

**BUREAU OF CONSUMER FINANCIAL PROTECTION**

**12 CFR Part 1016**

**[Docket No. CFPB-2016-0032]**

**RIN 3170-AA60**

**Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act (Regulation P)**

**AGENCY:** Bureau of Consumer Financial Protection.

**ACTION:** Proposed rule with request for public comment.

**SUMMARY:** The Bureau of Consumer Financial Protection (Bureau) is proposing to amend Regulation P, which requires, among other things, that financial institutions provide an annual notice describing their privacy policies and practices to their customers. The amendment would implement a December 2015 statutory amendment to the Gramm-Leach-Bliley Act providing an exception to this annual notice requirement for financial institutions that meet certain conditions.

**DATES:** Comments must be received on or before **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]**.

**ADDRESSES:** You may submit comments, identified by Docket No. CFPB-2016-0032 or RIN 3170-AA60, by any of the following methods:

- *Electronic:* <http://www.regulations.gov>. Follow the instructions for submitting comments.
- *Mail:* Monica Jackson, Office of the Executive Secretary, Consumer Financial Protection Bureau, 1700 G Street, NW., Washington, DC 20552.
- *Hand Delivery/Courier:* Monica Jackson, Office of the Executive Secretary, Consumer Financial Protection Bureau, 1275 First Street NE., Washington, DC 20002.

*Instructions:* All submissions should include the agency name and docket number or Regulatory Information Number (RIN) for this rulemaking. Because paper mail in the Washington, DC area and at the Bureau is subject to delay, commenters are encouraged to submit comments electronically. In general, all comments received will be posted without change to <http://www.regulations.gov>. In addition, comments will be available for public inspection and copying at 1275 First Street NE., Washington, DC 20002 on official business days between the hours of 10 a.m. and 5 p.m. Eastern Time. You can make an appointment to inspect the documents by telephoning (202) 435-7275.

All comments, including attachments and other supporting materials, will become part of the public record and subject to public disclosure. Sensitive personal information, such as account numbers or Social Security numbers, should not be included. Comments generally will not be edited to remove any identifying or contact information.

**FOR FURTHER INFORMATION CONTACT:** Joseph Devlin and Nora Rigby, Counsels; Office of Regulations, at (202) 435-7700.

**SUPPLEMENTARY INFORMATION:**

**I. Summary of the Proposed Rule**

Title V, Subtitle A of the Gramm-Leach-Bliley Act (GLBA)<sup>1</sup> and Regulation P, which implements the GLBA, mandate that financial institutions provide their customers with annual notices regarding those institutions' privacy policies. If financial institutions share certain consumer information with particular types of third parties, the annual notices must also provide customers with an opportunity to opt out of the sharing. Regulation P sets forth requirements for how financial institutions must deliver these annual privacy notices. In certain circumstances,

---

<sup>1</sup> 15 U.S.C. 6801 through 6809.

Regulation P permits financial institutions to use an alternative delivery method to provide annual notices. This method requires, among other things, that the annual notice be posted on a financial institution's website.

On December 4, 2015, Congress amended the GLBA as part of the Fixing America's Surface Transportation Act (FAST Act). This amendment, titled Eliminate Privacy Notice Confusion,<sup>2</sup> added new GLBA section 503(f). This subsection provides an exception under which financial institutions that meet certain conditions are not required to provide annual privacy notices to customers. Section 503(f)(1) requires that to qualify for this exception, a financial institution must not share nonpublic personal information about customers except as described in certain statutory exceptions. (Sharing as described in these specified statutory exceptions does not trigger the customer's statutory right to opt out of the financial institution's sharing.) In addition, section 503(f)(2) requires that the financial institution must not have changed its policies and practices with regard to disclosing nonpublic personal information from those that the institution disclosed in the most recent privacy notice it sent.

The Bureau proposes to amend Regulation P to implement this GLBA amendment. As part of its implementing proposal, the Bureau also proposes to amend Regulation P to provide timing requirements for delivery of annual privacy notices if a financial institution that qualified for this annual notice exception later changes its policies or practices in such a way that it no longer qualifies for the exception. The Bureau further proposes to remove the Regulation P provision that allows for use of the alternative delivery method for annual privacy notices because the Bureau believes the alternative delivery method will no longer be used in light of the

---

<sup>2</sup> FAST Act, Public Law 114-94, section 75001.

annual notice exception. Finally, the Bureau proposes to amend Regulation P to make a technical correction to one of its definitions.

## **II. Background**

### *A. The Statute and Regulation*

The GLBA was enacted into law in 1999 and governs the privacy practices of a broad range of financial institutions.<sup>3</sup> Rulemaking authority to implement the GLBA privacy provisions was initially spread among many agencies. The Federal Reserve Board (Board), the Office of Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS) jointly adopted final rules in 2000 to implement the notice requirements of the GLBA.<sup>4</sup> The National Credit Union Administration (NCUA), Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), and Commodity Futures Trading Commission (CFTC) were part of the same interagency process, but each of these agencies issued separate rules.<sup>5</sup> In 2009, all of the agencies with the authority to issue rules to implement the GLBA privacy provisions issued a joint final rule with a model form that financial institutions could use, at their option, to provide required initial and annual disclosures.<sup>6</sup>

In 2011, the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act)<sup>7</sup> transferred GLBA privacy notice rulemaking authority from the Board, NCUA, OCC,

---

<sup>3</sup> Public Law 106–102, 113 Stat. 1338 (1999).

<sup>4</sup> 65 FR 35162 (June 1, 2000).

<sup>5</sup> 65 FR 31722 (May 18, 2000) (NCUA final rule); 65 FR 33646 (May 24, 2000) (FTC final rule); 65 FR 40334 (June 29, 2000) (SEC final rule); 66 FR 21236 (Apr. 27, 2001) (CFTC final rule).

<sup>6</sup> 74 FR 62890 (Dec. 1, 2009).

<sup>7</sup> Public Law 111–203, 124 Stat. 1376 (2010).

OTS, the FDIC, and the FTC (in part) to the Bureau.<sup>8</sup> The Bureau then restated the implementing regulations in Regulation P, 12 CFR part 1016, in late 2011.<sup>9</sup>

The Bureau has the authority to promulgate GLBA privacy rules for depository institutions and many non-depository institutions. However, rulewriting authority with regard to securities and futures-related companies is vested in the SEC and CFTC, respectively, and rulewriting authority with respect to certain motor vehicle dealers is vested in the FTC.<sup>10</sup> The four agencies are required to consult with each other and with representatives of State insurance authorities to assure, to the extent possible, consistency and comparability between implementing rules.<sup>11</sup> Toward that end, the Bureau has consulted and coordinated with these agencies and with the National Association of Insurance Commissioners (NAIC) concerning this proposed rule. The Bureau has also consulted with prudential regulators and other appropriate Federal agencies, as required under Section 1022 of the Dodd-Frank Act as part of its general rulewriting process.<sup>12</sup>

The GLBA and Regulation P require that financial institutions provide consumers with certain notices describing their privacy policies.<sup>13</sup> Financial institutions are generally required to provide an initial notice of these policies when a customer relationship is established and to

---

<sup>8</sup> Public Law 111-203, section 1093. The FTC retained rulewriting authority over any financial institution that is a person described in 12 U.S.C. 5519 (*i.e.*, motor vehicle dealers predominantly engaged in the sale and servicing of motor vehicles, the leasing and servicing of motor vehicles, or both).

<sup>9</sup> 76 FR 79025 (Dec. 21, 2011).

<sup>10</sup> 15 U.S.C 6804; 12 CFR 1016.1(b).

<sup>11</sup> 15 U.S.C. 6804(a)(2).

<sup>12</sup> 12 U.S.C. 5512(b)(2)(B).

