

---

## Legal Updates & News

### Legal Updates

---

#### Federal Agencies Issue Model GLBA Privacy Form

December 2009

---

The federal banking agencies and the CFTC, FTC, NCUA and SEC (“Agencies”) have issued a final rule amending their privacy rules under Title V of the Gramm-Leach-Bliley Act (“GLBA”). The purpose of the amendments is to provide a model privacy form that financial institutions may use to describe their privacy policies and to provide consumers with the opportunity to opt out of the sharing of information with nonaffiliated third parties, as required by the GLBA.<sup>[1]</sup> The model privacy form also addresses relevant opt outs under the Fair Credit Reporting Act (“FCRA”) relating to the sharing of information with affiliates. The model privacy form, which had been under development for several years, is similar to the form proposed by the Agencies on March 29, 2007, with modifications to address comments received on the proposal. The Agencies believe that the model privacy form is easier to understand and use than most forms currently used by financial institutions. While use of the model privacy form is not required, a financial institution that uses the form (consistent with instructions included in the rule) will be deemed in compliance with the GLBA notice content requirements for privacy policies and opt-out notices.

#### Related Practices:

- ▶ [Financial Services Law](#)
- ▶ [Privacy and Data Security](#)

As described below, the final rule provides numerous detailed requirements for how the model privacy form must be presented and what information must be included in the model privacy form. The final rule will become effective on December 31, 2009. In addition, the Agencies have eliminated the safe harbor from the existing sample clauses included in the GLBA privacy rules effective December 31, 2010.

#### Background

Section 503 of the GLBA (and the various implementing regulations issued by the Agencies) requires each financial institution to provide its consumer customers with an initial and annual notice of its privacy policies and practices. More specifically, a privacy notice must describe the financial institution’s policies and practices regarding the disclosure of nonpublic personal information about the consumer to both affiliated and nonaffiliated third parties. In addition, the notice must provide the consumer with a reasonable opportunity to direct the institution not to share (that is, to “opt out” of sharing) nonpublic personal information about the consumer with nonaffiliated third parties. However, this opt-out right does not extend to instances where the statute provides an exception permitting a financial institution to share information with third parties, such as for transaction processing and responding to legal processes.

In recent years, the Agencies have emphasized the importance of improving consumer privacy disclosures so that information provided effectively informs consumers of what they need to know to make appropriate decisions. In particular, the Agencies have acknowledged the ineffectiveness of privacy disclosures mandated by the GLBA, including sample clauses provided earlier by the Agencies, and have studied ways of delivering more effective privacy disclosures. In this regard, in December 2003, the Agencies published an advance notice of proposed rulemaking soliciting comments on improving privacy notices and whether the Agencies should conduct consumer testing to develop a model privacy notice (which the Agencies then began). In addition, in October 2006, Congress passed the Financial Services Regulatory Relief Act of 2006, which directed the Agencies to jointly develop a model form that could be used at the option of financial institutions for the purpose of providing disclosures under section 503 of the GLBA, *i.e.*, privacy policies and opt-out notices. In response, the Agencies continued the work that they began in 2003 to improve privacy notices. In doing so, the Agencies conducted extensive qualitative and quantitative consumer testing, including consumer interviews and focus groups, in order to develop the final version of the model privacy form.

### **Model Privacy Form Replaces Sample Clauses as Safe Harbor**

The final rule provides that use of the model privacy form (consistent with the detailed instructions included with the form) will “constitute[] compliance with the notice content requirements” of the privacy rule for privacy policies and opt-out notices. The Agencies clarified, however, that “[w]hile the model form provides a legal safe harbor, institutions may continue to use other types of notices that vary from the model form so long as these notices comply with the privacy rule.”

In this regard, the existing privacy rules of the Agencies provide sample clauses that financial institutions may use to comply with the notice content requirements of the rules, including, for example, a sample clause describing the categories of nonpublic personal information that a financial institution collects. Effective January 1, 2012, these sample clauses will be removed from the privacy rules; but, there will be a safe harbor for a financial institution using one or more clauses in its privacy policies and opt-out notices to comply with the requirements of the rule until December 31, 2010. The Agencies explained that, after December 31, 2010, “institutions may continue to use notices containing these clauses, so long as these notices comply with the privacy rule,” but there will be no safe harbor for using the sample clauses after that date.

