Complying with the GLBA Privacy and Safeguards Rules

By Robert J. Scott and Adam W. Vanek

SCOTT IP
TECHNOLOGY ATTORNEYS

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the Gramm–Leach–Bliley Act (the "GLBA"), also known as the Financial Services Modernization Act of 1999, effectively repealed the Banking Act of 1933 and amended the Bank Holding Company Act of 1956.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

example, the notice must use easily readable font, present the information in clear, concise sentences, using definite, everyday words, and short, explanatory sentences whenever possible.[13] Similarly, any changes in the privacy policy must be clear and conspicuous and the consumer must be reasonably notified of such changes.[14]

2. Disclosure Obligations: Consumer v. Customer.

The type and frequency of the notice is dependent on whether the information belongs to a "consumer" or a "customer." The primary distinction between a consumer and a customer depends upon the relationship that exists between the individual and the financial institution.

a. The Disclosure Requirements for a Consumer.

A consumer is an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes.[15] Typically, however, a consumer has a limited, "one time" connection with the financial institution.[16] For example, a consumer may be an individual who uses an automatic teller machine to withdraw cash from an account he or she may have at another financial institution, or the consumer obtains a loan from a company that does not retain the rights to service the loan.[17]

A financial institution is only required to send a privacy notice when it shares or intends to share the consumer's nonpublic personal information with a nonaffiliated third party.[18] Therefore, if a financial institution does not share or intend to share the consumer's information with a nonaffiliated third party, no privacy notice is required.

b. The Disclosure Requirements for a Customer.

A customer is a consumer who has a "continuing relationship" with the financial institution.[19] It is the nature of the relationship, not how long it lasts, that defines a customer.[20] For example, a customer may have a deposit or investment account with a bank, obtain a loan, purchase an insurance product or hold an investment account through a brokerage or investment company.[21] If the consumer relationship is a principal one, then the consumer is also a customer.

Financial institutions are required to provide customers with a privacy notice as soon as the customer relationship is established, whether or not the institution plans to share the customer's nonpublic personal information.[22] Additionally, the institution is required to provide its customer with a privacy notice annually for as long as the customer relationship exists.[23] For purposes of the Privacy Rule, a former customer is considered a consumer.

3. Required Information.

The privacy notice must accurately reflect the institution's information collection and sharing practices. The privacy notice must contain the following:

1. The categories of nonpublic personal information the institution collects;
2. The categories of nonpublic personal information the institution discloses;
3. The categories of affiliates and nonaffiliated third parties to whom the institution discloses nonpublic personal information (with certain statutory exceptions);
4. The categories of nonpublic personal information the institution discloses about its former customers and the categories of affiliates and nonaffiliated third parties in which the institution shares its former customer information (with certain statutory exceptions);
5. If an institution shares nonpublic personal information to a nonaffiliated third party, the institution is required to provide a separate statement of the

categories of information institutions disclose and the categories of third parties with whom the institution contracted;
6. An explanation of the customer's rights to opt–out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right at that time;
7. Any disclosures an institution makes pursuant to the Fair Credit Reporting Act; and
8. An institution's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.[24]

In other words, a financial institution must provide written notice of its privacy policies and practices, describe the conditions under which the institution may disclose the consumer's nonpublic personal information to nonaffiliated companies, and provide a method for consumers to opt–out of such information sharing, if required by law. The GLBA defines nonpublic personal information as "personally identifiable financial information provided by a consumer to a financial institution resulting from any transaction with the consumer or any service performed for the consumer or otherwise by the financial institution."[25] (*e.g.* first and last name, home address, email address, telephone number, Social Security number, credit card account number, and a customer number held in a "cookie" that identifies an individual consumer).[26]

B. The Opt–Out Notice and its Exceptions.

1. What is Required in an Opt–Out Notice.

If a financial institution intends to share nonpublic personal information with a nonaffiliated third party, the institution must provide its consumers with an opportunity to "opt–out" and instruct the institution not to share his or her nonpublic personal information in most instances.[27] This opt–out notice is required to be delivered to the consumer within a reasonable time and must be included or incorporated within the privacy notice itself.[28] Just like the privacy notice, the opt–out notice must be clear and conspicuous and state that: (1) the institution reserves the right to disclose the consumer's nonpublic personal information to a nonaffiliated third party; (2) that the consumer has the right to opt–out; and (3) provide a reasonable means by which the consumer may opt–out.[29] For example, an institution may provide the consumer with a toll–free telephone number or a detachable form which includes a check–off box and mailing information.[30] However, the FTC determined that requiring a consumer to write a letter as the sole means to opt–out fails to meet the reasonable means standard. [31]

2. The Exceptions to the Opt–Out Notice.

a. Service Providers and Joint Marketing.

