FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

New and improved FTC data security orders: Better guidance for companies, better protection for consumers

Share This Page

Andrew Smith, Director, FTC Bureau of Consumer Protection
Jan 6, 2020

TAGS: Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Data Security

When Chairman Simons and I arrived at the FTC, one of our first priorities was to strengthen the FTC's orders in data security cases. We've already made three major changes that improve data security practices and provide greater deterrence, within the bounds of our existing authority.

Since the early 2000s, our data security orders had contained fairly standard language. For example, these orders typically required a company to implement a comprehensive information security program subject to a biennial outside assessment. As part of the FTC's Hearings on Competition and Consumer Protection in the 21st Century, we held a hearing in December 2018 that specifically considered how we might improve our data security orders. We were also mindful of the 11th Circuit's 2018 LabMD decision, which struck down an FTC data security order as unenforceably vague.

Based on this learning, in 2019 the FTC made significant improvements to its data security orders. These improvements are reflected in seven orders announced this year against an array of diverse companies: ClixSense (pay-to-click survey company), i-Dressup (online games for kids), DealerBuilt (car dealer software provider), D-Link (Internet-connected routers and cameras), Equifax (credit bureau), Retina-X (monitoring app), and Infotrax (service provider for multilevel marketers).

The improvements fall into three categories.

First, the orders are more specific. They continue to require that the company implement a comprehensive, process-based data security program, and they require the company to implement specific safeguards to address the problems alleged in the complaint. Examples have included yearly employee training, access controls, monitoring systems for data security incidents, patch management systems, and encryption. These requirements not only make the FTC's expectations clearer to companies, but also improve order enforceability.

Second, the orders increase third-party assessor accountability. We still rely on outside assessors to review the comprehensive data security program required by the orders, and now we require even more rigor in these assessments. For example, the orders clearly and specifically require assessors to identify evidence to support their conclusions,

including independent sampling, employee interviews, and document review. The assessors must retain documents related to the assessment, and cannot refuse to provide those documents to the FTC on the basis of certain privileges. When FTC staff can access working papers and other materials, they are better able to investigate compliance and enforce orders. Perhaps most importantly, our new orders give us the authority to approve and re-approve assessors every two years. If an assessor falls down on the job, we will withhold approval and force the company to hire a different assessor.

Third, the orders elevate data security considerations to the C-Suite and Board level. For example, every year companies must now present their Board or similar governing body with their written information security program — and, notably, senior officers must now provide annual certifications of compliance to the FTC. This will force senior managers to gather detailed information about the company's information security program, so they can personally corroborate compliance with an order's key provisions each year. Requiring these kinds of certifications under oath has been an effective compliance mechanism under other legal regimes (e.g., securities law), and we expect it will likewise ensure better year-round governance and controls regarding FTC data security orders.

Regarding that third point, research suggests the FTC's efforts to improve corporate governance on data security issues are timely and well founded. Boards are becoming increasingly involved in cybersecurity governance, as demonstrated by surveys of practitioners[1] and the growth of literature aimed at educating board members on cybersecurity.[2] Some studies suggest that Board attention to data security decisions can dramatically improve data safeguarding. For example, one study found a 35% decrease in the probability of information security breaches when companies include the Chief Information Security Officer (or equivalent) in the top management team and the CISO has access to the board.[3] Our new orders are consistent with this research: they create additional incentives for high-level oversight of, and appropriate attention to, data security.[4]

---

[1] See, e.g., Protiviti, *Vendor Risk Management Benchmark Study: Running Hard to Stay in Place* (2019), https://www.protiviti.com/sites/default/files/2019-vendor-risk-management-benchmark-study-sharedassessments-protiviti.pdf (noting that the number of boards that are highly engaged in vendor risk management issues has increased in the last three years, from 26 percent to 32 percent).

[2] *Navigating the Digital Age, The Definitive Cybersecurity Guide for Directors and Officers* (Second Edition), Palo Alto Networks & NYSE, https://www.securityroundtable.org/navigating-the-digital-age-2nd-edition.

[3] See Kwon, J., Ulmer, J., & Wang T., *The Association between Top Management Involvement and Compensation and Information Security Breaches*, Journal of Information Systems, Vol. 27, No. 1 (Spring 2013), pp. 219-236 ("…the involvement of an IT executive decreases the probability of information security breach reports by about 35 percent…").

[4] See Higgs, J., Pinsker, R., Smith, T., & Young, G., *The Relationship between Board-Level Technology Committees and Reported Security Breaches*, Journal of Information Systems (Fall 2016), Vol. 30, No. 3, pp. 79-98 ("[A]s a technology committee becomes more established, its firm is not as likely to be breached. To obtain further evidence on the perceived value of a technology committee, this study uses a returns analysis and finds that the presence of a technology committee mitigates the negative abnormal stock returns arising from external breaches.").

ftc.gov