### **Format of the Model Privacy Form**

The final rule provides three versions of the model privacy form: (1) a model form with no opt out; (2) a model form with opt out by telephone and/or online; and (3) a model form with opt out by mail. The basic model privacy form itself, however, is a standardized form, and the final rule provides detailed requirements for the page layout, content, format, style, pagination and shading of the form. In order for the safe harbor to be applicable, a financial institution must ensure that its privacy notice complies with each specified requirement for the model form. For example, a financial institution seeking to take advantage of the safe harbor cannot modify the model privacy form, except where expressly permitted by the final rule. The model privacy form, however, may be incorporated into another document, so long as it is done in a manner that meets all the formatting requirements.

Specifically, the model privacy form consists of two pages, which may be printed on both sides of a single piece of paper or on two separate pages. Unlike the proposed rule, the final rule does not mandate that the model privacy form be included on a specific paper size, but the pages must be in portrait orientation and large enough to accommodate the minimum font size, spacing, and content requirements. For example, a financial institution must use an “easily readable type font” that is a minimum of 10-point (except where otherwise expressly permitted in the rule). In addition, the model privacy form must be printed on white or light color paper with black or other contrasting ink color. While a corporate logo may be included on either page of the model privacy form, it cannot interfere with the readability requirements or space constraints, and no other images or slogans may be included on the model privacy form.

### **Page One of the Model Privacy Form**

The first page of the model privacy form consists of five parts: (1) a title; (2) an introductory section; (3) a disclosure table relating to the sharing of personal information; (4) a section describing how a consumer

may opt out; and (5) a questions section.

**Title.** Page one begins with the title; specifically, the title must read “What Does [Name of Financial Institution] Do with Your Personal Information?” In the title and in other places in the model privacy form where the phrase “[Name of Financial Institution]” appears, the name of the financial institution providing the notice or a common identity of affiliated institutions jointly providing the notice must be provided.

**Introductory Section.** The second part of page one of the model privacy form is an introductory section, called the “Key Frame,” with individual boxes labeled “Why?,” “What?,” and “How?” According to the Agencies, the key frame is intended to provide a context so that consumers can understand the purpose of the notice. The “Why?” box describes why the consumer is to receive the notice, including a statement that the financial institution is required to notify the consumer about how it collects, shares and protects personal information relating to the consumer and that the consumer has the right to limit some, but not all, information sharing by the institution.

The “What?” box identifies the types of personal information that the financial institution collects and shares. A financial institution must include the term “Social Security number” in the first bullet of the list of information it collects. In addition, the Agencies have provided a menu of other types of information from which a financial institution must tailor the notice to its sharing practices. Specifically, a financial institution must select four types of information, in addition to Social Security number, to identify the types of personal information that it collects and shares. For example, the types of information that may be disclosed in this section include a consumer’s income, credit scores, overdraft history, mortgage rates and payments, checking account information and employment information.

The “How?” box informs the consumer that the next section of the model form will describe the reasons institutions are generally permitted to share personal information, the reasons the financial institution providing the notice shares personal information and whether or not the consumer can limit the types of sharing identified.

**Sharing Disclosure Table.** The third part of page one of the model privacy form provides the consumer with information regarding the financial institution’s sharing of personal information. Specifically, this table is broken down into three columns that identify the reasons financial institutions are permitted to share personal information, the reasons the financial institution providing the notice shares personal information and whether or not the consumer can limit this type of sharing.

The left column of this table lists the reasons for which a financial institution may share personal information in accordance with the GLBA and the FCRA. This column identifies the following categories of activities:

1. Sharing for everyday business purposes, which covers sharing pursuant to section \_\_\_\_.13 of the privacy rules relating to service providers, other than for marketing purposes, sharing pursuant to section \_\_\_\_.14 for processing and servicing transactions, and sharing pursuant to section \_\_\_\_.15, including, for example, for fraud prevention purposes;
2. Sharing for the institution’s own marketing purposes, which includes sharing information with service providers for the institution’s own marketing purposes pursuant to section \_\_\_\_.13 of the privacy rules;
3. Sharing for joint marketing with other financial companies, which covers sharing information under joint marketing agreements pursuant to section \_\_\_\_.13 of the privacy rules;
4. Sharing of information about transactions and experiences for the everyday business purposes of the financial institution’s affiliates, which covers the sharing of transaction and experience information among affiliates as permitted by the related FCRA exception to the definition of “consumer report”;<sup>[2]</sup>
5. Sharing of information about creditworthiness for the everyday business purposes of the financial institution’s affiliates, which covers the sharing of consumer report and some application information under the FCRA after notice and opt out;

