



OVERVIEW OF LAWS AND REGULATIONS

Privacy

Privacy

Executive Summary:

The privacy regulation, also known as Federal Reserve Regulation P, became effective on November 13, 2000, with mandatory compliance delayed until July 1, 2001. The regulation was issued pursuant to Title V, "Privacy," of the 1999 Gramm-Leach-Bliley Act (GLBA). Title V represents the first broad legislative effort to restrict the information shared by a financial institution about its customers with non-affiliated third parties.

In brief, the privacy regulation sets forth three elements: (1) requires a financial institution to provide notice to its customers about its privacy policies and practices; (2) describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and, (3) provides a method for consumers to prevent the sharing described in element 2. As noted, the privacy regulation is applicable to all financial institutions since individual customers must be apprised of the information sharing practices of their institution, regardless of how liberal or restrictive they might be. If the institution shares information (as described in element 2), the individual is entitled to a written notice of "opt out" which prevents the distribution of nonpublic personal financial information, with some exceptions.

The privacy regulation acknowledges that, in very many instances, the routine business of banking relies on the unrestricted flow of personal financial data to service providers, data processors, regulatory authorities, et. al. Therefore, the regulation attempts to craft a solution that permits the individual consumer to elect limits on the sharing of data while not inhibiting the necessary flow of information for the payments system to function efficiently. This is accomplished through the three principal exceptions in the regulation, sections 13 – 15, addressing joint marketing arrangements, processing and servicing, and other specific, unique circumstances.

The privacy regulation employs a number of very specialized definitions. Terms such as "nonpublic personal information" and the distinctions drawn between such everyday terms as "customer" and "consumer" should be well understood prior to drafting privacy notices or training bank personnel. Because the privacy regulation was drafted in contemplation of its application to an online environment, there are particular provisions directed to those institutions offering electronic products and services. Finally, a distinction in the privacy regulation from most other federal consumer protection regulations is its deference to more consumer-protective state laws governing privacy and information-sharing. This is of particular significance to financial institutions operating on a multi-state basis; monitoring the progress of state legislative efforts may affect the practices of the corporate entity overall.



Business Areas Impacted:

- New Accounts
- Teller Operations
- Deposit Operations/Processing
- Marketing of Accounts
- Customer Service



REQUIREMENTS/RECOMMENDATIONS	TIME FRAME	WRITTEN DOCUMENT OR RECORD
<p>Policy/Procedures</p> <p>Establish a privacy policy that accurately states the institution's collection and use of consumers' financial information. The policy should address all issues pertinent to the flow of information within the institution, some of which might include:</p> <ol style="list-style-type: none"> 1. an <u>inventory</u> of existing information collection practices 2. an <u>evaluation</u> of the need to continue, rescind or add to existing information collection practices and of the efforts needed to comply with the regulation 3. the <u>development</u> of appropriate policies, practices, controls and training 4. the <u>implementation</u> of the regulation and a process for continuous monitoring thereafter. 	<p>Continuing</p>	<p>Privacy Policy</p>
<p>Coverage</p> <p>The Privacy regulation applies only to individuals seeking financial products or services for their personal, family or household use. Its coverage does <i>not</i> extend to individuals acting in a business capacity.</p> <p>The most critical terms to understand are the following:</p> <ol style="list-style-type: none"> 1. <u>Customer & Consumer</u> - A "consumer" is the broader of the two terms, generally defined as an individual seeking a financial product or service for personal, family or household use. A "customer" is a sub-group of consumers, specifically those with whom a financial institution establishes an on-going relationship. 	<p>Continuing</p>	<p>Privacy Policy</p>



REQUIREMENTS/RECOMMENDATIONS	TIME FRAME	WRITTEN DOCUMENT OR RECORD
<p>2. <u>Nonpublic Personal Information (NPI)</u> - This is the term applied to the type of information protected by the Privacy regulation. It is comprised of two other types of information also defined in the regulation: <i>publicly available</i> information (from government records, media distribution, et. al.) that is not personally identifiable information (from sources such as loan applications, credit bureau reports, et. al.)</p>		
<p>Privacy Notices</p> <p>Privacy notices are generally divided into two categories: initial notice and annual notice. The regulation allows for some additional varieties (revised, short form and simplified), but these apply only in fairly narrow circumstances. Since the initial and annual notices will be far more prevalent, this guidance will focus principally on these two types of notices.</p> <p>1. <u>Initial Notice</u> - The initial notice must be provided to:</p> <ul style="list-style-type: none"> a. <i>a consumer</i> prior to sharing any nonpublic personal information about the individual with an unaffiliated third party. b. <i>a customer</i> no later than when a customer relationship is established (although the financial institution may provide the notice even earlier, if it so chooses). <p>2. <u>Annual Notice</u> - The annual notice is exclusive to customers. As a function of the on-going relationship characteristic of a customer relationship, the regulation provides for a periodic communication about financial privacy. In this way, a customer is reminded of the policy and practices of its institution and offers (if applicable), the continuing right to opt out.</p>	<p>No later than at the creation of the customer relationship (initial notice) and Annually (annual notice).</p>	<p>Initial Privacy Notice and Annual Privacy Notice</p>