<sup>13</sup> When a financial institution has a continuing relationship with the consumer, an annual privacy notice is required and the consumer is then referred to as a “customer.” 12 CFR 1016.3(i); 1016.3(j)(1).

provide an annual notice to customers every year that the customer relationship continues.<sup>14</sup> Except as otherwise authorized in the regulation, if a financial institution chooses to disclose nonpublic personal information about a consumer to a nonaffiliated third party other than as described in its initial notice, the institution is also required to deliver a revised privacy notice.<sup>15</sup> The types of information required to be included in the initial, annual, and revised notices are identical. Each notice must describe whether and how the financial institution shares consumers' nonpublic personal information with other entities.<sup>16</sup> The notices must also briefly describe how financial institutions protect the nonpublic personal information they collect and maintain.<sup>17</sup>

Section 502 of the GLBA and Regulation P also require that initial, annual, and revised notices provide information about the right to opt out of certain financial institution sharing of nonpublic personal information with some types of nonaffiliated third parties. For example, a mortgage customer has the right to opt out of a financial institution disclosing his or her name and address to an unaffiliated home insurance company. On the other hand, a financial institution is not required to allow a consumer to opt out of the institution's disclosure of his or her nonpublic personal information to third party service providers and pursuant to joint marketing arrangements subject to certain requirements; disclosures relating to maintaining and servicing accounts, securitization, law enforcement and compliance, and consumer reporting; and certain other disclosures described in the GLBA and Regulation P as exceptions to the opt-out requirement.<sup>18</sup>

---

<sup>14</sup> 12 CFR 1016.4(a)(1); 12 CFR 1016.5(a)(1). Financial institutions are also required to provide initial notices to consumers before disclosing any nonpublic personal information to a nonaffiliated third party outside of certain exceptions. 12 CFR 1016.4(a)(2).

<sup>15</sup> 12 CFR 1016.8.

<sup>16</sup> 12 CFR 1016.6(a)(1)-(5), (9).

<sup>17</sup> 12 CFR 1016.6(a)(8).

<sup>18</sup> 15 U.S.C. 6802(b)(2), (e); 12 CFR 1016.13, 1016.14, 1016.15.

In addition to opt-out rights under the GLBA, annual privacy notices also may include information about certain consumer opt-out rights under the Fair Credit Reporting Act (FCRA). The privacy notices under the GLBA/Regulation P and affiliate disclosures under the FCRA/Regulation V interact in two ways. First, section 603(d)(2)(A)(iii) of the FCRA excludes from that statute's definition of a consumer report<sup>19</sup> the sharing of certain information about a consumer with the institution's affiliates if the consumer is notified of such sharing and is given an opportunity to opt out.<sup>20</sup> Section 503(c)(4) of the GLBA and Regulation P require financial institutions to incorporate into any required Regulation P notices the notification and opt-out disclosures provided pursuant to section 603(d)(2)(A)(iii) of the FCRA, if the institution provides such disclosures.<sup>21</sup>

Second, section 624 of the FCRA and Regulation V's Affiliate Marketing Rule provide that an affiliate of a financial institution that receives certain information (*e.g.*, transaction history)<sup>22</sup> from the institution about a consumer may not use the information to make solicitations for marketing purposes unless the consumer is notified of such use and provided with an opportunity to opt out of that use.<sup>23</sup> Section 624 of the FCRA and Regulation V also permit (but do not require) financial institutions to incorporate any opt-out disclosures provided

---

<sup>19</sup> The FCRA defines "consumer report" generally as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for: (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. 1681a(d).

<sup>20</sup> 15 U.S.C. 1681a(d)(2)(A)(iii).

<sup>21</sup> 15 U.S.C. 6803(c)(4); 12 CFR 1016.6(a)(7).

<sup>22</sup> The type of information to which section 624 applies is information that would be a consumer report, but for the exclusions provided by section 603(d)(2)(A)(i), (ii), or (iii) of the FCRA (*i.e.*, a report solely containing information about transactions or experiences between the consumer and the institution making the report, communication of that information among persons related by common ownership or affiliated by corporate control, or communication of other information as discussed above).

<sup>23</sup> 15 U.S.C. 1681s-3 and 12 CFR pt. 1022, subpart C.

under section 624 of the FCRA and subpart C of Regulation V into privacy notices provided pursuant to the GLBA and Regulation P.<sup>24</sup>

*B. The Alternative Delivery Method for Annual Privacy Notices*

In pursuit of the Bureau's goal of reducing unnecessary or unduly burdensome regulations, the Bureau in December 2011 issued a Request for Information (RFI) seeking specific suggestions from the public for streamlining regulations the Bureau had inherited from other Federal agencies. In that RFI, the Bureau specifically identified the annual privacy notice as a potential opportunity for streamlining and solicited comment on possible alternatives to delivering the annual privacy notice.<sup>25</sup> Numerous industry commenters responded to the RFI by advocating for the elimination or limitation of the annual notice requirement.

Financial institutions historically have provided annual notices generally by U.S. postal mail.<sup>26</sup> In 2014, the Bureau adopted a rule to allow financial institutions to use an alternative delivery method to provide annual privacy notices through posting the notices on their websites if they meet certain conditions.<sup>27</sup> Specifically, financial institutions can use the alternative delivery method for annual notices if: (1) no opt-out rights are triggered by the financial institution's information sharing practices under the GLBA; (2) no FCRA section 603 opt-out notices are required to appear on the annual notice and any opt-outs required by FCRA section 624 had previously been provided, if applicable, or the annual notice is not the only notice provided to satisfy those requirements; (3) the information included in the annual notice has not

---

<sup>24</sup> 15 U.S.C. 1681s-3(b); 12 CFR 1022.23(b).

<sup>25</sup> 76 FR 75825, 75828 (Dec. 5, 2011).

<sup>26</sup> Regulation P, however, does allow financial institutions to provide notices electronically (*e.g.*, by email) with consent. 12 CFR 1016.9(a) (stating that a financial institution may deliver the notice electronically if the consumer agrees). The Bureau believes that most consumers do not receive privacy notices electronically.

<sup>27</sup> 79 FR 64057 (revising 12 CFR 1016.9(c)). The Bureau's alternative delivery method became effective on October 28, 2014. *Id.*



changed since the customer received the previous notice; and (4) the financial institution uses the model form provided in Regulation P as its annual notice.

In addition, to assist customers with limited or no access to the internet, an institution using the alternative delivery method is required to mail annual notices to customers who request them by telephone. To make customers aware that its annual privacy notice is available through the website or by phone, the institution is required to include a clear and conspicuous statement of availability at least once per year on an account statement, coupon book, or a notice or disclosure the institution issues under any provision of law.

### *C. Statutory Amendment*

On December 4, 2015, Congress amended the GLBA as part of the FAST Act. This amendment, titled Eliminate Privacy Notice Confusion,<sup>28</sup> added new GLBA section 503(f), which provides an exception under which financial institutions that meet two conditions are not required to provide annual notices to customers.<sup>29</sup> New GLBA section 503(f)(1) states the first condition for the annual notice exception: that a financial institution must provide nonpublic personal information only in accordance with certain exceptions in GLBA; providing nonpublic personal information under these exceptions does not trigger consumer opt-out rights.<sup>30</sup> New GLBA section 503(f)(2) states the second condition for the annual notice exception: that a financial institution must not have changed its policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed in the most

---

<sup>28</sup> FAST Act, Public Law 114-94, section 75001.

<sup>29</sup>The Bureau notes that a financial institution that qualifies for the annual notice exception could provide a privacy notice to a customer without jeopardizing the availability of the exception, such as in response to a customer specifically requesting a copy of the notice.

<sup>30</sup> These provisions are GLBA section 502(b)(2) or (e) and are incorporated into existing Regulation P at § 1016.13, § 1016.14, and § 1016.15. They provide exceptions from the requirement that a financial institution provide notice and an opportunity to opt out of sharing nonpublic personal information with a nonaffiliated third party.

recent disclosure sent to consumers in accordance with GLBA section 503. The statutory amendment became effective upon enactment in December 2015. This proposed rule would implement the statutory amendment.

#### *D. Effective Date*

As discussed above, the statutory exception to the annual notice requirement is already effective. The Bureau contemplates that these proposed amendments to Regulation P would be effective 30 days after any final rule is published in the *Federal Register*.

