

## FCC Grants Time to Comply with No Fax Ad Rule

*'Established relationship' exception scrapped*

By D. Reed Freeman Jr.

Over the last month or so, the Federal Communications Commission's (FCC) changes to its rule regulating unsolicited faxes has been generating some high-volume buzz.

The original rule, in place for more than a decade, stems from the federal Telephone Consumer Protection Act, which prohibits sending an advertisement to a business' or individual's fax machine without the prior express permission of, or an invitation from, the recipient.

The act required the FCC to draft a rule implementing this prohibition and, in 1992, the FCC did so. Its rule contained the act's general prohibition but provided one limited exception: It allowed a company to send an unsolicited fax advertisement to a person or business with whom it had an "existing business relationship," as long as the recipient had not terminated the relationship.

### NEW GAME RULES

In July, the FCC revised the rule. Among its changes was a scrapping of the "established business relationship" exception. The FCC determined in its rule-making that the mere existence of a business relationship between fax sender and recipient does not

*continued on page 4*

## You Need To Know

### The FTC Safeguards Rule: An Expansion of Gramm-Leach-Bliley

By Marie Flores

Just when businesses thought their privacy policies were finally perfect and that it was safe to assume they had seen the last of the privacy laws, the issue struck again.

And this time, it struck where businesses and their legal advisers might least have expected it, turning regular e-businesses into "financial institutions" and requiring implementation of yet another set of rules.

#### HISTORY OF GLB

On Nov. 12, 1999, Congress enacted the Financial Services Modernization Act, commonly referred to as the Gramm-Leach-Bliley Act (GLB). The purpose of the act was to bring the banking industry up-to-date by allowing banks to engage in a broad range of activities, including offering insurance and brokering services with new affiliates. Subtitle A in Title V of the act, "Disclosure of Nonpublic Personal Information" (NPPI), limits the range of instances in which a financial institution may disclose NPPI about a consumer to nonaffiliated third parties. The act also requires financial institutions to disclose to their customers privacy policies and practices regarding customer information shared with affiliates and nonaffiliated third parties.

On May 12, 2000, the Federal Trade Commission (FTC) issued the Privacy of Consumer Financial Information Rule, which implemented GLB's Subtitle A. Financial companies were required to comply with the new privacy rule by July 1, 2001.

Title V also requires the FTC to establish standards for financial institutions relating to administrative, technical and physical safeguards (Safeguards Rule) to ensure security and confidentiality of customer records and information. On May 17, 2002, the FTC issued its Safeguards Rule, which mandates these standards. (See [www.ftc.gov/os/2002/05/67fr36585.pdf](http://www.ftc.gov/os/2002/05/67fr36585.pdf).)

*continued on page 2*

#### IN THIS ISSUE

The FTC Safeguards Rule: An Expansion of Gramm-Leach-Bliley	.1
FCC Grants Time to Comply with No Fax Ad Rule	.....1
Federal Task Force Urges Rules for Electronic Proofs in Criminal Cases	....3
E-Commerce Docket Sheet	.....5
Developments of Note	.....8

PERIODICALS



## FTC Safeguards

continued from page 1

### AN OVERVIEW OF GLB

The act requires financial institutions to notify customers about the institution's information-sharing practices and to tell consumers of their right to "opt-out" if they do not want their information shared with certain nonaffiliated third parties. Any entity that receives consumer financial information from a financial institution may be restricted in its reuse and re-disclosure of that information.

GLB's definition of *financial institution* is extremely broad. Under Section 16 C.F.R. §313.3(k)(1) of the privacy rule, a financial institution is defined as "any institution the business of which is engaged in financial activities as described in 4(k) of the Bank Company Holding Act of 1956 (12 U.S.C. 1843 (k))." Suddenly, some e-businesses that have not been commonly thought of as being a type of financial institution are finding themselves labeled as such because they conduct "financial transactions." In today's e-world, one can trade stock, bank, apply for a credit card, have taxes prepared, request a copy of a credit report and apply for a car or home loan online. All of these transactions qualify the service provider as a "financial institution." In fact, even activities such as exchanging or transferring money for others, or providing financial data processing and transmission services, qualify a company as a financial institution under GLB.

