ALSTON & BIRD

WWW.ALSTON.COM

CYBER ALERT ■

JANUARY 17, 2020

FTC Blog Post Highlights Efforts to Strengthen Data Security Orders

By Kathleen Benway and Emily Poole

On January 6, 2020, the Federal Trade Commission's (FTC) Bureau of Consumer Protection Director Andrew Smith published a blog post summarizing the agency's "new and improved FTC data security orders," as part of its efforts to provide "better guidance for companies" and "better protection for consumers." Smith noted that strengthening the FTC's orders in data security cases was one of his and Chairman Joe Simons's first priorities. Smith highlights three primary areas where the agency strengthened order provisions over the past year:

- Increased specificity.
- Increased accountability of third-party assessors.
- Improved corporate governance on data security issues.

Each category of improvement is reflected in seven data security orders issued by the FTC over the past year against companies in a range of industries: 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).

Companies would be well advised to review these orders closely because they send a clear signal of what the FTC expects an adequate data security program to include.

Background

The FTC's effort to strengthen its orders followed and was likely influenced by the 11th Circuit's 2018 *LabMD* decision, which declared that the FTC's data security order against LabMD was overly vague and unenforceable and found that the order would require LabMD's data security program "to meet an indeterminable standard of reasonableness." Before the *LabMD* decision, data security orders were typically modeled on the requirements of the Gramm–Leach–Bliley Safeguards Rule, which applies to financial institutions under FTC jurisdiction.

The Safeguards Rule requires those institutions to develop, implement, and maintain a comprehensive information security program that meets broad objectives, but does not specify required elements for the programs. In March 2019, the FTC proposed changes to the Safeguards Rule that would include more specificity, such as requiring specific controls to secure customers' information, including encryption and multifactor authentication. The proposed changes are based primarily on the cybersecurity regulations issued by the New York Department of Financial Services, 23 NYCRR 500, and the insurance data security model law issued by the National Association of Insurance Commissioners. The public comment period on the proposed regulations has closed, but the agency has not yet issued final regulations, which could include changes to the proposed regulations based on the comments.

In addition, as part of its series of hearings, "Competition and Consumer Protection in the 21st Century," the FTC held a hearing in December 2018 on its data security program and welcomed comments on how the FTC might improve its data security enforcement orders, but it has not yet issued a report or taken other public action following those hearings.

Strengthened Data Security Orders

As noted above, Smith identified three general categories of improvements that the FTC has made to its 2019 data security orders: increased specificity in order provisions, increased accountability of third-party assessors, and improved corporate governance on data security issues.

Specificity

Smith notes that while the FTC's orders continue to generally require companies to implement a comprehensive information security program, enforcement orders now include more detailed requirements for the implementation of specific information security safeguards. Recent examples cited in the blog post include requirements to implement employee training (DealerBuilt and Equifax orders), access controls (DealerBuilt, Equifax, and Retina-X orders), monitoring systems for data security incidents (InfoTrax order), patch management systems (Equifax order), and encryption (DealerBuilt, Equifax, Retina-X, and InfoTrax orders).

Third-party assessor accountability for post-enforcement reporting

The FTC's recent orders contain more rigorous requirements for the third-party assessors that review an entity's data security program as part of an FTC enforcement order. For example, assessors are required to identify specific supporting evidence for their conclusions, and documentation generated by assessors as part of the review cannot be withheld from the FTC on the basis of certain privileges, such as attorney-client privilege, attorney work product, or proprietary or trade secrets (DealerBuilt, D-Link, Equifax, Retina-X, and InfoTrax orders). Moreover, the FTC's orders allow the FTC to reapprove qualified assessors every two years (DealerBuilt, D-Link, Equifax, Retina-X, and InfoTrax orders).

C-Suite and board involvement

The FTC's recent orders also specify that certain data security considerations must be elevated to a company's senior executives and/or board. Citing to research that reflects the positive correlation between a board's security awareness and the overall strength of a company's cybersecurity program, the FTC's blog post highlights certain steps that companies may be required to take, such as presenting the board with the company's written information security program (DealerBuilt, D-Link, Equifax, Retina-X, and InfoTrax orders) or providing the FTC with an annual certification of compliance from the company's senior officers (included in all seven orders).

Takeaways

Smith's blog post is the latest example of the FTC's evolving approach to data security enforcement. Following the *LabMD* decision, the FTC has publicly committed to increasing the amount of detail in its data security enforcement orders, and companies would be well advised to view these additional details as clear indicators of what the FTC views as reasonable data security. In addition, the specific measures highlighted by the FTC enforcement orders may affect what other regulators, including state attorneys general, view as a reasonable information security program. While there is no one-size-fits-all approach to cybersecurity, and not every measure specified in the enforcement orders may make sense for every company, the FTC orders illustrate the FTC's growing areas of focus, and they therefore provide a useful guidepost for companies as they build out and develop their information security programs.

Cybersecurity Preparedness & Response Team Co-Chairs

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com

www.alstonsecurity.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, TX 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 5th Floor, Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 950 Page Mill Road ■ Palo Alto, California USA, 94304-1012 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333