SCOTT IP
TECHNOLOGY ATTORNEYS

Complying with the GLBA Privacy and Safeguards Rules

By Robert J. Scott and Adam W. Vanek

"It is the policy of Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[1]

I. INTRODUCTION.

In 2006 an estimated 9 million American adults were the victims of identity fraud at a total cost of $56.6 billion.[2] There are a number of legislative efforts designed to protect the privacy, security, and confidentiality of customer data. One such law, the Gramm–Leach–Bliley Act (the "GLBA"), also known as the Financial Services Modernization Act of 1999, effectively repealed the Banking Act of 1933 and amended the Bank Holding Company Act of 1956.

The GLBA requires financial institutions to protect themselves against unauthorized access, anticipate security risks, and safeguard a consumer's nonpublic information, it also prohibits individuals and companies from obtaining consumer information using false representations.[3] The GLBA charged the Federal Trade Commission (the "FTC"), and other government agencies that regulate financial institutions, with the duty to enforce, carry out, and implement the GLBA.

The GLBA separates individual privacy protection into three principal categories: (1) the Financial Privacy Rule; (2) the Safeguards Rule; and (3) Pretexting Provisions.[4] The Financial Privacy Rule and the Safeguards Rule apply to "financial institutions," which include banks, securities firms, insurance companies and other companies providing financial products and services to consumers. The Pretexting Provisions apply to individuals and companies, who obtain or attempt to obtain personal financial information under false pretenses.

This article provides a brief overview of the GLBA and a financial institution's obligations under the Financial Privacy and Safeguards Rules. This article outlines a financial institution's notice and disclosure requirements. It also outlines the importance of conducting a thorough risk assessment and implementing a comprehensive information security program.

II. THE FINANCIAL PRIVACY RULE.

The Financial Privacy Rule (the "Privacy Rule") applies to financial institutions that collect and receive nonpublic personal information from consumers, and requires them to disclose and provide a written notice of its policies and procedures to its customers, stating how the customer's nonpublic personal information is protected and shared.[5] The privacy notice must also provide consumers with a reasonable opportunity to "opt–out" of any information sharing, if required by statute.[6]

The term "financial institution" is defined as any business that is significantly engaged in activities that are financial in nature,[7] as well as companies that receive information that is "incidental"[8] or "complementary"[9] to such financial activity. Financial activities include, but are not limited to lending, exchanging, transferring, investing for others, safeguarding money or securities, providing financial, investment, or economic advice, underwriting, dealing in or making a market in securities, non–bank mortgage lending, real estate settlement services, credit counseling, check–cashing services and individual tax return services.[10]

A. Notice Requirements.

1. Clear and Conspicuous.

First and foremost the privacy notice must be "clear and conspicuous."[11] This means that the notice must be understandable and designed to call attention to the nature and significance of the information within the notice.[12] For