#### *E. Privacy Considerations*

In developing this proposed rule, the Bureau considered its potential impact on consumer privacy. The proposed rule would not affect the collection or use of consumers' nonpublic personal information by financial institutions. The proposal implements a new statutory exception to limit the circumstances under which financial institutions subject to Regulation P will be required to deliver annual privacy notices to their customers. Delivery of annual privacy notices is required under the proposal if financial institutions make certain types of changes to their privacy policies or if their annual notices afford customers the right to opt out of financial institutions' sharing of customers' nonpublic personal information under the GLBA. The statutory exception does not affect the requirement to deliver an initial privacy notice, and all consumers will continue to receive such notices describing the privacy policies of any financial institutions with which they do business to the extent currently required.

### **III. Legal Authority**

The Bureau is issuing this proposed rule pursuant to its authority under section 504 of the GLBA, as amended by section 1093 of the Dodd-Frank Act.<sup>31</sup> The Bureau is also issuing this rule pursuant to its authority under sections 1022 and 1061 of the Dodd-Frank Act.<sup>32</sup> The Bureau seeks comment on all aspects of the proposal.

### **IV. Section-by-Section Analysis**

#### *Section 1016.3 Definitions*

##### *3(s)(1)*

In addition to proposed changes below to implement the amendment to GLBA section 503, the Bureau proposes a technical amendment to a definition in Regulation P. Regulation P's substantive requirements, including the requirement to deliver privacy notices, are generally imposed upon entities that meet the definition of "You" in § 1016.3(s)(1). That provision defines "You" as a "financial institution or other person for which the Bureau has rulemaking authority under section 504(a)(1)(A) of the GLBA." The Bureau has rulemaking authority over entities other than financial institutions pursuant to GLBA section 504(a)(1)(A).<sup>33</sup> The statute's privacy notice requirements, however, specifically only apply to financial institutions.<sup>34</sup> The Bureau therefore believes that the definition of "You" in § 1016.3(s)(1) should be limited to financial institutions.

---

<sup>31</sup> 15 U.S.C. 6804.

<sup>32</sup> 12 U.S.C. 5512, 5581.

<sup>33</sup> Such rulemaking authority has been exercised with respect to nonaffiliated third parties to which a financial institution discloses nonpublic personal information and that third party's affiliates for purposes of GLBA section 502(c)'s limits on reuse of information. *See* 12 CFR 1016.11(c)-(d).

<sup>34</sup> *See* GLBA sections 502(a)-(b) and 503(a).

To ensure consistency between Regulation P and the GLBA, the Bureau proposes a technical amendment to § 1016.3(s)(1) to remove “or other persons.” With this change, the definition of “You” is limited to financial institutions. The Bureau does not believe this technical amendment to § 1016.3(s)(1) will change the settled understanding of the scope of Regulation P’s privacy notice requirements. Instead, the Bureau believes it will clarify that the scope of Regulation P’s privacy notice requirements is consistent with the understanding of stakeholders. The Bureau invites comment on this proposed technical amendment.

### *Section 1016.5 Annual Privacy Notice to Customers Required*

#### *5(a) General Rule*

The proposed rule would amend the general requirement in § 1016.5(a)(1) that financial institutions provide annual notices, to clarify that the Bureau has added an exception to this requirement in § 1016.5(e) to incorporate the amendment to GLBA section 503.

#### *5(e) Exception to Annual Notice Requirement*

The Bureau proposes to add new § 1016.5(e) to incorporate into Regulation P the exception created by new section 503(f) of the GLBA. Under proposed § 1016.5(e), as in section 503(f), a financial institution would be exempt from providing an annual notice if it meets the two conditions described below.

##### *5(e)(1) When Exception Available*

###### *5(e)(1)(i)*

New GLBA section 503(f)(1) states the first condition for the annual privacy notice exception: that a financial institution provide nonpublic personal information only in accordance with the provisions of subsection (b)(2) or (e) of section 502 of the GLBA; these provisions describe disclosures concerning sharing with nonaffiliated third parties that do not trigger

consumer opt-out rights. Proposed § 1016.5(e)(1)(i) would incorporate this condition by requiring that to qualify for the annual notice exception, any nonpublic personal information that financial institutions provide to nonaffiliated third parties must be provided only in accordance with § 1016.13, § 1016.14 or § 1016.15 of Regulation P; these regulatory sections implement subsections (b)(2) and (e) of section 502.<sup>35</sup> A financial institution sharing information pursuant to these exceptions is not required to provide customers with a right to opt out of that sharing.

The Bureau notes that § 1016.6(a)(7) requires that annual privacy notices incorporate opt-out disclosures provided under FCRA section 603(d)(2)(A)(iii). Further, the notices may incorporate opt-out disclosures provided under FCRA section 624.<sup>36</sup> GLBA section 503(f)(1) does not mention these FCRA opt-out disclosures. Based on its expertise and experience with respect to consumer financial markets, the Bureau is proposing that the presence or absence of these FCRA disclosures on a financial institution's privacy notice would not affect whether the institution satisfies GLBA section 503(f)(1) and proposed § 1016.5(e)(1)(i). The Bureau notes, however, that financial institutions that choose to take advantage of the annual notice exception must still provide any opt-out disclosures required under FCRA sections 603(d)(2)(A)(iii) and 624, if applicable. Under the FCRA, neither of these opt-outs is required to be provided annually.<sup>37</sup> Accordingly, institutions can provide these disclosures through other methods, for example, through their initial privacy notices in most circumstances.

---

<sup>35</sup> The sharing described in these provisions includes, among other things, sharing involving third party service providers, joint marketing arrangements, maintaining and servicing accounts, securitization, law enforcement and compliance, and reporting to consumer reporting agencies.

<sup>36</sup> 15 U.S.C. 1681s-3(b); 12 CFR 1022.23(b).

<sup>37</sup> See 15 U.S.C. 1681a(d)(2)(A)(iii); 12 CFR 1022.21, 1022.27; 72 FR 62910, 62930 (Nov. 7, 2007).

*5(e)(1)(ii)*

New GLBA section 503(f)(2) states the second condition for the annual notice exception: that a financial institution not have changed its policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed in the most recent notice sent to consumers in accordance with GLBA section 503. Proposed § 1016.5(e)(1)(ii) would incorporate this provision by requiring that, to qualify for the annual notice exception, a financial institution must not have changed its policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed to the customer under § 1016.6(a)(2) through (5) and (9) in the most recent privacy notice the financial institution provided.

Paragraphs (1) through (9) of § 1016.6(a) list the specific information that must be included in privacy notices. Section 1016.6(a)(2) through (5) and (9) require a financial institution to include information related to its policies and practices with regard to disclosing nonpublic personal information, but § 1016.6(a)(1) (information collection) and § 1016.6(a)(8) (confidentiality and security) do not.<sup>38</sup> Based on its expertise and experience with respect to consumer financial markets, the Bureau proposes that only changes to an institution's policies and practices that would require changes to any of the disclosures required by § 1016.6(a)(2) through (5) and (9) would cause a financial institution to be unable to use the exception in proposed § 1016.5(e)(1)(ii).<sup>39</sup>

---

<sup>38</sup> The information specified in § 1016.6(a)(6) describes the consumer's right pursuant to Regulation P to opt out of an institution's disclosure of information and would be inapplicable where a financial institution qualifies for the annual notice exception.