Financial institutions often contract with outside service providers to perform certain ordinary business functions such as data processing or servicing accounts. The opt–out requirements do not apply when financial institutions share information with service providers who perform such services or ordinary business functions on the institution's behalf as long as: (1) the institution provides an initial notice to the consumer; and (2) the institution enters into a contractual agreement with the service provider that prohibits it from disclosing or using the information, other than to carry out the function for which it was hired.[32] These service provider contracts should specify the appropriate use of consumer nonpublic personal information, the requirements for safeguarding such personal information, and expressly prohibit any unauthorized and unlawful use of personal information. This exception also applies to third parties who perform joint marketing services, such as the marketing of an institution's own products and services or financial products offered by one or more affiliated financial institutions.[33] Again,

there must be a contractual agreement with the financial institution that carries out any joint marketing expressly prohibiting the disclosure of information, other than what is necessary in the ordinary course of business.

b. Servicing Transactions.

A second exception to the opt–out notice requirements allows the sharing of nonpublic personal information that is necessary for a financial institution to "effect, administer, or enforce" a transaction that a customer requests or authorizes.[34] These customer–authorized transactions include: (1) servicing or processing a financial product or service that a consumer requests or authorizes; (2) maintaining or servicing the consumer's account, including servicing another entity such as a private label credit card program; or (3) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to the consumer.[35] For example, the GLBA allows a financial institution to proceed with a consumer's loan application without having to provide the consumer with an opt–out notice. The premise of this exception is that the consumer authorizes disclosure of personal information, which is necessary in order to obtain the loan(s) they requested.

c. Other Exceptions to Notice and Opt–Out Requirements.

Finally, Section 313.15 provides a laundry list of exceptions which allows a financial institution to disclose a consumer's nonpublic personal information.[36] These exceptions include:

- When the customer consents to his or her information being shared.
- To protect the confidentiality or security of the consumer's records and to protect against or prevent actual or potential fraud.
- To resolve customer disputes or inquiries.
- To a consumer's legally appointed representative, such as a power of attorney, or persons acting in a fiduciary capacity on the behalf of the consumer.[37]
- To provide information to insurance rate advisory organizations, guaranty funds, or agencies that rate the institution, persons assessing an institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors.
- To the extent permitted or required by law and in accordance with the Right to Financial Privacy Act.
- To a consumer reporting agency in accordance with the Fair Credit Reporting Act.
- To comply with all Federal, State or local laws, including court orders.

C. The Safe Harbor Rule.

The Privacy Rule does not require any specific format or uniform wording to be included in an institution's privacy notice. Instead, the GLBA allows an institution to draft its own privacy notice as long as it is clear and conspicuous and furnishes the required information. However, Congress recognized that this broad discretion may result in some confusion. Therefore, Congress attached an appendix to the Privacy Rule that provided model language called "Sample Clauses."[38] With some specific industry exceptions,[39] if a financial institution incorporated the Sample Clauses within its privacy notice, the financial institution has complied with the GLBA requirements as a matter of law.

