

Privacy & Security Law Update

New Fax Rules Take Effect

The Federal Communications Commission has finalized its revisions to Telephone Consumer Protection Act (TCPA) implementing the Junk Fax Prevention Act (JFPA). The new rules took effect on August 1. The rules apply to all unsolicited commercial faxes, including business-to-business faxes.

History

Since 1991 the TCPA has prohibited unsolicited fax advertising unless the sender had the prior consent of the recipient. Companies assumed that they had implied consent to send faxes based on their existing business relationships (EBRS). Complaints led the FCC to propose requiring senders to get prior *written* consent that included the specific fax number. Business outcry led the FCC to stay the rule.



In 2005, Congress enacted

the JFPA to amend the TCPA and allow faxing based on an EBR. It required senders to offer an opt-out. The JFPA required the FCC to issue new rules to define the parameters of the EBR exception and to specify the opt-out process requirements.

EBRs

Companies may send unsolicited commercial faxes to individuals with whom they have an EBR. An EBR exists when (1) the recipient has a business relationship with the sender, *and* (2) the recipient provides the fax number to the sender or makes it available publicly. Please consider the following points:

- A business relationship is formed by voluntary two-way communication (such as an inquiry) between the parties involving the products or services offered by the company. An inquiry about store locations or the mere visiting of a



website does not establish an EBR.

- The EBR only applies to the entity which had the communication with the individual. *It does not extend to affiliates or business partners of that entity.*

- Unless the sender had the fax number before July 9, 2005, it must obtain the number from the recipient or from sources available to the general public. A sender can use fax numbers obtained from third parties only if it can demonstrate that fax number was voluntarily provided for

continued on page 2

IN THE SPOTLIGHT... PCI Security Standard

The Payment Card Industry Data Security Standard is an industry-issued set of security requirements to protect personal and account information of VISA, MasterCard, Discover and American Express cardholders. The rules apply to industry members, merchants and service providers.

If your company handles payment card data, your security team should be aware of the PCI requirements, including self-assessment rules.

Company counsel need to be aware of the rules as well. If a security breach exposes cardholder data, the PCI rules require specific notifications. For example, if VISA cardholder data is compromised, the incident must be reported to the Visa Fraud Control Group within 24 hours.

Additionally, lawyers should consider how the PCI rules impact contracts. Companies should include representations regarding compliance

with the Standard in vendor contracts, if the vendor handles payment card data.

Similarly, if a company is asked to make representations about its own security program, it should verify that it has successfully completed the self-assessment process prior to making those statements.

The PCI rules and guidance can be found on the VISA and MasterCard websites.



One Year and Counting...

PIMS proudly celebrated its first anniversary on October 1. Many thanks to all of you for your support, friendship and business!

**Privacy
Studio.com**

The Art of Information Management

New Fax Rules

use by the general public. For example, if a company publishes its fax number on its website, the fax number can be used. But if the number comes from a list, the sender must verify that the company agreed to make that number available to the public. The FCC recommends that verification be done by phone or email.

- There is no limit on the duration of the EBR. Faxes may be sent until the recipient opts-out.

Process Requirements

Under the new rule, faxes must contain a notice stating that the recipient is entitled to opt out of receiving future faxes. Specific requirements include:

- The opt-out notice must be on the first page of the advertisement. The FCC encourages senders that use cover pages to include the notice on both the first page of the advertisement and the cover page.
- The opt-out notice must be clear and conspicuous and separate from the advertising copy. It must be placed at either the top or the bottom of the page.

Congratulations Tanya

On September 23, our own Tanya Foster married Todd Wilson in a lovely ceremony in Marietta, Georgia.



The happy couple honeymooned in the Dominican Republic, and Tanya is back as Tanya Foster Wilson. Her email and phone have not changed.

Please join us in wishing Tanya and Todd a lifetime of happiness!

- The opt-out notice must include a phone and a fax number for receiving opt-out requests. The sender must also offer a cost-free opt-out mechanism, such as a toll-free phone or fax number, website or email address. A local telephone number may be used if the faxes are only sent to local customers.
- The opt-out mechanisms must be available at all times, and opt-outs processed within 30 days.
- Opt-out requests do not expire. If a company wants to send faxes to a number that has opted out (if, for example, the company owning the number is under new management), the sender must get prior express permission to restore that fax number to its database.

Other Provisions

Definition of Unsolicited Fax

Certain types of transactional communications, such as communications confirming an existing order or relationship, are not unsolicited advertisements and are not subject to the requirements set forth above.

To be transactional, the fax must relate specifically to an *existing account or ongoing transactions*. Communications about new products are not transactional – these faxes are covered by the rules. The FCC noted that all faxes regarding new products, services, and events are unsolicited advertisements, *even if the products, services and events are free*.

The FCC also considered whether a sender could combine “a small amount of advertising” on a transactional fax without triggering the new rule. The addition of a company logo or business slogan does not convert a transactional communication into an advertisement.

If a sender does not have an EBR, it must receive prior express permission.

Permission may be obtained via any channel, including email or a website form, in writing or orally. The burden is on the sender to demonstrate that permission exists. Permission cannot be obtained by a failure to opt-out of receiving faxes.

Enforcement

The new fax rules are part of the TCPA, and enforcement can come from the FCC or state authorities. It has a private right of action and provides for statutory damages of \$500-\$1,500 per violation (*i.e.*, fax sent).

Preemption

The TCPA and JFPA do not preempt state regulations. California has enacted an opt-in fax law that applies to all entities that do business in California. A trial court has ruled that California cannot regulate interstate faxes. The restrictions as applied to intrastate faxes are still in play.

Several other states have older statutes, some of which require consent and do not mention an EBR exception. Other states have process requirements that senders must respect for EBR faxes. For example, some states require opt-outs to be processed in less than 30 days. Others require unsolicited faxes to be sent only at certain times, contain disclosures in certain formats, or respect page limits.

A group has asked the FCC to declare that these state laws are preempted by the JFPA. It is unclear when the FCC will rule on this petition or what the likelihood is that the state laws will be preempted. Companies should continue to comply with these state laws as well as the new JFPA regulations.

If you have questions about these rules, please call Peggy at 404-914-1163.

This newsletter is intended for clients and friends of Privacy & Information Management Services—Margaret P. Eisenhauer, P.C. PIMS is a Georgia Law Firm specializing in privacy, security and information management. If you do not wish to receive communications from PIMS, please email tanya@privacystudio.com—we will gladly remove you from our mailing list.

The information contained in this newsletter has been prepared for informational purposes only and is not legal advice. This communication is not intended to create an attorney-client relationship. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials. If you are not a current client of PIMS, please do not send any confidential information.

Privacy & Information Management Services—Margaret P. Eisenhauer, P.C.
4355 Cobb Parkway—Suite J-280, Atlanta GA 30339
Phone: 404-914-1163
www.privacystudio.com