<sup>39</sup> To use the Bureau's alternative delivery method, the information a financial institution is required to convey on its annual privacy notice pursuant to § 1016.6(a)(1) through (5), (8), and (9) must not have changed from the information disclosed in the most recent privacy notice provided to the consumer. 12 CFR 1016.9(c)(2)(D). Thus, changes to the information a financial institution is required to convey pursuant to § 1016.6(a)(1) and (8) would

Section 1016.6(a)(7) requires that any disclosures an institution makes under FCRA section 603(d)(2)(A)(iii), which describe sharing with an institution's affiliates, be included on the privacy notice. The statute does not clearly state whether a financial institution that changes its policies and practices with regard to disclosing nonpublic personal information *to affiliates* satisfies the requirement in GLBA section 503(f)(2). The Bureau believes that the statute could be interpreted such that a financial institution that changes its disclosure required under § 1016.6(a)(7) would not satisfy GLBA section 503(f)(2). The Bureau seeks comment on whether proposed § 1016.5(e)(1)(ii) should include changes to disclosures required by § 1016.6(a)(7) and on how frequently institutions change that disclosure. The Bureau further seeks comment on whether institutions would prefer to inform customers of these changes through sending an annual privacy notice or through sending a disclosure describing only the FCRA section 603(d)(2)(A)(iii) opt-outs and seeks comment on the impact on consumers of these two methods.

The Bureau notes that a financial institution would satisfy proposed § 1016.5(e)(1)(ii) if it changes its disclosures describing policies and practices with regard to disclosing nonpublic personal information that are included in the institution's privacy notice without being required by GLBA or § 1016.6 (*e.g.*, disclosures describing sharing with affiliates under FCRA section 624 or voluntary disclosures and opt-outs). The Bureau seeks comment on whether changes to

---

prevent a financial institution from using the alternative delivery method but such changes would not prevent a financial institution from satisfying proposed § 1016.5(e)(1)(ii) for the annual notice exception. Because institutions that include information on their privacy notice pursuant to § 1016.6(a)(7) (which relates to opt-out notices provided pursuant to the FCRA) are not permitted to use the alternative delivery method in any case, § 1016.6(a)(7) is not listed as a type of information that if changed would prevent a financial institution from using the alternative delivery method.

disclosures that are not required to be included in privacy notices by the GLBA or § 1016.6 should cause an institution not to satisfy proposed § 1016.5(e)(1)(ii).

*5(e)(2) Delivery of Annual Privacy Notice after Financial Institution No Longer Meets Requirements for Exception*

New GLBA section 503(f) states that a financial institution that meets the requirements for the annual notice exception will not be required to provide annual notices “until such time” as that financial institution fails to comply with the criteria described in section 503(f)(1) and 503(f)(2), which would be implemented in proposed § 1016.5(e)(1)(i) and (ii). A financial institution may no longer meet the requirements for the exception either by beginning to share nonpublic personal information in ways that trigger rights to opt-out notices under GLBA and Regulation P, or by otherwise changing its policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed in the most recent privacy notice the financial institution provided.

Financial institutions that no longer meet the conditions for the exception must provide customers with annual privacy notices. The GLBA, including new GLBA section 503(f), does not clearly specify when institutions must provide these notices. The statute could be read to require the financial institution to actually provide an annual privacy notice by the time it changes its policies or practices such that it no longer qualifies for the exception. Alternatively, it could be read to subject the financial institution, at the time it changes its policies or practices such that it no longer qualifies for the exception, to the requirement to provide an annual privacy notice while being silent as to the timing for actually providing an annual privacy notice. Pursuant to its authority in GLBA section 504 to issue rules to implement the GLBA and based on its expertise and experience with respect to consumer financial markets, the Bureau proposes



to adopt this second reading and issue standards for when institutions must provide these notices. Specifically, the Bureau is using its rulemaking authority under GLBA section 504(a) to propose in § 1016.5(e)(2) timing requirements for providing an annual notice in these circumstances. The Bureau is proposing to establish these requirements to ensure that delivery of the annual privacy notice in these circumstances is consistent with the existing timing requirements for privacy notices in the regulation, where applicable, and to provide clarity to financial institutions regarding these requirements.

In developing the proposed framework, the Bureau has looked to existing requirements under the statute and regulation because they already address circumstances in which a financial institution might change its policies and procedures in a way that affects the content of the notices. Specifically, § 1016.8 requires that the financial institution provide a revised notice to consumers *before* implementing certain types of changes; in other cases, the statute and regulation currently contemplate that a change in policy and procedure that affects the content of the notices would simply be reflected on the next regular annual notice provided to the customer. The Bureau is therefore proposing different timing requirements for the resumption of annual notices, depending on whether the change at issue would trigger the requirement for a revised notice under § 1016.8 prior to the change taking effect.

Accordingly, the timing requirements in proposed § 1016.5(e)(2) would differ depending on whether the change that causes the financial institution to no longer satisfy the conditions for the annual notice exception also triggers a requirement under existing Regulation P to deliver a revised notice. Section 1016.8 currently requires that financial institutions provide revised notices to consumers before the institutions share nonpublic personal information with a nonaffiliated third party if their sharing would be different from what the institution described in

the initial notice it delivered. After delivering the revised notice, the financial institution must also give the consumer a reasonable opportunity to opt out of any new information sharing beyond the Regulation P exceptions before the new sharing occurs.

*5(e)(2)(i) Changes Preceded by a Revised Privacy Notice*

For changes to a financial institution's policies or practices that cause it to no longer satisfy the conditions for the exception and also trigger an obligation to send a revised notice prior to the change, the Bureau proposes in § 1016.5(e)(2)(i) that financial institutions would be required to resume delivery of their subsequent regular annual notices pursuant to the existing timing requirements that govern delivery of annual notices generally. Because the revised notice informs the customer of the institution's changed policies and practices before any new sharing occurs, the Bureau believes that there is no clear urgency regarding delivery of the first annual notice subsequent to implementation of the new policies and procedures.

Specifically, § 1016.4(a)(1) generally requires a financial institution to provide an initial notice to an individual who becomes the institution's customer no later than when it establishes a customer relationship. Section 1016.5(a) requires a financial institution to provide a privacy notice to its customers "not less than annually" during the continuation of any customer relationship. Section 1016.5(a)(1) defines annually to mean "at least once in any period of 12 consecutive months." It further provides that a financial institution "may define the 12-consecutive-month period, but [] must apply it to the customer on a consistent basis." Section 1016.5(a)(2) provides an example of the meaning of "annually" in relation to the delivery of the first annual notice after the initial notice:

You provide a notice annually if you define the 12-consecutive-month period as a calendar year and provide the annual notice to the customer once in each calendar year following the calendar year in which you provided the initial notice. For

example, if a customer opens an account on any day of year 1, you must provide an annual notice to that customer by December 31 of year 2.

The example in § 1016.5(a)(2) provides financial institutions with the flexibility to select a specific date during the year to provide annual notices to all customers, regardless of when a particular customer relationship began. This flexibility avoids burdening institutions with either having to provide annual notices on the anniversary of initial notices, or alternatively providing two notices in the first year of the customer relationship to get all accounts originated in a given calendar year on the same cycle for delivering subsequent annual notices.

The Bureau proposes that the approach to timing of the annual notice in § 1016.5(a)(2) be applied if a financial institution makes a change that causes it to lose the exception and triggers the requirement to deliver a revised notice prior to the change. Under the proposed approach, if a financial institution provides a revised notice on any day of year 1 in advance of changing its policies or practices such that it loses the exception, that revised notice would be treated as analogous to an initial notice in § 1016.5(a)(2). Assuming that the financial institution defines the 12-month period as the calendar year, the financial institution would have to provide the first annual notice after losing the exception by December 31 of year 2.

The Bureau proposes to use the same approach in proposed § 1016.5(e)(2)(i) as in existing § 1016.5(a)(2) for two reasons. First, customers would have received a revised notice informing them of the change in the financial institution's policies or practices before the change occurred, and thus customers would not be harmed by allowing the financial institution a longer period of time in which to deliver the first annual notice after the annual notice exception has been lost. Second, this approach would preserve flexibility for financial institutions and avoid requiring them to deliver a revised notice and an annual notice in the same year in order to choose a convenient delivery date for annual notices for all customers. The Bureau believes this

flexibility is justified because a financial institution that is required to deliver a revised privacy notice pursuant to § 1016.8 may have continuing annual notice obligations after the exception is lost. This is the case because such an institution could be sharing other than as described in the Regulation P exceptions and thus fail to satisfy proposed § 1016.5(e)(1)(i), making the annual notice exception unavailable in future years.