6. Use of information by the financial institution's affiliates to market to the consumer, which covers the affiliate information marketing requirements of section 624 of the FCRA; and
7. Sharing of information with nonaffiliates of the financial institution to market to the consumer, which covers the information-sharing and opt-out requirements of sections \_\_\_\_\_.7 and \_\_\_\_\_.10(a) of the privacy rules.

Of these categories, only the sixth relating to affiliate information marketing under the FCRA may be excluded from the list of activities where appropriate. Specifically, a financial institution may exclude this "reason" from the list if it does not have affiliates or does not disclose personal information to affiliates, if the institution's affiliates do not use personal information in a manner that requires an opt-out under the FCRA, or if the institution elects to provide the FCRA affiliate information marketing notice separately. If a financial institution is required to provide an FCRA affiliate information marketing notice and includes this "reason" in its privacy notice, the institution must provide an accompanying opt out of indefinite duration. That is, if the institution wishes to limit a consumer's opt out to five years as is permitted by section 624 of the FCRA, it must use a separate form to do so.

In the middle column of the table, the financial institution must indicate whether it shares personal information for any of the purposes identified. Specifically, a financial institution must state "Yes" or "No" next to each of the above categories of information sharing in order to accurately reflect its information sharing practices.

And, in the right column, the financial institution must indicate whether the consumer may opt out of that type of information sharing. Specifically, for each of the categories described, the institution must provide one of the following three responses, as applicable: (1) "Yes," if it is required to or voluntarily provides an opt out; (2) "No," if it does not provide an opt out; or (3) "We don't share," if it answers "No" in column two.

**Limiting Information Sharing.** The fourth part of page one of the model privacy form provides information on how a consumer may opt out of sharing. A financial institution is only required to include this part if it actually shares information in a manner that requires an opt out. If so, the financial institution must select one or more of the following opt-out methods: (1) telephone; (2) Web site; or (3) mail-in opt-out form. The final rule includes a model form for each type of opt out. Also, an institution that allows consumers to opt out online must provide either a specific Web address that takes consumers directly to the opt-out page, or a general Web address that provides a clear and conspicuous direct link to the opt-out page.

If an institution chooses to provide a mail-in opt-out option, the mail-in form must appear at the bottom of page one. However, this mail-in form is to be included only if the financial institution specifies that consumers may opt out by mail. The mail-in opt-out form must include, as applicable, a check box allowing the consumer to opt out of the various categories of sharing described in the privacy notice. This mail-in opt-out form raises an important consideration for the design of privacy notices; specifically, the reverse side of the mail-in portion of the opt out must not include any content of the model privacy form, so that the language of the privacy notice itself can be retained by the consumer.

**Questions.** The final part of page one of the model privacy form is a "Questions" box that provides contact information through which a consumer can obtain additional information. A financial institution may elect to provide a phone number, Web address or both.

## **Page Two of the Model Privacy Form**

The second page of the model privacy form includes four sections of additional information designed to ensure that all notice content requirements from the privacy rules are addressed in the model privacy form. Specifically, page two of the form includes: (1) a "who we are" section; (2) a "what we do" section; (3) a definitions section; and (4) an "other important information" section.

**Who We Are.** The first part of page two contains a section entitled "Who we are." If two or more financial institutions jointly provide the notice, the institutions must use this section to identify themselves.<sup>[3]</sup> If the list of institutions would exceed four lines, the form must identify the types of

institutions jointly providing the notice and separately identify those institutions, in 8-point font, at the bottom of page two. If a list of institutions is provided at the bottom of page two, it may be provided in a multi-column format. If the list of institutions exceeds the space available on the page, the list may be completed on a third page. This requirement to list all institutions that are jointly providing a notice could prove cumbersome when a large group of affiliated institutions wishes to provide the privacy notice jointly to its customers.

