Akin®

Recent FTC Settlements Highlight Risks of Flawed Information Security Practices and Related Representations

Jul 22, 2019

Reading Time : **5 min**

By: Natasha G. Kohne

In April 2019, when the Commission announced its case against ClixSense, it noted its intention to strengthen its orders in data security cases. (FTC Statement, FTC Matter Nos. 1723002 & 1723003 (Apr. 24, 2019).) In particular, its intentions, where appropriate, are to incorporate into its data security orders new requirements (e.g., a senior officer must provide annual certifications of compliance to the FTC) and to expand existing requirements (e.g., third-party assessors must examine a company's entire data security program and provide specific evidence for findings). The ClixSense and D-Link settlements are examples of this more stringent approach in practice.

The ClixSense Complaint

ClixSense is an online rewards website. The Commission brought charges against James V. Grago, Jr. as ClixSense's sole owner.

ClixSense collects individuals' personal information at the time they sign up for its rewards website. In 2016, ClixSense reported a data breach that affected the data of some 6.6 million consumers. The data of at least 2.7 million consumers was apparently sold online as a result.

In the aftermath of the breach, the Commission filed a complaint against ClixSense and its owner Grago for alleged violations of Section 5 of the FTC Act, including: (1) deceptive practices in the form of misrepresentations about encryption, (2) deceptive practices in the form of misrepresentations about using the latest security techniques, and (3) unfair practices in the form of failure to employ reasonable security practices. (ClixSense Compl.)

The Commission claimed that ClixSense did not employ reasonable security given that it: failed to limit access between computers on its network, as well as between ClixSense's computers and the Internet; let employees store plain text user credentials in personal email accounts on ClixSense's laptops; failed to change default login credentials for third-party company network resources; and maintained consumers' personal information in plain text on networks and devices. The Commission alleged that these failures could have been fixed with basic measures and that, by failing to do so, ClixSense facilitated hackers' access to consumers' data.

To settle these claims, Grago agreed not to misrepresent the extent to which any company he controls protects the personal information it collects. He also agreed that if any company he controls collects or maintains personal information he will implement a comprehensive information security program, obtain biennial assessments of that program by an independent third party for 20 years, is prohibited from making misrepresentations to the third party performing the assessment, and will annually certify its compliance with the Commission.

The D-Link Complaint

D-Link is a hardware manufacturer that develops and markets smart home devices including routers and IP cameras. Due to the company's alleged security failures, thousands of its routers and cameras were vulnerable to a range of attacks. Attackers utilized those vulnerabilities to access consumers' home and office networks and sensitive personal information. At the same, D-Link promoted its products as "easy to secure" and as having "the best possible encryption."

The Commission brought an enforcement action against D-Link in January 2017, after the vulnerabilities came to light. (D-Link Compl.) The Commission claimed that D-Link violated Section 5 of the FTC Act by engaging in: (1) unfair acts or practices through its failure to take reasonable steps to secure the software for its products; (2) deceptive acts through its misrepresentations in its security policies concerning the reasonableness of its actual data security practices; (3) deceptive acts through its misrepresentations in its promotional materials about the security of its routers and its IP cameras; and (4) deceptive acts through its misrepresentations in its routers' and IP cameras' user interface concerning their security.

The Commission's complaint alleged that D-Link's protection of its routers and cameras was unreasonable because it: failed to address easily preventable flaws such as saving device passwords and other sensitive data in plain text; improperly handled the security key used by

the manufacturer to sign software, resulting in the key's public exposure for a six-month period; and inappropriately stored users' mobile app login credentials in plain text on users' mobile devices. According to the Commission, many of these vulnerabilities could have been mitigated using free software or basic protocols to restrict and oversee access to sensitive information.

To settle these claims, D-Link agreed to implement a comprehensive software security program, including specific measures to protect its routers and IP camera devices. It also agreed to biennial assessments by a third-party for a 10-year period following an initial assessment. The third-party assessor must keep all documents it relies on for its assessment for five years and to provide them to the Commission upon request. In another sign of the Commission's more serious approach, the third party assessor is also required to identify specific evidence for its findings. The Commission is empowered to approve the third-party assessor D-Link selects.

In an interesting development, the Commission provided D-Link the option of meeting its requirement of adopting a comprehensive security program by ensuring its program complies with the secure product development standard set by the International Electrotechnical Commission (IEC). The third-party assessor D-Link selects would have to certify D-Link's compliance with the IEC standard. D-Link cannot take advantage of this option if it provides any misleading or false information during its assessments or audits.

Moving Forward – Expect Enhanced Oversight in Data Security Cases

The oversight terms in the ClixSense and D-Link settlements confirm the Commission's willingness to utilize new and expanded requirements in its data security orders. Companies should anticipate that in future data security cases the Commission may advocate for terms such as: (1) Commission approval of third-party assessors; (2) more expansive assessments by third-party assessors to include review of companies' revised security programs, assessment of the programs' implementation and identification of any gaps or weaknesses;[1] (3) prohibitions against companies misrepresenting any material fact to third-party assessors; (4) requirement that a senior officer certify the company's compliance to the Commission; or (5) requirement that the company notify the Commission of any unauthorized access to consumers' personal information. The best way to defend against these terms is to take steps now to ensure your information security program adequately meets your needs and avoid making any misrepresentation of your security procedures or program.

[1] In the past, third-party assessors were required only to identify specific safeguards employed by the company, explain the utility of the safeguards in protecting users' personal data and certify that the safeguards operate with sufficient effectiveness.

Categories

Cybersecurity & Information Security | FTC

© 2025 Akin Gump Strauss Hauer & Feld LLP. All rights reserved. Attorney advertising. This document is distributed for informational use only; it does not constitute legal advice and should not be used as such. Prior results do not guarantee a similar outcome. Akin is the practicing name of Akin Gump LLP, a New York limited liability partnership authorized and regulated by the Solicitors Regulation Authority under number 267321. A list of the partners is available for inspection at Eighth Floor, Ten Bishops Square, London E1 6EG. For more information about Akin Gump LLP, Akin Gump Strauss Hauer & Feld LLP and other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.