The Bureau requests comment on the timing for delivery of annual notices proposed in § 1016.5(e)(2)(i) generally and specifically on whether another timing method or a stated period of time would be more appropriate, and if so, what that period of time should be.

*5(e)(2)(ii) Changes Not Preceded by a Revised Privacy Notice*

Proposed § 1016.5(e)(2)(ii) would specify a deadline for delivering the annual notice for financial institutions that change their policies and practices in such a way as to lose the exception, but do not share information in a way that triggers the requirement under § 1016.8 to deliver a revised notice prior to the change. For these changes, the proposal would require a financial institution to deliver the annual notice within 60 days after the change that caused the institution to lose the exception. The Bureau proposes this 60-day period for providing the annual notice in this situation because customers would not receive a revised notice from the financial institution prior to the institution's change in policies or practices. The Bureau believes that delivery of the annual privacy notice within a relatively short time is necessary and appropriate to inform customers of the change.

In addition, the Bureau believes that this deadline would not impose undue or unreasonable costs on financial institutions, particularly since the delivery requirement is effectively a one-time burden absent additional changes to their policies and practices. Specifically, after providing the one annual notice, the financial institution would once again

meet both of the conditions for the exception—it would not be sharing other than as described in a Regulation P exception and its policies and practices would not have changed since it provided the annual notice. Because the financial institution would once again meet the conditions for the exception, it would not be required to provide future annual notices. In other words, these financial institutions would likely lose the exception for only a single year. Given that financial institutions in this situation would have no continuing obligation at all to send annual notices, they would not need flexibility in choosing a convenient delivery date for future annual notices.<sup>40</sup>

The Bureau also notes that financial institutions have substantial flexibility in managing the burden involved in sending the one annual notice because institutions can choose when they change their policies or practices. Accordingly, an institution could choose when to make the change triggering the commencement of the 60-day period for delivery of the annual notice, so that the date of delivery can be as convenient and low-cost as possible. The Bureau requests comment on whether 60 days is an appropriate period for delivering annual notices in these circumstances or if another period would be more appropriate.

*5(e)(2)(iii) Example*

Proposed § 1016.5(e)(2)(iii) would provide an example for when an institution must provide an annual notice after changing its policies or practices such that it no longer meets the requirements for the annual notice exception set forth in proposed § 1016.5(e)(1). The Bureau proposes this example to facilitate compliance with proposed § 1016.5(e)(2). The proposed example would assume that an institution changes its policies or practices effective April 1 of

---

<sup>40</sup> If the financial institution were to make changes in the future to its practices and policies, these changes could trigger a new obligation to provide annual privacy notices.

year 1 and defines the 12-consecutive-month period pursuant to existing § 1016.5(a)(1) as a calendar year. Proposed § 1016.5(e)(2)(iii) states that the institution must provide an annual notice by December 31 of year 2 if the institution were required to provide a revised notice prior to the change and provided that revised notice on March 1 of year 1 in advance of the change. Proposed § 1016.5(e)(2)(iii) further states that the institution must provide an annual notice by May 30 of year 1 if the institution were not required to provide a revised notice prior to the change. The Bureau invites comment on proposed § 1016.5(e)(2)(iii) generally and specifically on whether it would facilitate compliance with proposed § 1016.5(e)(2).

#### *Section 1016.9 Delivering Privacy and Opt Out Notices*

##### *9(c)(2) Alternative Delivery Method for Providing Certain Annual Notices*

As discussed in Part II, the Bureau amended Regulation P in October 2014 to allow financial institutions that meet certain criteria to deliver annual notices pursuant to the “alternative delivery method.” The Bureau adopted the alternative delivery method to reduce information overload for consumers receiving duplicative mailed annual privacy notices and to reduce the cost to financial institutions from delivering them. Financial institutions that meet the conditions in Regulation P to use the alternative delivery method also would meet the conditions for the statutory exception in section 503(f). Financial institutions that use the alternative delivery method to decrease their cost of delivering annual notices may now entirely eliminate the cost by not sending the notices at all. Because the alternative delivery method is no longer necessary to decrease burden in light of the new statutory exception in section 503(f), the Bureau proposes to remove the alternative delivery method from Regulation P.

Specifically, any financial institution that meets the conditions to use the alternative delivery method will also meet the conditions to be excepted from delivering an annual privacy

notice pursuant to new GLBA section 503(f) because the two conditions that must be met for section 503(f) to apply are closely related to conditions for using the alternative delivery method. First, new GLBA section 503(f)(1) is substantively identical to the first requirement for using the alternative delivery method:<sup>41</sup> that the financial institution share nonpublic personal information about customers with nonaffiliated third parties only in ways that do not give rise to the customer's right to opt out of that sharing.<sup>42</sup> Second, new GLBA section 503(f)(2) is similar to the fourth requirement for using the alternative delivery method: that the institution must not have changed its policies and practices with regard to disclosing nonpublic personal information from those that were disclosed to the customer in the most recent privacy notice.<sup>43</sup> Accordingly, any financial institution that meets the requirement in § 1016.9(c)(2)(i)(D) would also meet the requirement of section 503(f)(2).

The Bureau believes that a financial institution that had both options available to it would choose not to send the annual privacy notice at all, rather than to deliver it pursuant to the alternative delivery method, so that it can eliminate rather than merely reduce the cost of providing annual notices. Given that any financial institution that qualifies to use the alternative delivery method for its annual notices also meets the qualifications for the new annual notice exception, the Bureau believes that including the alternative delivery method in Regulation P is no longer useful.

---

<sup>41</sup> 12 CFR 1016.9(c)(2)(i)(A).

<sup>42</sup> This sharing is pursuant to GLBA section 503(b)(2) and (e), which correspond to Regulation P § 1016.13, § 1016.14, and § 1016.15.

<sup>43</sup> 12 CFR 1016.9(c)(2)(i)(D). The requirement in § 1016.9(c)(2)(i)(D) is somewhat more restrictive because it requires a financial institution not to have changed its practices with respect to disclosing nonpublic personal information and protecting the confidentiality and security of nonpublic personal information whereas section 503(f)(2) requires that the institution not have changed its policies only with respect to disclosing nonpublic personal information. See the section-by-section analysis of proposed § 1016.5(e)(1)(ii) for further discussion.

The Bureau notes that financial institutions that delivered annual notices using the alternative delivery method while it was in effect have complied with Regulation P, notwithstanding that the alternative delivery method provisions may ultimately be removed from the regulation, as proposed. The Bureau further notes that financial institutions that qualify for the new exception may still choose to post privacy notices on their websites or deliver privacy notices to consumers who request them. Such activities would not affect a financial institution's eligibility for the new 503(f) exception.

Accordingly, the Bureau proposes to remove § 1016.9(c)(2) and to renumber existing § 1016.9(c)(1) as § 1016.9(c). The Bureau invites comment on its proposal to remove the alternative delivery method.

## **V. Section 1022(b)(2) of the Dodd-Frank Act**

### *A. Overview*

In developing the proposed rule, the Bureau has considered the potential benefits, costs, and impacts.<sup>44</sup> The Bureau requests comment on the preliminary analysis presented below as well as the submission of additional data that could inform the Bureau's analysis of the benefits, costs, and impacts of the rule. The Bureau has consulted and coordinated with the SEC, CFTC, FTC, and NAIC, and consulted with or offered to consult with the OCC, Federal Reserve Board, FDIC, NCUA, and HUD, including regarding consistency with any prudential, market, or systemic objectives administered by such agencies.

---

<sup>44</sup> Specifically, section 1022(b)(2)(A) of the Dodd-Frank Act calls for the Bureau to consider the potential benefits and costs of a regulation to consumers and covered persons, including the potential reduction of access by consumers to consumer financial products or services; the impact on depository institutions and credit unions with \$10 billion or less in total assets as described in section 1026 of the Dodd-Frank Act; and the impact on consumers in rural areas.



