Document hosted at JDSUPRA
http://www.jdsupra.com/post/DocumentViewer.aspx?fid=d30c0e67-25e7-402e-8ea8-949aeca2eca3

ANYTHING YOU SAY WILL BE USED AGAINST YOU

by Ron Gorsline, Blake Sims, Justin Hosie, and Clint Heyworth
Chambliss, Bahner & Stophel, P.C.

Most financial service providers are now well aware of their consumer-privacy duties under the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and various regulations under those laws. However, many still don't realize *compliance* means much more than just posting a privacy policy. Financial service providers must implement and actually follow written policies for sensitive information and then provide an accurate copy to consumers.

Unfortunately, many financial service providers publish websites assuring consumers that sensitive information will be secure, regardless of their actual policies. Typical assurances state:

- Patented security features are automatically provided for free
- Safer than sending information through the mail
- You can be confident that your accounts will be secure and protected
- You can be sure that your accounts are secure
- You are protected from any unauthorized activity on your accounts
- We use encryption technology, such as Secure Socket Layer (SSL), to prevent unauthorized access to data
- Special security features

Before casually making these representations on your website, you should remember one key mantra: Do what you say, and say what you do. Various federal agencies have been using their enforcement powers to echo this mantra for years.

One of the most notorious and longstanding examples involves a 2002 Federal Trade Commission (FTC) action against **Microsoft**. In its complaint, the FTC charged Microsoft with making false security and privacy promises about its *Passport* Web services. Passport collected and stored credit card numbers, allowing consumers to use the stored information for certain Web purchases.

According to the FTC, Microsoft misrepresented that its services achieved "a high level of Web security." Microsoft told consumers that Passport would "prevent unauthorized access," and that information would be "protected by powerful online security and a strict privacy policy." The FTC also alleged Microsoft collected more information than it told consumers it collected. In other words, the company said one thing to the customers, but actually did something else.

Commenting on the incident, then FTC Chairman Timothy J. Muris told reporters:

> *Microsoft made a number of misrepresentations. Privacy and security promises must be kept. It's good business. It's the law. And we'll take action against companies that don't keep their promises.*

© September 15, 2008

Document hosted at JDSUPRA
http://www.jdsupra.com/post/DocumentViewer.aspx?fid=d30c0e67-25e7-402e-8ea8-949aeca2eca3

The 2002 FTC action involving Microsoft was not the first time a federal agency punished a financial service provider for misleading security statements, and it won't be the last. Earlier this year, the FTC filed a complaint against Goal Financial alleging the company misrepresented its security practices. This was the FTC's 17th case against companies handling sensitive consumer information, challenging their data security practices.

In this matter, the FTC alleged Goal Financial violated federal law by failing to provide reasonable and appropriate security for sensitive personal information. Specifically, the FTC alleged violations of its Safeguards Rule, the Privacy Rule, and the FTC Act for providing customers with a privacy policy that contained false or misleading statements, and for falsely representing that it implements reasonable and appropriate measures to protect personal information.

Goal Financial collected personal information and had security failures resulting in employees transferring consumer information to third parties without authorization. One employee even sold hard drives that held information about consumers in clear text.

The FTC's consent orders with Microsoft and Goal Financial prohibited future misrepresentations, mandated comprehensive information security programs, and mandated independent security program certification. Once the FTC issues a final consent order, it carries the force of law with respect to future actions. Each violation can result in an $11,000 civil penalty.

To help prevent your company from becoming a target of the federal regulators:

- Don't overstate the level of security you provide;
- Implement and follow the required privacy policies;
- Regularly review and update your security standards and policies; and
- Ensure the policies are accurate: "Do what you say, say what you do."

Numerous laws, regulations, guidelines, and standards apply which are not addressed by this article. For example, privacy matters are also addressed in the rules related to Disposal of Consumer Report Information and Records, the Children's Online Privacy Protection Act of 1998, the Children's Online Privacy Protection Rule, the policies established by previous unfairness and deception actions related to the FTC's privacy initiatives, other enforcement actions related to the Safeguards Rule, and enforcement actions related to pretexting.

The FTC and the federal banking agencies continually investigate potential actions concerning data security and privacy matters. Also, keep in mind that most states now have their own laws concerning the privacy and safeguarding of personal information, as well as data breaches. Always seek the advice of counsel before drafting, preparing, and training employees regarding privacy policies, and before publishing a privacy policy on your website. Always remember, "Say what you do and do what you say."

About the Authors

Ron Gorsline, Blake Sims, Justin Hosie, and Clint Heyworth are attorneys at Chambliss, Bahner & Stophel P.C. in Chattanooga, TN; <cbslawfirm.com>, (423) 756-3000, consumerfinance@cbslawfirm.com

This article is intended to be informational and does not provide legal advice nor create an attorney-client relationship. Laws are constantly changing, and each federal law, state law, and regulation should be checked by legal counsel for the most current version and before acting on this information. Certification as a Specialist in Consumer Finance Law by the Tennessee Commission on Continuing Legal Education and Specialization is not currently available. None of the attorneys listed in this communication are certified in any area of specialization.

© September 15, 2008