### FTC's SAFEGUARDS RULE STANDARDS FOR DATA

The Safeguards Rule mandates standards relating to administrative, technical and physical information safeguards for financial institutions. This rule became effective on May 23, 2003. The stated goals of the Safeguards Rule are to:

- Ensure security and confidentiality of customer records and information;
- Protect against any anticipated threats or hazards to the security or integrity of such records; and
- Guard against any unauthorized access to or use of such records or

information that could result in substantial harm or inconvenience to any customer.

### MAIN PROVISIONS OF THE RULE

The Safeguards Rule requires all covered financial institutions to:

- Designate an employee or employees to coordinate the financial institution's security measures to implement the Safeguards Rule;
- Identify and assess security risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of current safeguards for controlling these risks;
- Design a safeguards program, and detail the plans to monitor it;
- Select appropriate service providers and require them (by contract) to implement the safeguards; and
- Evaluate the program, and explain adjustments relevant to business arrangements or to results of security tests.

The FTC notes that when implementing the Safeguards Rule, a business must consider all operating areas, particularly employee training and management, information systems and possible managing-system failures.

### EMPLOYEE MANAGEMENT AND TRAINING

In addition to step one of the Safeguards Rule, the FTC has issued a few other suggestions on how employees can help manage security risk.

- Have every employee sign an agreement to follow the organization's confidentiality and security standards for handling customer information;
- Train employees to take basic steps to maintain security of customer information such as locking rooms and filing cabinets where records are kept, changing passwords periodically and referring calls or requests for customer information to designated employees who have had safeguard training;
- Restrict access to customer information to employees who need such access for business purposes; and
- Impose disciplinary measures for

continued on page 7

## e-commerce LAW & STRATEGY®

PUBLISHER ..... Marjorie A. Weiner  
ASSOCIATE PUBLISHER ..... Sofia Pablos  
EDITOR-IN-CHIEF ..... Michael Law-Orlowski  
MANAGING EDITOR ..... Steven Salkin, Esq.  
ART DIRECTOR ..... Claire C. O'Neill-Burke  
GRAPHIC DESIGNER ..... Louis F. Bartala

BOARD OF EDITORS  
NEIL A. ABRAMS ..... IBM Corp.  
Somers, NY  
RICHARD BUCHARD ..... Juno Online Services Inc.  
New York  
JEFFREY P. CONARD ..... Debevoise & Plimpton  
Washington, DC  
WALTER A. EFFROSS ..... American University  
Washington, DC  
D. REED FREEMAN JR. .... Collier Shannon Scott  
Washington DC  
BRUCE GAYLORD ..... JPMorgan Chase Bank  
New York  
PAUL R. GUPTA ..... LeBoeuf, Lamb,  
Greene & MacLean LLP  
Boston  
THOMAS HEYMANN ..... Wilkie, Farr & Gallagher  
Frankfurt, Germany  
JULIAN S. MILLSTEIN ..... Brown Rayman Millstein Felder  
& Steiner  
New York  
JEFFREY D. NEUBURGER ..... Brown Rayman Millstein Felder  
& Steiner  
New York  
EDWARD A. PISACRETA ..... Brown Rayman Millstein Felder  
& Steiner  
New York  
JOHN SHORT ..... Taylor Vinters Solicitors  
Cambridge, England  
HOWARD SIEDEL ..... Pryor Cashman  
Sherman & Flynne LLC  
New York  
SIMON SMITH ..... Taylor Vinters Solicitors  
Cambridge, England  
PHILLIP L. SPECTOR ..... Paul, Weiss, Rifkind,  
Wharton & Garrison LLP  
New York  
J.T. WESTERMEIER, JR. .... Piper & Marbury  
Washington, DC  
JOSEPH P. ZAMMIT ..... Fairbright & Jaworski  
New York

e-Commerce Law & Strategy™ (ISSN 0747-8933) is published by  
Law Journal Newsletters, a division of American Lawyer Media.

© 2003 NLP-IP Company. All rights reserved.

No reproduction of any portion of this issue is allowed  
without written permission from the publisher.

Telephone: (800) 999-1916

Editorial e-mail: steven@palawnet.com

Circulation e-mail: subs@palawnet.com

e-Commerce Law & Strategy P0000-235

Periodicals Postage Pending at Philadelphia, PA

POSTMASTER: Send address changes to:

American Lawyer Media

1617 JFK Blvd., Suite 1750, Philadelphia, PA 19103

Annual Subscription: \$335

Published by:

Law Journal Newsletters

1617 JFK Boulevard, Suite 1750, Philadelphia, Pa 19103



## FTC Safeguards

continued from page 2

any breach of the company's customer privacy policy.