The proposal would implement the December 2015 amendment to the GLBA and amend § 1016.5 of Regulation P to provide that a financial institution is not required to deliver an annual privacy notice if it:

(1) Provides nonpublic personal information to nonaffiliated third parties only in accordance with the provisions of § 1016.13, § 1016.14, or § 1016.15; and

(2) Has not changed its policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed to the customer under § 1016.6(a)(2) through (5) and (9) in the most recent privacy notice provided.

In considering the potential benefits, costs, and impacts of the proposal, the Bureau takes as the baseline for the analysis the regulatory regime that currently exists.<sup>45</sup> This includes the current provisions of Regulation P. The Bureau assumes that all financial institutions that can use the alternative delivery method provided in § 1016.9(c)(2) are doing so.

#### *B. Potential Benefits and Costs to Consumers and Covered Persons*

The impact on consumers of proposed § 1016.5(e) depends on whether the particular consumer prefers or would otherwise benefit from receiving an annual privacy notice that does not offer the consumer an opt-out under the GLBA and is largely unchanged from previous notices.<sup>46</sup> Under the proposal, financial institutions that meet the requirements for the annual notice exception would not be required to provide consumers with annual privacy notices, and the Bureau anticipates that many institutions would decide not to provide notices in these circumstances. While there is no data available on the number of consumers who are indifferent

---

<sup>45</sup> The Bureau has discretion in each rulemaking to choose the relevant provisions to discuss and to choose the most appropriate baseline for that particular rulemaking.

<sup>46</sup> As discussed in part IV in the section-by-section analysis of proposed § 1016.5(e)(1)(ii), certain changes to an institution's policies or practices would not cause the institution to lose the annual notice exception.

to (or dislike) receiving unchanged privacy notices every year, the limited use of opt-outs and anecdotal evidence suggest that there are such consumers.<sup>47</sup> For this group of consumers, proposed § 1016.5(e) would provide a benefit because it would be available to some institutions that cannot use the alternative delivery method, so that more consumers would stop receiving mailed annual privacy notices.

For other consumers who would prefer or otherwise benefit from receiving the annual notices, there would be some cost because some institutions that previously delivered notices—whether through the standard delivery methods or through the alternative delivery method that includes posting on the institution’s website—would no longer deliver annual notices. Consumers may be less informed about opportunities to limit a financial institution’s information sharing practices if the financial institution meets the requirements for the annual notice exception and chooses not to provide annual notices. For example, some consumers will receive fewer notices in which a financial institution offers *voluntary* opt-outs, *i.e.*, opt-outs that the financial institution is not required by Regulation P to offer (because, for example, the type of sharing the financial institution does is covered by an exception) but that the institution decides to provide anyway via the annual privacy notice. Voluntary opt-outs do not appear to be common, however.<sup>48</sup> Further, institutions could continue to offer voluntary opt-outs and could offer them through other mechanisms even if they do not provide annual privacy notices.

---

<sup>47</sup> One early analysis of the use of the opt-outs reported that at most 5% of consumers make use of them in any year, and likely fewer. See Jeffrey M. Lacker, *The Economics of Financial Privacy: To Opt Out or Opt In?*, 88/3 Fed. Res. Bank Rich. Econ. Q., at 11 (Summer 2002), available at [https://www.richmondfed.org/-/media/richmondfedorg/publications/research/economic\\_quarterly/2002/summer/pdf/lacker.pdf](https://www.richmondfed.org/-/media/richmondfedorg/publications/research/economic_quarterly/2002/summer/pdf/lacker.pdf).

<sup>48</sup> See Lorrie Faith Cranor et al., *Are They Actually Any Different? Comparing Thousands of Financial Institutions’ Privacy Practices*, available at <http://www.econinfosec.org/archive/weis2013/papers/CranorWEIS2013.pdf> (submitted as part of The Twelfth Workshop on the Economics of Information Security (WEIS 2013), June 11–12, 2013, Georgetown University, Washington, DC). Their findings (Table 2) imply that at most 15% of the 3,422 FDIC insured depositories that post the model privacy form on their websites offer at least one voluntary opt-out.

If financial institutions choose not to provide notices pursuant to the annual notice exception, consumers also may be less informed of their opt-out rights under the FCRA. Section 503(c)(4) of the GLBA and Regulation P require financial institutions providing initial and annual privacy notices to incorporate into them any notification and opt-out disclosures provided pursuant to section 603(d)(2)(A)(iii) of the FCRA.<sup>49</sup> Section 624 of the FCRA and Regulation V also permit (but do not require) financial institutions providing initial and annual privacy notices under Regulation P to incorporate any opt-out disclosures provided under section 624 of the FCRA and subpart C of Regulation V into those notices.<sup>50</sup> Because financial institutions may decide not to provide annual notices pursuant to the exception in proposed § 1016.5(e), consumers may be less informed of their opt-out rights pursuant to these sections of the FCRA to the extent that institutions use less effective methods to convey information about these rights to consumers.<sup>51</sup> Consumers also may be less informed about a financial institution's data collection practices and its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Regarding benefits and costs to covered persons, the primary effect of the proposal would be burden reduction by lowering the costs to industry of providing annual privacy notices. Proposed § 1016.5(e) would impose no new compliance requirements on any financial institution. Any institution that could use the alternative delivery method will meet the

---

Data from a much larger group of financial institutions analyzed by Cranor et al. (undated) imply (Table 2) that at most 27% of the 6,191 financial institutions that post the model privacy form on their websites offer at least one voluntary opt-out.

<sup>49</sup> 15 U.S.C. 6803(c)(4); 12 CFR 1016.6(a)(7).

<sup>50</sup> 15 U.S.C. 1681s-3(b); 12 CFR 1022.23(b).

<sup>51</sup> As explained in the section-by-section analysis to proposed § 1016.5(e)(1)(i) in part IV, the annual notice exception in proposed § 1016.5(e) does not relieve financial institutions of the obligation to provide consumers with the information that is required under FCRA sections 603(d)(2)(A)(iii) or 624.

requirements for the annual notice exception pursuant to § 1016.5(e).<sup>52</sup> A financial institution that is in compliance with current law would be required to take any different or additional action only to the extent it chose to take advantage of the annual notice exception and thus was required to separately meet its opt-out obligations, if any, pursuant to the FCRA.<sup>53</sup>

The expected cost savings to financial institutions from the proposed revisions to § 1016.5(e) depend on whether the financial institution uses the alternative delivery method under the baseline. Financial institutions that currently use the alternative delivery method may cease complying with the requirements in current § 1016.9(c)(2) since they necessarily comply with the proposed exception to the annual notice requirement and thus would no longer be required to deliver an annual notice.<sup>54</sup> The Bureau expects that financial institutions changing from using the alternative delivery method to provide annual notices to not providing these notices at all would yield little savings in costs to the institutions.<sup>55</sup> Financial institutions that currently do not use the alternative delivery method would be expected to use the proposed annual notice exception if the expected costs of any changes required to use the exception and the costs of any consequences of not providing the annual disclosure would be lower than the costs of complying with current Regulation P. The Bureau believes that few such financial institutions would find it in their interests to change their information sharing practices in order

---

<sup>52</sup> Any financial institution that meets the conditions to use the alternative delivery method will also meet the conditions to be excepted from delivering an annual privacy notice pursuant to new GLBA section 503(f) because the two conditions for section 503(f) are closely related to conditions for using the alternative delivery method. See the section-by-section analysis of § 1016.9(c) for further explanation.

<sup>53</sup> See the section-by-section analysis to proposed § 1016.5(e)(1)(i) in part IV for an explanation of the interaction between the annual notice exception and the opt-outs provided under FCRA sections 603(d)(2)(A)(iii) and 624.

<sup>54</sup> See *supra* note 52.

