

Client Alert

An informational newsletter from Goodwin Procter LLP

FTC Consent Decree Outlines Security Minimums for Companies Handling Sensitive Consumer Data

Recently, the Federal Trade Commission (“FTC”) entered into yet another consent decree with a company regarding its information security practices. This time, the FTC took issue with the practices of retailer Life is Good. This enforcement action may serve as a roadmap for other companies handling sensitive consumer data on a regular basis. The case should also serve as a caution to any company that makes generic claims in its privacy policy about the security of the information it collects from its customers.

On its website, Life is Good, Inc. claimed:

“We are committed to maintaining our customers’ privacy. We collect and store information you share with us – name, address, credit card and phone numbers along with information about products and services you request. *All information is kept in a secure file* and used to tailor our communications with you.”

The FTC charged, however, that contrary to the above highlighted language, Life is Good “failed to provide reasonable and appropriate security for the sensitive consumer information stored on its network.”

Specifically, the FTC alleged that customer credit card information was stored “indefinitely, in clear, readable text” on Life is Good’s network, along with credit card security codes; that Life is Good had failed to implement certain low-cost and readily available measures to protect against SQL and similar attacks; and that Life is Good failed to take measures to monitor its network and detect unauthorized access. Consequently, according to the FTC, a hacker was able to use SQL injection attacks to access Life is Good’s network and steal the credit card information of thousands of customers.

The consent decree requires Life is Good to establish a data security program which includes administrative, technical and physical safeguards similar to those outlined in the FTC’s Safeguards Rule, which applies to companies covered by the Gramm-Leach-Bliley Act. The security program must be specifically tailored to the retailer’s size and the sensitivity of the data it handles. Specifically, the FTC requires that Life is Good:

- Dedicate one or more employees to the coordination of a security program;
- Identify internal and external risks to information security and assess the safeguards now in place;
- Establish safeguards to protect against the risks identified in the assessment, and the means to monitor their effectiveness;
- Evaluate and adjust the security program as necessary to reflect the results of monitoring, material changes to the company's structure or operations, and "other circumstances that may impact the effectiveness" of the security program;
- Develop reasonable steps to retain service providers capable of adequately protecting customer information they receive from Life is Good, and require those service providers by contract to implement and maintain safeguards; and
- Maintain its books and records in a way that facilitates FTC monitoring of its compliance with the consent decree.

In addition, Life is Good faces the burdensome and costly requirement of obtaining an independent, third-party auditor to review and assess its security measures once every two years for the next twenty years.

As in other cases, including those involving retailers Guess.com, DSW, and BJ's Wholesale Club, the FTC's complaint against Life is Good was grounded not in any specific privacy or financial services regulation, but in the agency's more generic jurisdiction over unfair or deceptive trade practices under the FTC Act. The agency took specific issue with the claims made by Life is Good in its privacy policy, and in its consent decree the FTC ordered that as part of the settlement, Life is Good "shall not misrepresent in any manner, expressly or by implication, the extent to which respondents maintain and protect the privacy, confidentiality, or integrity of any personal information collected from or about consumers." This case is similar in that regard to the 2003 case the agency brought against Guess.com, which also alleged in the wake of an SQL attack that the retailer's online privacy policy misled consumers.

Well-intentioned privacy policies like the one that appeared on the Life is Good website have become standard in Internet commerce. Companies that post and rely on them, however, must take a long look both at the language of their privacy policy and at the actual security of the consumer data they collect, and ensure that their security measures stack up. It is also important to renew that analysis from time to time, so as to protect against what the FTC often refers to as "commonly known" attacks or vulnerabilities.

In the FTC's 2005 complaints against DSW and BJ's, it took no such issue with those retailers' privacy policies, but simply alleged that their inadequate data safeguards – which the agency deemed neither "reasonable" nor "appropriate" – were inherently unfair to consumers. Whether or not the actual language of a

company's privacy policy makes promises on which it fails to deliver, the agency has demonstrated little tolerance for what it perceives as slack security by retailers.

At a minimum, any company that handles sensitive customer data should have in place safeguards at the three levels cited by the FTC: administrative, technical and physical. Employees should be trained in the secure handling of consumer information. Appropriate network systems and software for information processing, storage, transmission and disposal should be in place. In addition, companies should install systems or mechanisms for detecting intrusions and responding to attacks. These measures may be reasonably tailored to the size of the company and the sensitivity of the data it handles, but they should represent the full spectrum of protections the FTC will expect from any company which handles private customer information, whether the company makes claims to protect its customers effectively or not.

If you have any questions about the issues raised in this alert and their potential implications for your business, please contact:

Jacqueline Klosek	jklosek@goodwinprocter.com	212.459.7464
Deborah S. Birnbach	dbirnbach@goodwinprocter.com	617.570.1339
Agnes Bundy Scanlan	abundyscanlan@goodwinprocter.com	617.570.1161

Kirstie M. Baker contributed to the preparation of this alert.

Full access to all articles on privacy and data security prepared by Goodwin Procter is available [here](#).

Full access to all articles prepared by Goodwin Procter is available [here](#).

This publication, which may be considered advertising under the ethical rules of certain jurisdictions, is provided with the understanding that it does not constitute the rendering of legal advice or other professional advice by Goodwin Procter LLP or its attorneys. Additionally, the foregoing discussion does not constitute tax advice. Any discussion of tax matters contained in this publication is not intended or written to be used, and cannot be used, for the purpose of avoiding penalties under the Internal Revenue Code or promoting, marketing or recommending to another party any transaction or matter. © 2008 Goodwin Procter LLP. All rights reserved.