REQUIREMENTS/RECOMMENDATIONS	TIME FRAME	WRITTEN DOCUMENT OR RECORD
<p>Since the regulation requires that both the initial and annual notice convey the same information elements (§573.6(a)(1-9); see below), the two notices will, most likely, appear similar. However, the regulation does not mandate that either notice be presented in a stand-alone format; the institution may include either notice along with other disclosures, just as long as the regulation's clear and conspicuous standard is satisfied.</p>		
<p>Content of Privacy Notices</p> <p>Ensure that privacy notices include all of the elements required under section 6. Briefly stated, the elements are:</p> <ol style="list-style-type: none"> 1. categories of NPI collected 2. categories of NPI disclosed 3. categories of affiliates and nonaffiliates to whom NPI is disclosed 4. disclosures relating to former customers 5. disclosures relating to joint marketing arrangements 6. description of opt out right and means by which to exercise 7. FCRA disclosures 8. summary of security procedures used to safeguard information <p>This list comprises the <u>minimum</u> level of information. If an institution chooses to include more, there is no explicit prohibition from doing so. However, keep in mind that the clear and conspicuous standard governs the "totality" of the notice's presentation. Any additional content, for example, marketing text, cannot obscure the required elements nor minimize their importance in any way.</p>	<p>Continuing</p>	<p>Privacy Notice(s)</p>



REQUIREMENTS/RECOMMENDATIONS	TIME FRAME	WRITTEN DOCUMENT OR RECORD
<p>Institutions who engage in no information sharing beyond the exceptions granted in sections 14 and 15 are permitted to offer a “simplified” notice at both the initial and annual notice stage. Under the simplified notice criteria (573.6(c)(5)), not all 8 elements must be included.</p>		
<p>Opt Out Notice</p> <p>The Opt Out Notice provides the means by which an individual can notify his/her financial institution that information sharing authority is being withheld. The notice can be a stand-alone document or it can be a component of the Initial or Annual Notice. And, while opt out notices offer a valuable right, they will not be offered by every financial institution because, in many cases, they will be unnecessary. If an institution only shares information falling under a section 14 or 15 exception, there is nothing from which the individual consumer need “opt out.”</p> <p>The Opt Out Notice must contain three separate pieces of information, per section 7(a)(1)(i-iii) of the regulation:</p> <ul style="list-style-type: none"> • that the financial institution discloses, or reserves the right to disclose, nonpublic personal information about its consumers to nonaffiliated third parties; • that the consumer has the right to opt out; and • the means by which the opt out right can be exercised. <p>Industry practices as of this writing generally reveal a preference to merge or append the opt out text to the privacy notice, rather than to provide a separate document. The regulation neither encourages nor discourages this practice; bear in mind, however, that the clear and conspicuous standard applies to</p>	<p>Continuing</p>	<p>Opt Out Notice</p>



REQUIREMENTS/RECOMMENDATIONS	TIME FRAME	WRITTEN DOCUMENT OR RECORD
<p>the opt out portion just as to the privacy notice overall.</p>		
<p>Notice Delivery</p> <p>Section 9 of the Privacy regulation addresses the appropriate methods for delivering the various types of notices. The delivery provisions are considerably detailed, with some uniquely applicable to one type of notice, but not to another. However, the initial paragraph in section 9 establishes a minimum standard that is applicable to <i>all</i> notices:</p> <p style="padding-left: 40px;">“You must provide any notices... that this part requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the customer agrees, electronically.”</p> <p>Overall, the delivery provisions offer guidance rather than a prescriptive approach. The financial institution is directed to employ a standard of “reasonableness” with respect to its customers. To illustrate: the institution cannot reasonably expect that a consumer, who does not conduct any banking business electronically, would be appropriately notified if his privacy notice were to be delivered via e-mail. Similarly, it would not effect a reasonable delivery to the vast majority of retail customers who bank via ATM and U.S. mail to post the institution’s singular privacy notice in the lobby of the main branch facility. Instead, the institution should consider the array of delivery choices and the preferences of its customer base.</p> <p>Section 9, in a few instances, does expressly require or prohibit a particular delivery mechanism. These are:</p> <ul style="list-style-type: none"> • Oral description of notice is insufficient 	<p>Continuing</p>	<p>All Notices (Initial, Annual, Opt out, Revised, Short-form and Simplified)</p>