Despite Congress' efforts to ensure that privacy notices were clear and conspicuous, consumers and customers still complained about the notices. "Reaction to the first privacy notices delivered in July 2001 was highly negative. . . . the notices received by millions were filled with legalese and confusing messages. Many consumers simply tossed the privacy notices, seeing them as just another bit of junk mail stuffed in with account statements."[40]

On October 13, 2006, Congress passed the Financial Services Regulatory Relief Act of 2006

(the "Relief Act").[41] The Relief Act charged eight federal agencies (the "Agencies")[42] to jointly develop a uniform model privacy notice, which would address concerns expressed by financial institutions and reduce consumer confusion.[43] Specifically, the Relief Act instructed the new model form to:

1. Be comprehensible to consumers, with a clear format and design;
2. Provide for clear and conspicuous disclosures;
3. Enable consumers to easily identify the sharing practices of a financial institution and to compare privacy practices among financial institutions; and
4. Be succinct, and use an easily readable format.[44]

On March 29, 2007, the Agencies submitted the Interagency Proposal for Model Privacy Form Under the Gramm–Leach–Bliley Act (the "Interagency Report").[45] The Interagency Report proposed several model forms that are straightforward and easier to understand than most privacy notices used by institutions today.[46] The Interagency Report, if adopted, would eliminate the existing Sample Clauses and replace them with the proposed new model form.[47] A financial institution could still elect to use the Sample Clauses, but would no longer receive safe–harbor protection. In order to provide a transition period for institutions to adopt the proposed new model forms, the Interagency Report recommended a one–year phase–in period once the final rule becomes effective. [48]

D. Notice of Breach.

The FTC acknowledges that "perfect security" is not attainable and that breaches in security may occur even when every reasonable precaution is taken.[49] The GLBA does not specifically require institutions to notify their customers of a security breach. However, the Safeguards Rule does charge institutions with 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."[50] In 2005, the FTC and other federal banking regulatory agencies adopted the Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice ("the Guidance").[51] The Guidance outlines a financial institution's notice responsibilities when its consumers' nonpublic personal information network is breached and highlights customer notice as a key feature of an institution's response program.

Once a financial institution discovers that its network was breached and sensitive customer information has been or will be misused, the institution is required to notify its primary Federal regulator.[52] Second, an institution is required to notify appropriate law enforcement authorities including filing a Suspicious Activity Report ("SAR"), when Federal criminal violations are involved. [53] Next, if the institution determines that misuse of customer information has occurred or is likely, then the institution is required to notify its affected customers as soon as possible.[54] However, an institution may delay customer notice if law enforcement determines that such notification will interfere with a criminal investigation.[55] The customer notice must be clear and conspicuous[56] and should be delivered in a manner designed to ensure that a customer can reasonably be expected to receive it.[57] The customer notification shall include:

- A description of the incident in general terms and the type of customer information that was subject to the unauthorized access or use;
- A description of what the institution has done to protect the customer's information from further unauthorized access;
- A telephone number customers may call for further information and assistance;
- A reminder that customers need to be vigilant over the next 12 to 24 months and to promptly report incidents of suspected identity theft to the institution. [58]

The FTC Guidance report encourages, but does not require, institutions to include in their customer notice:

- A recommendation that the customer review account statements and immediately report any suspicious activity to the institution;
- A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports to put the customer's creditors on notice that the customer may be a victim of fraud;
- A recommendation that the customer periodically obtains credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;
- An explanation of how the customer may obtain a credit report free of charge;
- Information about the availability of the FTC online guidance regarding steps a consumer can take to protect against identity theft. [59]

The Guidance also encourages institutions to notify the nationwide consumer credit reporting agencies prior to sending notices to its customers.[60] In addition to the FTC Guidance report, many states, such as California, passed their own breach notification laws. Institutions must be aware of each state's requirements and comply accordingly. [61]

III. THE SAFEGUARDS RULE.

"Safeguarding information is not a product, but a process." [62]

The Safeguards Rule requires financial institutions to conduct a thorough risk assessment of its security measures and design a comprehensive information security program to protect nonpublic personal information.[63] Specifically, the Safeguards Rule requires financial institutions to "develop, implement, and maintain a comprehensive information security program that is written... and contains administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information."[64] The statutory objective of the Safeguards Rule is to: (1) ensure the security and confidentiality of customer information; (2) protect against anticipated threats or hazards to the security or integrity of such information; and (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. [65]

A. An Information Security Program Must be Appropriate.

The Safeguards Rule requires an institution to develop, implement, and maintain a comprehensive information security program that is written, contains administrative, technical and physical safeguards, is "appropriate" to the institution's size and complexity, as well as the nature and scope of its activities, and is appropriate to the sensitivity of the customer information at issue.[66] Therefore, an institution may exercise some latitude in developing its security program. While some critics may view this subjective standard as unenforceable, the FTC places a high level of responsibility upon financial institutions to keep up with the latest technology and the constant bombardment of potential identity thieves.

