority to prosecute data breach claims under the FTC act and arguing that it had not had fair notice that its security practices could trigger liability.

The 3rd Circuit rejected the company's objections, expressing little doubt that the FTC could regulate cybersecurity. The court also found it immaterial that the actual harm was caused by hackers. The company could not (and did not) argue that the breaches were unforeseeable, particularly after it became aware of system vulnerabilities following the first breach. The court held that the allegations were sufficient to withstand a motion to dismiss and sent the case back to the district court.

The court also found that, under the relatively low standard for fair notice in the civil context, the company could "reasonably foresee that a court could construe its conduct as falling within the meaning of the statute." While the reasonableness of security measures is not one-size-fits-all, the first breach provided ample notice that of inadequacy of system security and the company's alleged failure to take appropriate measures thereafter was, in the court's words, "too little and too late."

The 3rd Circuit clarified that the FTC would have to prove three specific elements under Section 5(n):

- The company engaged in acts or practices that caused (or were likely to cause) substantial injury to consumers.
- Consumers could not reasonably avoid the substantial injury alleged.
- The injury was not outweighed by "countervailing benefits" to either consumers or to the company's competition.

Unfortunately, we won't see how the case fares on remand. The FTC and hotel chain settled the case in early December under terms requiring the company to establish a comprehensive information security program and undergo annual audits, but with no monetary payment or admission of liability.

Not every security gap will necessarily support a federal case.

While the administrative law judge decision rejecting the FTC's claims against now-defunct LabMD doesn't have deep value as precedent and could eventually be overturned on appeal, the ALJ's rejection of the case in full is a setback that may influence the FTC's actions in the future.

LabMD, which conducted mail-away clinical laboratory testing of specimen samples for various medical issues, maintained personal and insurance information associated with the samples. In 2008, Triversa, consulting on data protection, informed LabMD that it found a billing spreadsheet containing sensitive patient data on a peer-to-peer file-sharing network. After LabMD turned down its consulting services, Triversa informed the FTC about the file.

The FTC commenced an enforcement action contending that LabMD had failed to provide reasonable and appropriate security for sensitive patient data.

What followed was a morass of increasingly vituperative court challenges, additional lawsuits, a congressional committee investigation, whistleblower accusations related to testimony by a former Triversa employee and allegations of unethical conduct by FTC attorneys as well as the eventual closing of LabMD (and a tell-all book by its CEO).

In November, the ALJ rejected the FTC's claims in their entirety, ruling that Section 5(n) requires a showing that substantial injury to consumers is

PRIVACY, TECHNOLOGY AND LAW

Nerissa Coyle McGinn

Nerissa Coyle McGinn is a Chicago-based partner at Loeb & Loeb LLP. Her practice focuses on matters involving the convergence of advertising and promotions, emerging media, technology, and privacy law, as well as intellectual property law, focusing on trademark clearance and counseling. She can be reached at nmcginn@loeb.com.

Even companies with robust security practices can't immunize themselves entirely against breaches. But vulnerability doesn't ultimately mean liability — at least in Federal Trade Commission enforcement actions.

probable, not merely possible, absent evidence of actual consumer injury.

The ALJ was not convinced that the FTC could meet that standard, particularly given that the file was identified in 2008 yet no evidence existed that any consumers had been injured in the intervening years. Another influential factor was the suggestion that the computer hack that led to the alleged breach was actually conducted by the security firm as a means to induce the defendant to retain its services, not by hackers motivated to commit identity fraud.

As the ALJ warned: "If an unspecified, theoretical 'risk' of a future data breach and resulting identity theft were sufficient to prove unfair conduct in the instant case, then the clear requirement in Section 5(n) that injury be 'likely' would be vitiated." In sum, the FTC's approach would read the injury requirement out of the statute and any breach would be an unfair act.

No harm, no liability?

These two recent rulings (among others) suggest that courts will continue to struggle to define the contours of liability for hackings and data breaches — and that the outcome of these cases is highly dependent on the facts. A security hiccup doesn't necessarily mean that the FTC will come calling or, if it does, that an investigation will lead to liability.

That said, companies that become the subject of FTC investigations shouldn't take the LabMD case as a sign that they should avoid settlements and gamble on litigation.

While the courts continue to develop clearer lines for Section 5 liability, companies should, at a minimum, take the FTC's often-repeated advice — keep any promises you make about your privacy practices and ensure that the actual practices are reasonable and appropriate.