REQUIREMENTS/RECOMMENDATIONS	TIME FRAME	WRITTEN DOCUMENT OR RECORD
<ul style="list-style-type: none"> For annual notices only, two unique methods of delivery are provided for e-banking customers and for those customers who have requested no postal correspondence For customers only, the various notices must be provided in a format that can be retained or accessed at a later date. 		
<p>Implementing Opt Out Elections</p> <p>Section 7(e) states: “You must comply with a consumer’s opt out direction as soon as reasonably practicable after you receive it.” The “reasonable” concept is explained in the Preamble to the Privacy regulation. Despite the request of many commenters to the proposed rule for a more precise standard, it was a deliberate multi-agency decision to retain a more general rule in light of the wide range of practices throughout the financial institution industry. To do otherwise, agency rationale stated, might disadvantage individual consumers in those situations when it would be within the bank’s ability to act before the prescribed deadline. Conversely, it could be that some financial institutions might face difficulties in complying with overly-rigid timeframes. Further, any standard established using current industry practices and capabilities could be rendered obsolete as advances in technology increase efficiency.</p>	Continuing	Opt Out Notice
<p>Reuse and Redislosure Limitations</p> <p>Section 11 addresses the various restrictions placed on information recipients who succeed the originally intended recipient. There are further qualifications placed on the information depending on whether or not it was shared pursuant to a section 14 or 15 exception to the privacy regulation. The table below offers a simplified graphic of the limitations to which subsequent recipients must adhere pursuant to this section:</p>	Continuing	Any contract(s) entered into by the financial institution and service providers (both affiliated and nonaffiliated).



<u>Nonpublic Personal Information:</u>			
Permissible Reuse and Redisclosure			
Received:			
Under an exception	To the affiliates of the <u>providing</u> financial institution	To the affiliates of the recipient, who are then subject to the same limits as the original recipient regarding reuse and redisclosure	To any party with whom the original recipient must transact business (e.g., subcontractor) in order to carry out the activity giving rise to the § 14/15 exception
Outside an exception	Same as above	Same as above	To any party, if the information could be properly conveyed by the <u>providing</u> financial institution
Disclosed:			
Under an exception	Same as above (i.e., the third party can disclose the info to your affiliates)	Same as above	To any party necessary, in the ordinary course of business, to carry out the activity giving rise to the § 14/15 exception under which you received the information (e.g., your subcontractor)
Outside an exception	Same as above (i.e., the third party can disclose the info to your affiliates)	Same as above	To any party, if the disclosure would be lawful if you, as the providing financial institution, made the disclosure directly to that party



REQUIREMENTS/RECOMMENDATIONS	TIME FRAME	WRITTEN DOCUMENT OR RECORD
<p>Training/Updating</p> <p>Provide training to all employees who perform duties subject to the requirements of the regulation. This would encompass all staff who deal with consumer financial products or services, either in a direct customer-contact role or in a back-office/information processing capacity. Training should precede the individual's access to nonpublic personal information about the institution's customers, if possible.</p> <p>For all other bank personnel, a basic understanding of privacy principles, as well as the institution's implementation of the GLBA privacy regulation, is recommended. At a minimum, this should involve familiarity with the institution's own privacy notice, opt out applicability and a privacy officer/liaison to whom customer inquiries can be directed.</p> <p>Update all applicable policies, procedures and operational manuals to reflect regulatory changes.</p>	<p>Continuing</p> <p>For new hires, prior to handling protected information.</p>	<p>Training Manual(s)</p>
<p>Monitoring/Internal Review</p> <p>Establish and implement standards and controls to supervise accurate execution of procedures and systems.</p>	<p>Continuing</p>	<p>Internal Review</p> <p>Procedures/Reports</p>