<sup>55</sup> The Bureau believes that the alternative delivery method imposes little ongoing cost to financial institutions that have adopted it. These costs derive from the additional text on an account statement, coupon book, notice or disclosure the institution already provides; maintaining a webpage dedicated to the annual privacy notice; responding to telephone calls from a very small number of consumers requesting that the model form be mailed; and mailing the forms prompted by these calls.

to use the annual notice exception. Thus, the Bureau takes the information sharing practices of financial institutions as given and considers how many financial institutions that do not currently meet the requirements to use the alternative delivery method could use the proposed annual notice exception.<sup>56</sup> As a practical matter, the Bureau identifies these institutions solely by their information sharing practices: that is to say, the Bureau identifies the financial institutions whose current information sharing practices do not meet the standards in § 1016.9(c)(2) but would meet the standards in proposed § 1016.5(e).<sup>57</sup> The Bureau then estimates the ongoing savings in costs to these financial institutions from no longer sending the annual privacy notice.

For the 2014 Annual Privacy Notice Rule, the Bureau collected a sample of privacy policies from banks and credit unions and estimated both the number of financial institutions that would adopt the alternative delivery method and the aggregate cost savings that would result.<sup>58</sup> Specifically, the Bureau examined the privacy policies of 19 banks with assets over \$100 billion as well as the privacy policies of 106 additional banks selected through random sampling. The Bureau previously concluded that 80% of banks could use the alternative delivery method set forth in § 1016.9(c)(2). For the current rulemaking, the Bureau re-analyzed this sample to identify banks with information sharing practices that do not meet the standard in § 1016.9(c)(2)

---

<sup>56</sup> Because the Bureau takes institutions' sharing practices as given and because the cost savings estimate is based on a single year, the expected cost savings for institutions does not account for a reduction or increase in aggregate cost savings that may occur if any institutions change their sharing practices in the future such that they no longer meet the requirements for the annual notice exception or they begin to meet those requirements.

<sup>57</sup> It is possible for a financial institution to be unable to use the alternative delivery method despite having information sharing practices that comply with § 1016.9(c)(2), such as where the institution does not use the model privacy notice and therefore does not satisfy § 1016.9(c)(2)(i)(E). This simplification will tend to understate the benefits of the annual notice exception, since the Bureau generally assumes that these financial institutions are using the alternative delivery method. The one exception is the case where a financial institution does not have a website, since in this case it cannot use the alternative delivery method but the Bureau also cannot (as a practical matter) obtain and evaluate its information sharing practices. In this case the Bureau assumes that the financial institution cannot use either the alternative delivery method or the proposed exception.

<sup>58</sup> See 79 FR 64057, 64076-64077 (Oct. 28, 2014). Note that the term "banks" as used throughout this proposal includes savings associations.

but would meet the standard in proposed § 1016.5(e). In the re-analysis, the Bureau finds that 48% of banks that could not use the alternative delivery method could use the proposed exception to the annual notice requirement. Most of these banks were not able to use the alternative delivery method because they offered opt-outs to consumers pursuant to FCRA section 603(d)(2)(A)(iii); a financial institution can meet the requirements for the annual notice exception in proposed § 1016.5(e) even if offers such opt-outs. Specifically, the Bureau previously estimated that approximately 1,350 banks could not use the alternative delivery method and our re-analysis shows that 650 of these banks (48%) would be able to use the annual notice exception.<sup>59</sup> For banks with assets over \$10 billion, 70% of those that could not use the alternative delivery method could use the annual notice exception. For banks with assets of \$10 billion or less and banks with assets of \$500 million or less, the respective figures are 47% and 40%.

The Bureau also previously examined the privacy policies of the four credit unions with assets over \$10 billion as well as the privacy policies of 50 additional credit unions selected through random sampling. The Bureau previously concluded that 46% of credit unions could use the alternative delivery method. The information evaluated in the re-analysis shows that none of the credit unions that could not use the alternative delivery method could use the exception to the annual notice requirement. Credit unions that clearly could not use the alternative delivery method generally shared information with nonaffiliated third parties other than as specified in the exceptions in § 1016.13, §1016.14, and § 1016.15. However, there are a number of cases in which the Bureau could not readily evaluate the information sharing practices

---

<sup>59</sup> While these 650 banks are just 9.5% of all banks, this percentage does not take into account the fact that the majority of banks could not potentially benefit from the exception to the annual privacy notice requirement since (by our previous analysis) they already use the alternative delivery method.

of the sampled credit union because it did not have a website, did not post the privacy notice on its website, or did not use the model form.<sup>60</sup> The Bureau requests data and other factual information on the use of the alternative delivery method by credit unions and the likely use of the proposed annual notice exception by credit unions that cannot use the alternative delivery method.

Regarding the number of non-depository financial institutions that would benefit from the proposed exception to the annual notice requirement, the Bureau uses the same basic methodology as in its prior analysis. Specifically, the Bureau assumes that the fraction of non-depository financial institutions that cannot use the alternative delivery method but can use the proposed annual notice exception is the same for non-depository institutions as for banks (9.5%).<sup>61</sup>

Having identified the financial institutions that would benefit from the proposed exception to the annual notice requirement, the Bureau estimates the benefit using the same basic methodology as in its prior analysis.<sup>62</sup> For banks, the Bureau allocated the total burden of providing the annual privacy notices to asset-size groups in proportion to the share of assets in the group. The Bureau then estimated an amount of burden reduction specific to each asset-size group using the results from the privacy notice analysis described above. The total burden reduction is then the sum of the burden reductions in each asset-size group. The estimated reduction in burden for banks using this methodology is approximately \$3.158 million annually.

---

<sup>60</sup> One or more of these conditions held for a number of credit unions with assets of \$500 million or less. If a financial institution did not have a website or did not post the privacy notice on their website, the Bureau made the conservative assumption that it did not benefit from the alternative delivery method and would not benefit from the proposed annual notice exception. If a financial institution did not use the model form, however, the Bureau assumed that it would adopt the model form if that was the only barrier to using the alternative delivery method. For further discussion, *see* 79 FR 64057, 64076 (Oct. 28, 2014).

<sup>61</sup> For further discussion, *see id.* at 64077.

<sup>62</sup> *See id.* at 64076-64077.

The estimated reduction in burden for non-depository financial institutions is an additional \$231,000 annually.<sup>63</sup> Thus, the Bureau believes that the total reduction in burden is approximately \$3.389 million dollars annually.<sup>64</sup> This represents about 28% of the total \$12.162 million annual cost of providing the annual privacy notice under Regulation P. The Bureau requests comment on this preliminary analysis as well as the submission of additional data that could inform the Bureau's consideration of the cost savings to financial institutions.

The proposed exception to the annual notice requirement implements a December 2015 statutory amendment to the GLBA. The Bureau considered alternatives to the timeline for delivery of annual notices when a financial institution that qualified for the annual exception changes its policies or practices such that it no longer qualifies. Because the estimates of costs and benefits to consumers and covered persons take institutions' sharing policies and practices as given, the alternatives with respect to the timeline for delivery of annual notices do not impact those estimates. Further, even if the estimates allowed for changes in sharing policies and practices that could cause institutions to meet or fail to meet the requirements for the annual notice exception, the aggregate annual benefits and costs of delivery would not likely be significantly impacted by the timeline for delivery of annual notices.

### *C. Impact on Depository Institutions With No More Than \$10 Billion in Assets*

The Bureau currently estimates that approximately 600 banks with \$10 billion or less in assets cannot use the alternative delivery method but could use the annual notice exception. This

---

<sup>63</sup> Note that this figure excludes auto dealers. Auto dealers are regulated by the FTC and would not be directly impacted by this amendment to Regulation P.