B. A Thorough Risk Assessment is Required.

The FTC requires companies to conduct a thorough risk assessment and address such risks to customer information in all areas of their operation, including administrative, technical, and physical safeguards.[67] As part of the risk assessment, the Safeguards Rule requires an institution to:

- Designate someone to coordinate the information security program;
- Perform a thorough risk assessment and identify reasonably foreseeable internal and external risks to the

> security, confidentiality, and integrity of customer information that could result in unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.

Reactions to the Safeguards Rule were mixed. Many companies carefully considered the costs of compliance compared to the costs of non–compliance. In fact, John Eubank, president of Nationwide Mortgage Group, evaluated whether to close his company because it would cost him $70,000 to comply with the Safeguards Rule and approximately $250,000 to fight the FTC if he elected not to comply.[68] The $250,000 did not include potential fines.

Another important factor for institutions to consider is the potential discoverability of risk assessments. If internal employees prepare the risk assessments, those assessments could be admitted as evidence, if they are relevant in court proceedings. For example, if a technical professional prepared a risk assessment indicating that the company should replace the firewall, and a security breach resulted due to the firewall before it could be replaced, the security assessment may be a damaging piece of evidence. To avoid potential discovery issues, companies should determine whether they could have their risk assessments covered by the attorney–client or the attorney work–product privileges. The rules regarding these privileges are state specific and should be examined carefully with experienced counsel.

1. Employee Training and Management.

A costs of compliance is related to employee training and management.[69] A financial institution's risk assessment should:

- Check employee references and perform background checks;
- Require employees to sign a confidentiality agreement;
- Limit employee access to sensitive customer information;
- Use password–activated screen savers to lock employee computers;
- Encrypt customer files on laptops and other computers in case of theft;
- Impose disciplinary measures for security policy violations;
- Prevent terminated employees from accessing customer information by immediately deactivating their passwords and user names.

The FTC noted in one of its publications that "the success of your information security plan depends largely upon the employees who implement it."[70]

2. Information Systems.

Second, the Safeguards Rule requires a financial institution to assess its information systems, including network and software design, as well as information processing, storage, transmission, and disposal.[71] A financial institution's written information security plan should include both technology concerns and the physical storage and destruction of nonpublic personal information. For example:

- Know where sensitive customer information is stored and stored securely;
- Ensure that the computer or server is accessible only by using a "strong" password and is kept in a physically secure area;
- Maintain secure backup records and keep archived data secure by storing it off–line and in a physically secure area;
- Take affirmative steps to secure transmission of customer information;
- Encrypt customer data if it is necessary for you to transmit such information by email or Internet;
- If you collect information online directly from customers, secure the data transmission automatically;
- Dispose of customer information

consistent with the FTC's Disposal Rule.[72]

3. Plan for System Attacks.

Third, the Safeguards Rule requires a financial institution to detect, prevent, and respond to attacks, intrusions, or other system failures.[73] A financial institution must remain constantly vigilant, and employ the latest security measures and technology in order to adequately protect its network. The FTC Guidance report suggests that financial institutions:

- Monitor the websites of software vendors and relevant industry publications for news about emerging threats and available defenses;
- Maintain up–to–date and appropriate programs and controls to prevent unauthorized access to customer information;
- Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information;
- Take affirmative steps to preserve the security, confidentiality, and integrity of customer information and consider notifying consumers, law enforcement, and credit bureaus in the event of a security breach;
- Oversee service providers by ensuring that they are able to take appropriate security precautions and in fact do so;
- Update the security program as necessary in response to frequent monitoring and material changes in the business.

