SHUMAKER
Shumaker, Loop & Kendrick, LLP

Client Alert

Business Information for
Clients and Friends of
Shumaker, Loop & Kendrick, LLP

September 20, 2017


Taaffe


Cherry


Malone


Wyant Jr.


Halpern

FTC Gives Guidance in Slaying the Data Breach Dragon

Michael S. Taaffe, Partner | mtaaffe@slk-law.com | 941.364.2720
Douglas A. Cherry, Partner | dcherry@slk-law.com | 941.364.2738
Jarrod J. Malone, Partner | jmalone@slk-law.com | 941.364.2715
David L. Wyant Jr., Associate | dwyant@slk-law.com | 941.364.2766
Jeremy M. Halpern, Associate | jhalpern@slk-law.com | 941.366.6660

The FTC has recently provided specific guidance on what it considers appropriate data breach protection activity by financial institutions. Such guidance came by virtue of a proposed consent order, dated August 29, 2017, specifically involving a data breach by TaxSlayer, LLC.

The data breach started with a hacker who obtained a list of usernames and passwords that were stolen from other websites. Since many people reuse the same username and password for multiple websites, the hacker was able to use these login credentials and gain access to thousands of accounts on TaxSlayer's website. After gaining access to the accounts, the hacker was able to remove the confidential financial information provided by over 8,000 of TaxSlayer's customers and file an unknown number of fraudulent tax returns. This obviously caused significant issues for each of TaxSlayer's customers affected by this data breach.

In its findings, the FTC found specific violations of the privacy and safeguard rules of the Gramm-Leach-Bliley Act (hereinafter "GLBA"). The proposed consent order contained a lengthy list of provisions designed to prevent TaxSlayer from engaging in similar practices that would result in a data breach. The order places a significant burden on TaxSlayer's future compliance and reporting obligations to the FTC over a 20 year period. It is likely the FTC will follow this same format for any other financial institution it finds in violation of the GLBA.

Most importantly, the FTC published four specific guidelines on its blog which financial institutions should follow. Financial institutions should strongly consider these four guidelines in an effort to avoid TaxSlayer's fate. These guidelines include:

1. Use of a broad definition of "financial institutions" which can include tax preparers, CPA firms, and the like.
2. Delivery of privacy notices must be conspicuous, and must be actually delivered to the client—a link to the privacy notice on a homepage is insufficient. In this regard, the FTC has provided a model notice.
3. Use of appropriate authentication procedures which may even require a multi-factor authentication process.
4. Once a written information security program is in place, it needs to be monitored, tested, and updated on a regular basis.

For more information on how to comply with the FTC's new detailed guidance on privacy requirements under GLBA, please contact the Shumaker attorneys listed above.

www.slk-law.com