**What We Do.** The second part of page two, entitled “What we do,” provides supplemental information about what the financial institution does with personal information. Specifically, this part is broken down into four subsections: (1) the protection of personal information; (2) the collection of personal information; (3) limitations on a consumer’s ability to opt out; and (4) opt outs on joint accounts.

First, the “What we do” section must identify how the financial institution protects personal information. In this regard, the model privacy form includes specific language that must be included to address the protection of personal information.

Second, the “What we do” section must identify how the financial institution collects personal information. Specifically, the financial institution must include examples of at least five separate instances in which it collects personal information. These examples must be selected from a list identified in the instructions to the model privacy form, which includes, for example, applying for loans, using a credit or debit card, showing a government-issued ID or providing income or employment information. In addition, if a financial institution collects personal information from affiliates, credit bureaus and/or other companies, the institution must include a separate disclosure stating this fact. Only institutions that do not collect any personal information from affiliates, credit bureaus or other companies may omit this disclosure category.

Third, the “What we do” section identifies when the consumer cannot limit the specified types of sharing. This part describes the extent of the consumer’s rights under federal law to limit sharing, and indicates that state law may provide additional rights. In addition to this required “response,” if a financial institution describes state privacy laws in the “Other important information” section (discussed below), the institution must indicate that the consumer can see that section of the form for more information on his or her rights under state law.

And, the “What we do” section identifies what happens when a consumer limits sharing for a joint account. Specifically, the financial institution must choose one of two statements for this section: (1) “Your choices will apply to everyone on your account.”; or (2) “Your choices will apply to everyone on your account—unless you tell us otherwise.” This disclosure only has to be included if the financial institution provides an opportunity to opt out.

**Definitions.** The third part of page two of the model privacy form is the definitions section. Specifically, this section defines the terms “affiliates,” “nonaffiliates” and “joint marketing.” Each definition must be customized by a financial institution. For example, for the definition of the term “affiliates,” the instructions to the model privacy form include three separate statements, one of which a financial institution must include in this section based on whether: (1) it has no affiliates; (2) it has affiliates, but does not share personal information with those affiliates; or (3) it shares personal information with its affiliates.

**Other Important Information.** The final part of page two of the model privacy form is an “other important information” section. This section is optional, but a financial institution may only include two types of information in this section. Specifically, this section may only include the following types of information: (1) a statement relating to state and/or international privacy law requirements; and/or (2) an acknowledgement of receipt form.

### **Institutions That Do Not Use the Model Privacy Form**

As indicated above, financial institutions are not required to use the model form to provide consumers with their privacy policies and opt-out notices. Instead, a financial institution may use a privacy notice that varies from the model privacy form, including a notice consisting of the sample clauses found in the existing privacy rules, so long as the notice complies with the GLBA.

The final rule also amends the privacy rules to provide a unique disclosure for institutions that choose not to use the model privacy form. Under the current rules, if a financial institution shares personal information with nonaffiliated third parties in a manner that does not require it to provide an opportunity to opt out, the institution is only required to state in its privacy notice that it engages in such sharing “as permitted by law.” All of the Agencies except the FTC are amending their rules to allow, as an alternative, a statement that the institution shares this information for its “everyday business purposes,” and to include a list of all applicable examples. The FTC is revising its rule to include a more specific statement that the institution shares this information for its “everyday business purposes, such as to process transactions, maintain account(s), respond to court orders and legal investigations, or report to credit bureaus.”

The following is a link to the Rule, as published in the Federal Register.

<http://edocket.access.gpo.gov/2009/pdf/E9-27882.pdf>

For further information or to discuss these issues at greater length, please contact Rick Fischer, at (202) 887-1566, Andrew Smith, at (202) 887-1558, Obrea Poindexter, at (202) 887-8741, Nathan Taylor, at (202) 778-1644 or Mark Gillett at (213) 892-5289.

---

#### Footnotes

[1] 74 Fed. Reg. 62,890 (Dec. 1, 2009).

[2] It is important to note that it is the GLBA and not the FCRA that requires a financial institution to disclose to a consumer that it shares transaction and experience information with third parties.

[3] This section may be omitted by a financial institution only if it is providing the privacy notice alone and the institution is clearly identified in the “title” on page one.