C. Implementing and Maintaining the Information Security Program.

Finally, the Safeguards Rule requires an institution to design and implement information safeguards to control the risks identified and regularly test and monitor the effectiveness of the information security program's key controls, systems, and procedures.[74] This duty also includes overseeing third–party service providers by taking reasonable steps to ensure that the service provider is capable of maintaining appropriate safeguards and requiring the service providers to contractually agree to implement and maintain such controls. [75] The Safeguards Rule requires a financial institution to evaluate and adjust its information security program in response to its system test results or in response to any changes in its operations or business circumstances. [76]

IV. CONCLUSION.

As Congress attempts to keep pace with the information age and balance the needs of commerce with those of individual protection, the Gramm–Leach–Bliley Act continues to evolve. Financial institutions must be aware of new Federal agency opinions as well as changing state laws. The Privacy and Safeguards Rules allow financial institutions to adopt policies and procedures that are appropriate for their specific needs and size, but the costs of compliance are often great. The costs of non–compliance can be even greater. As technology advances, so does the level of appropriateness a financial institution is required to maintain. Protecting the privacy of consumer information is not only good for business, it's a legal duty.

[1] 15 U.S.C.A. § 6801 (West 1998 & Supp. 2005).
[2] *See* Michelle Chen, *White House ID Theft Plan Soft on Industry, Critics Say,* THE NEW STANDARD located at http://newstandardnews.net/content/index.cfm/items/4756.
[3] *See* 15 U.S.C.A. § 6801 (West 1998 & Supp. 2005)
[4] *See id.*
[5] FTC, *The Gramm–Leach–Bliley Act*, http://www.ftc.gov/privacy/privacyinitiatives/glbact.html (last visited May 3, 2007).
[6] 15 U.S.C.A. § 6805 (West 1998 & Supp. 2005).
[7] 12 U.S.C.A. § 1843(k) (West 1998 & Supp. 2005).
[8] 12 U.S.C.A. § 1843(k)(1)(A) (West 1998 & Supp. 2005).
[9] 12 U.S.C.A. § 1843(k)(1)(B) (West 1998 & Supp. 2005).
[10] 12 U.S.C.A. § 1843(k)(4) (West 1998 & Supp. 2005).
[11] 16 C.F.R. § 313.4(a)(2006); *see also* 16 C.F.R. § 313.5(a)(1)(2006).
[12] 16 C.F.R. § 313.3(b)(1)(2006).
[13] 16 C.F.R. § 313.3(b)(1)(i)(2006).
[14] 16 C.F.R. § 313.8; *see also In re Nations Title Agency, Inc., et. al.*, 2006 WL 1367834, *4 (FTC May 10, 2006)
[15] 15 U.S.C.A. § 6809(9) (West 1998 & Supp. 2005).
[16] 16 C.F.R. § 313.3(h)(ii) (2006).
[17] *Id.*
[18] FTC, *How to Comply with the Privacy of Consumer Financial Information of the Gramm–Leach–Bliley Act* (2002), http://www.ftc.gov/bcp/conline/pubs/buspubs/glblong.pdf (last visited May 3, 2007).
[19] 16 C.F.R. § 313.3(i)(1) (2006).
[20] FTC, *How to Comply, supra* note 18 at 3.
[21] 16 C.F.R. § 313.3(i)(2)(i) (2006).
[22] 16 C.F.R. § 313.4(a)(1) (2006).
[23] 16 C.F.R. § 313.5(a)(1) (2006).
[24] 16 C.F.R. § 313.6(a) (2006).
[25] 15 U.S.C.A. § 6809(4)(A) (West 1998 & Supp. 2005).
[26] *In re Nations Title Agency, Inc., et. al.*, 2006 WL 1367834, *4 (FTC May 10, 2006).
[27] 15 U.S.C.A. § 6802(b)(West 1998 & Supp. 2005); *see also* 16 C.F.R. § 313.1(3)(2006).
[28] *Id.*; FTC, *How to Comply, supra* note 18, at 9.
[29] 16 C.F.R. § 313.7(a)(1)(2006).
[30] FTC, *How to Comply, supra* note 18, at 9.
[31] *Id.*
[32] 16 C.F.R. § 313.13(a) (2006).
[33] 16 C.F.R. § 313.13(b) (2006).
[34] 16 C.F.R. § 313.14(a) (2006).
[35] *Id.*
[36] 16 C.F.R. § 313.15(a)(1) (2006).
[37] *Id.*
[38] 16 C.F.R. § 313, App. A (2006).
[39] For example the SEC's privacy rule does not provide a safe harbor for financial institutions that use current Sample Clauses. Rather, the SEC merely recognizes the Sample Clauses as "guidance" concerning the SEC's privacy rule application. Accordingly, the SEC would eliminate the meaning of the Sample Clauses, entirely.
[40] http://www.privacyrights.org/fs/fs24d–FinancialFAQ.htm.
[41] P.L. 109–3511996 (October 13, 2006), 120 Stat. 1966.