### INFORMATION SYSTEMS

Step two of the Safeguards Rule requires identification and assessment of security risk. Below are some of the FTC's suggestions on how to maintain customer information security:

- Store records in a secure area and provide only authorized employees access to the records;
- Provide a means for securely transmitting or collecting customer information;
- Dispose of customer information in a secure manner; and
- Use appropriate oversight or audit procedures to detect improper disclosure or theft of customer information.

### MANAGING SYSTEM FAILURES

Step three of the Safeguards Rule requires a security plan. Some steps the government recommends for meeting this requirement are:

- Maintain up-to-date programs and controls by following a written contingency plan to address any breaches in administrative or technical safeguards;
- Maintain up-to-date firewalls and antivirus software that updates automatically;
- Maintain systems and procedures to ensure that access to nonpublic customer information is granted only to legitimate users; and
- Notify customers promptly if personal information is lost or is illegally accessed.

### PROTECTIVE MEASURES REQUIRED

The Safeguards Rule's fourth step mandates that financial institutions take "reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue." The FTC opted not to

**Marie Flores, J.D.**, is assistant vice president and contracts department manager at Southwest Bank of Texas, N.A., in Houston. Contact her at [marieflores@wanderingeyeprod.com](mailto:marieflores@wanderingeyeprod.com).

require specific contractual language, stating in the commentary to the rules that "The commission believes that financial institutions are well positioned to develop and implement appropriate contracts with their service providers" (67 Fed. Reg. 36490). For those looking for more guidance, the following contractual language is suggested:

- The contract should include a provision stating that the parties wish to keep customer nonpublic, personal information strictly confidential in order to comply with regulatory requirements.
- A stipulation that the information

***Suddenly, some e-businesses***

***that have not been commonly***

***thought of as being a type***

***of financial institution are***

***finding themselves labeled as***

***such because they conduct***

***"financial transactions."***

will be held in strict confidence and accessed only for the explicit business purposes of the proposed transaction.

- A guarantee from the receiving party that it will protect the information it accesses no less rigorously than it protects its own customers' confidential information and that it has the safeguard measures in place as required by the FTC for such types of information.
- A provision allowing auditing of the receiving party to ensure compliance with contract requirements.
- Provisions allowing for return or destruction of all confidential information disclosed to the receiving party upon request of the disclosing party.
- A provision stating that the receiving party agrees upon written request from the disclosing party that it will not continue to use the disclosing parties' customer information.
- A provision should be included allowing equitable relief and indemnification.

- A stipulation should be made that any violation of the contract's protective conditions amounts to a material breach of contract and entitles the party to immediately terminate the contract without penalty.

A provision ensuring that the contract's protective requirements will survive any termination agreement.

The last step of the Safeguards Rule simply requires institutions to evaluate their security programs and adjust them as their business or technology changes, or as otherwise necessary.

### CONCLUSION

The FTC Safeguards Rule is another bend in the e-commerce superhighway, one more in the ever-growing list of regulations that e-businesses and their advisers must know well. These days, it's prudent for any business that collects personal information from customers to have a security plan to protect the confidentiality and integrity of that information. For "financial institutions," it's not only prudent — it's the law. Awareness is the key. Remember: Knowing is half the battle. For more information on this topic visit the following links:

- [www.ftc.gov/privacy/glbact](http://www.ftc.gov/privacy/glbact);
- [www.fdic.gov/regulations/information/bulletins/brochure1.html](http://www.fdic.gov/regulations/information/bulletins/brochure1.html);
- [www.ftc.gov/infosecurity](http://www.ftc.gov/infosecurity);
- [www.fdic.gov/regulations/information/bulletins/brochure2.html](http://www.fdic.gov/regulations/information/bulletins/brochure2.html); and
- [www.fdic.gov/regulations/information/bulletins/brochure3.html](http://www.fdic.gov/regulations/information/bulletins/brochure3.html).

## LAW JOURNAL NEWSLETTERS REPRINT SERVICE

Reprints of this article or any other article published by  
**LAW JOURNAL NEWSLETTERS**  
are available in bulk quantities.

Call Karen Dispo  
at 212-545-6226 or e-mail  
[kdispo@amlaw.com](mailto:kdispo@amlaw.com)  
for a free quote.

Reprints are available in  
paper and PDF format.