Proskauer

FTC Ramps up COVID-19 Activity After Improving its Data Security Enforcement Orders

Proskauer on Privacy Blog on **March 31, 2020**

With the spread of the novel coronavirus (COVID-19), cybersecurity criminals and scammers are ramping up their efforts to target vulnerable employers and workforces. The FTC announced today that since January they have received more than 7,800 fraud complaints from consumers related to the COVID-19 pandemic. But the FTC isn't slowing down either. Even with the FTC having to change its own procedures due to COVID-19, the FTC has been publishing guidance on COVID-19 scams and also sending out warning letters to sellers of false treatments.

This spate of new consumer protection threats from COVID-19 scams comes at critical time after the FTC recently revised its enforcement order policies. In early January, before COVID-19 had fully spread to the United States, Director of the Federal Trade Commission ("FTC") Bureau of Consumer Protection, Andrew Smith, published a blog post detailing how the FTC has been working to improve the clarity of FTC orders in data security cases over the past year.

As key background, the FTC has broad authority under Section 5 of the FTC Act to police "unfair or deceptive acts or practices in or affecting commerce…" 15 U.S.C. § 45(a). Under this authority, the FTC has become one of the primary regulators in the data privacy and security landscape in the U.S. The FTC takes action against companies that it believes put consumer data at risk. The FTC notes that its orders typically require companies to "implement a comprehensive information security program subject to a biennial outside assessment."

However, in 2018, the Eleventh Circuit held an FTC data security order against LabMD, Inc. unenforceable for vagueness. (*LabMD, Inc. v. FTC*, 894 F.3d 1221 (11th Cir. 2018)). In its cease and desist order, the FTC argued that LabMD failed to "implement reasonable security measures to protect the sensitive consumer information on its computer network." The Eleventh Circuit held that the order did not "instruct LabMD to stop committing a specific act or practice. Rather, it commands LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness." The Eleventh Circuit vacated the order (importantly, the appeals court did not rule that inadequate data security practices cannot be regulated under Section 5 of the FTC Act).

The FTC's blog post specifically cites the LabMD case as a learning opportunity, after which the FTC made improvements to its data security orders. One settlement from the past year is instructive on this point. In July 2019, the FTC (along with the Consumer Financial Protection Bureau (CFPB) and 50 state attorneys general) settled with consumer credit reporting agency Equifax Inc. over a 2017 mega breach that affected 147 million individuals. Beyond the sizeable financial penalty, the FTC outlined Equifax's myriad of basic security failures that led to the breach and also required Equifax to take several concrete measures in shoring up its information security program (e.g., annually assess patch management protocols and associated risks, ensure vendors implement security safeguards, and obtain certifications from the Board attesting compliance with the settlement terms).

The FTC's blog post claims that improvements like these are reflected in seven data security-related orders it announced during 2019. In particular, the FTC has made three improvements to its orders:

1. **Specificity:** While the FTC still mandates comprehensive security programs, it will endeavor to list specific improvements that will need to be made based on the alleged security failures, such as "yearly employee training, access controls, monitoring systems for data security incidents, patch management systems, and encryption." An example of more specific measures was found in the April 2019 settlement with i-Dressup and Clixsense, wherein the FTC included explicit language which prohibits each company from "making misrepresentations to the third parties conducting assessments of their data security programs." The FTC added that "these new requirements will provide greater assurances that

consumers' data will be protected going forward."

2. **Increased third-party assessor accountability:** The FTC will now specify in its orders that it has the authority to approve (and re-approve) assessors every two years. Orders will now require assessors to support conclusions about data security programs with evidence, which must be retained and provided to the FTC upon request. For example, in an order against Retina-X in October 2019, the FTC required Retina-X to disclose all materials facts to the third party assessor and provide or otherwise make available all information in their possession and control that is relevant to the assessment for which there is no claim of privilege.
3. **Elevation of data security to C-Suite and Board level:** The FTC's orders may now require senior executives to provide annual certifications of compliance with the updated information security programs to the FTC. For example, in the Clixsense and i-Dressup orders, the FTC ordered each company to have a senior officer provide annual certifications of privacy compliance to the FTC.These improvements detail what we can expect to see in data security orders going forward, but the FTC could certainly adjust its approach depending on the circumstances of each action. Thus, in the wake of the *LabMD* ruling, the FTC's recalibration of its strategy will only add to the growing body of privacy and data security orders the FTC has issued over the years, offering further guidance to companies on "reasonable" data security practices and giving the agency more confidence its orders will ultimately be enforceable. It remains to be seen whether the FTC will implement its strategy against perpetrators of COVID-19 scams, but the increase in fraud against consumers has certainly caught the attention of agency.

Improving the specificity of its data security-related order may benefit all parties involved, because the FTC will presumably lay out in more detail what steps the entity needs to take to comply, as opposed to the previous vaguer standard of requiring entities to "implement reasonable security measures." The latter two improvements give FTC orders more bite. Entities will have to take care in managing quality third-party assessors, because now the FTC will be scrutinizing not only the content of the assessment, but also the level of evidence gathered by assessments. Failure to obtain an industry-standard assessor may invite more scrutiny from the FTC. Additionally, senior executives will now have to review and certify their data security compliance under oath. The FTC blog post cites a study claiming that having a Chief Information Security Officer with access to the Board within a company may correlate to a 35% decrease in probability of breaches.

These improvements detail what we can expect to see in data security orders going forward, but the FTC could certainly adjust its approach depending on the circumstances of each action. Thus, in the wake of the *LabMD* ruling, the FTC's recalibration of its strategy will only add to the growing body of privacy and data security orders the FTC has issued over the years, offering further guidance to companies on "reasonable" data security practices and giving the agency more confidence its orders will ultimately be enforceable. It remains to be seen whether the FTC will implement its strategy against perpetrators of COVID-19 scams, but the increase in fraud against consumers has certainly caught the attention of agency.

Proskauer's cross-disciplinary, cross-jurisdictional Coronavirus Response Team is focused on supporting and addressing client concerns. Visit our Coronavirus Resource Center for guidance on risk management measures, practical steps businesses can take and resources to help manage ongoing operations.

View Original