[42] The eight federal agencies include: the Office of the Comptroller of the Currency; the Board of Governors of the Federal Reserve System; the Federal Deposit Insurance Corporation; the Office of Thrift Supervision of the Department of Treasury; the National Credit Union Administration; the Federal Trade Commission; the Commodity Futures Trading Commission; and the Securities and Exchange Commission.
[43] 72 Fed. Reg. 14, 940, et. seq, (March 29, 2007).
[44] P.L. 109–3511996, § 728(e), 120 Stat. 1966, *2003.
[45] 72 FR 14940, (March 29, 2007).
[46] *See* 72 Fed. Reg. 14, 940, 14, 944.
[47] *See id.; see also* P.L. 109–351, § 728(e)(4).
[48] 72 Fed. Reg. 14, 944.
[49] Kathryn E. Picanso, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 364 October 2006 (citing *Data Breaches and Identity Theft: Hearing Before the Senate Comm. on Commerce, Sci. and Transp.*, 109th Cong. 6 (2005)(statement of Deborah Platt Majoras, Chairman, FTC)).
[50] 15 U.S.C.A. § 6801 (West 1998 & Supp. 2005).
[51] 70 Fed. Reg. 15,736 (12 C.F.R. pt. 30, Supp. A to App. B (2005)(OCC).
[52] *Id.* at II(A)(1)(b).
[53] *Id.* at II(A)(1)(c); *see also* 12 C.F.R. § 21.11.
[54] *Id.* at III(A).
[55] *Id.*
[56] *Id.* at III(B)(1).
[57] *Id.* at III(C).
[58] *Id.* at III(B)(1).
[59] *Id.*
[60] *Id.* at III(B)(2).
[61] *See* Julie Machal–Fulks and Robert J. Scott, *Privacy, Network Security and the Law*, http://www.scottandscottllp.com/resources/article_privacy_network_law.asp (last visited May 3, 2007).
[62] *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 258 [fn. 97](citing Thomas J. Smedinghoff, *The New Law of Information Security: What Companies Need to Do Now*, COMPUTER & INTERNET LAW., Nov. 2005, at 9, 13).
[63] 16 C.F.R. Part 314, et. seq.
[64] 16 C.F.R. § 314.3(a)
[65] 16 C.F.R. § 314.3(b) (2006).
[66] 16 C.F.R. § 314.3(a) (2006).
[67] FTC, *Complying with the Safeguards Rule*; http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.pdf (last visited May 3, 2007); *see* 16 C.F.R. § 314.3(a) (2006).
[68] *Safeguards Rule Could Be Hidden Danger in '05*. DMNews December 30, 2004 located at http://www.complyfast.com/doc/dmnews_1230_mortage_brokers_ftc_action.pdf.
[69] 16 C.F.R. § 313.4(b) (2006).
[70] FTC, *Complying with the Safeguards Rule, supra* note 67, at 2.
[71] 16 C.F.R. § 313.4(b) (2006).
[72] *See* FTC Disposal Rule, www.ftc.gov/os/2004/11/041118disposalfrn.pdf.
[73] 16 C.F.R. § 313.4(b) (2006).
[74] 16 C.F.R. § 314.4(c) (2006).
[75] 16 C.F.R. § 314.4(d) (2006).
[76] 16 C.F.R. § 314.4(e) (2006).

SCOTT IP
TECHNOLOGY ATTORNEYS

1256 Main Street :: Suite 200 :: Southlake,Texas 76092 :: t 800.596.6176 :: f 800.529.3292 :: scottandscottllp.com