<sup>64</sup> Some of these banks and non-depository financial institutions that currently include on their annual privacy notice the opt-out notices pursuant to FCRA section 603(d)(2)(A)(iii) or FCRA section 624 and the Affiliate Marketing Rule may now be required to deliver these notices separately. The Bureau does not have the data necessary to estimate the frequency with which these opt-out notices would be delivered separately or to subtract the cost of delivering them separately against the savings from no longer providing the annual privacy notice.



constitutes 47% of banks with \$10 billion or less in assets that do not use the alternative delivery method and 8.8% of all banks with \$10 billion or less in assets. As reported above, 70% of banks with more than \$10 billion in assets that do not use the alternative delivery method could use the proposed exception to the annual notice requirement. This is 55% of all banks with more than \$10 billion in assets. Thus, the proposed rule may have different impacts on federally insured depository institutions with \$10 billion or less in assets as described in section 1026 of the Dodd-Frank Act. The Bureau currently believes that no credit unions of any size that could not use the alternative delivery method could use the exception to the annual notice requirement.

*D. Impact on Access to Credit and on Consumers in Rural Areas*

The Bureau does not believe that the proposed rule would reduce consumers' access to consumer financial products or services or have a unique impact on rural consumers.

**VI. Regulatory Flexibility Act**

The Regulatory Flexibility Act (RFA) as amended by the Small Business Regulatory Enforcement Fairness Act of 1996, requires each agency to consider the potential impact of its regulations on small entities, including small businesses, small governmental units, and small not-for-profit organizations. The RFA defines a "small business" as a business that meets the size standard developed by the Small Business Administration pursuant to the Small Business Act. The RFA generally requires an agency to conduct an initial regulatory flexibility analysis (IRFA) and a final regulatory flexibility analysis (FRFA) of any rule subject to notice-and-comment rulemaking requirements, unless the agency certifies that the rule will not have a significant economic impact on a substantial number of small entities.<sup>65</sup> The Bureau also is subject to certain additional procedures under the RFA involving the convening of a panel to

---

<sup>65</sup> 5 U.S.C. 603 through 605.

consult with small business representatives prior to proposing a rule for which an IRFA is required.<sup>66</sup>

An IRFA is not required here because the proposal, if adopted, would not have a significant economic impact on a substantial number of small entities. The Bureau does not expect the proposal to impose costs on small entities. All methods of compliance under current law will remain available to small entities if the proposal is adopted. Thus, a small entity that is in compliance with current law need not take any different or additional action if the proposal is adopted. In addition, based on the data analysis described previously, the Bureau believes that the proposed annual notice exception would allow some small institutions to stop sending the annual notice and to thereby reduce costs. However, there are a number of cases in which the Bureau could not readily evaluate the information sharing practices of small banks and especially small credit unions because the institution did not have a website, did not post the privacy notice on its website, or did not use the model form. The Bureau seeks comment on this analysis.

Accordingly, the undersigned certifies that this proposal, if adopted, would not have a significant economic impact on a substantial number of small entities.

## **VII. Paperwork Reduction Act**

Under the Paperwork Reduction Act of 1995 (PRA),<sup>67</sup> Federal agencies are generally required to seek Office of Management and Budget (OMB) approval for information collection requirements prior to implementation. This proposal would amend Regulation P, 12 CFR part 1016. The collections of information related to Regulation P have been previously reviewed and approved by OMB in accordance with the PRA and assigned OMB Control Number 3170-0010.

---

<sup>66</sup> 5 U.S.C. 609.

<sup>67</sup> 44 U.S.C. 3501 through 3558.

Under the PRA, the Bureau may not conduct or sponsor, and, notwithstanding any other provision of law, a person is not required to respond to an information collection, unless the information collection displays a valid control number assigned by OMB.

As explained below, the Bureau has determined that this proposed rule does not contain any new or substantively revised information collection requirements other than those previously approved by OMB. The proposal would implement the December 2015 amendment to the GLBA and amend § 1016.5 of Regulation P to provide that a financial institution is not required to deliver an annual privacy notice if it:

(1) Provides nonpublic personal information to nonaffiliated third parties only in accordance with the provisions of § 1016.13, § 1016.14, or § 1016.15 and;

(2) Has not changed its policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed to the customer under § 1016.6(a)(2) through (5) and (9) in the most recent privacy notice provided.

Under Regulation P, the Bureau generally accounts for the paperwork burden for the following respondents pursuant to its enforcement/supervisory authority: federally insured depository institutions with more than \$10 billion in total assets, their depository institution affiliates, and certain non-depository institutions. The Bureau and the FTC generally both have enforcement authority over non-depository institutions subject to Regulation P. Accordingly, the Bureau has allocated to itself half of the final rule's estimated reduction in burden on non-depository financial institutions subject to Regulation P. Other Federal agencies, including the FTC, are responsible for estimating and reporting to OMB the paperwork burden for the institutions for which they have enforcement and/or supervision authority. They may use the Bureau's burden estimation methodology, but need not do so.

The Bureau does not believe that this proposed rule would impose any new or substantively revised collections of information as defined by the PRA, and instead believes that it would have the overall effect of reducing the previously approved estimated burden on industry for the information collections associated with the Regulation P annual privacy notice. Using the Bureau's burden estimation methodology, the reduction in the estimated ongoing burden would be approximately 62,197 hours annually for the roughly 13,500 banks and credit unions subject to the proposed rule, including Bureau respondents, and the roughly 29,400 entities regulated by the FTC also subject to the proposed rule (*i.e.*, entities over which the FTC has Regulation P administrative enforcement authority). The reduction in estimated ongoing costs from the reduction in ongoing burden would be approximately \$3.389 million annually.<sup>68</sup>

The Bureau believes that the one-time cost of adopting the annual notice exception for financial institutions that would adopt it is *de minimis*. The Bureau's methodology for estimating the reduction in ongoing burden was discussed above. The method is similar to that described in the PRA analysis in the 2014 Annual Privacy Notice Rule. The only difference is that instead of estimating the fraction of institutions that would be able to use the alternative delivery method, the Bureau estimates the fraction of institutions that would be able to use the annual notice exception and are not already using the alternative delivery method, to compute the reduction in burden relative to the baseline.<sup>69</sup>

The Bureau takes all of the reduction in ongoing burden from banks and credit unions with assets \$10 billion and above and half the reduction in ongoing burden from the non-depository institutions subject to the FTC enforcement authority that are subject to the Bureau's

---

<sup>68</sup> The total hours and costs consist of: (a) 51,230 hours at banks and credit unions evaluated at \$61.65/hour; and (b) 10,967 hours at entities regulated by the FTC also subject to the proposed rule evaluated at \$21.07/hour.

<sup>69</sup> See 79 FR 64057, 64080 (Oct. 28, 2014).

Regulation P. The total reduction in ongoing burden taken by the Bureau is 53,216 hours or \$3.058 million annually.<sup>70</sup>

The Bureau has determined that the proposed rule does not contain any new or substantively revised information collection requirements as defined by the PRA and that the burden estimate for the previously approved information collections should be revised as explained above. The Bureau welcomes comments on these determinations or any other aspect of the proposal for purposes of the PRA. Comments should be submitted as outlined in the **ADDRESSES** section above. All comments will become a matter of public record.

SUMMARY OF BURDEN CHANGES			
Information collections	Previously approved total burden hours	Net change in burden hours	New total burden hours
Notices and disclosures .....	366,134	-53,216	312,917

**List of Subjects in 12 CFR Part 1016**

Banks, banking, Consumer protection, Credit, Credit unions, Foreign banking, Holding companies, National banks, Privacy, Reporting and recordkeeping requirements, Savings associations, Trade practices.

**Authority and Issuance**

For the reasons set forth in the preamble, the Bureau proposes to amend Regulation P, 12 CFR part 1016, as set forth below:

**PART 1016—PRIVACY OF CONSUMER FINANCIAL INFORMATION**

---

<sup>70</sup> The total hours and costs consist of: (a) 47,733 hours at banks and credit unions evaluated at \$61.65/hour; and (b) 5,484 hours at entities regulated by the FTC also subject to the proposed rule evaluated at \$21.07/hour.

**(REGULATION P)**

1. The authority citation for part 1016 continues to read as follows:

**Authority:** 12 U.S.C. 5512, 5581; 15 U.S.C. 6804.

2. Section 1016.3 is amended by revising paragraph (s)(1) to read as follows:

**§ 1016.3 Definitions.**

\* \* \* \* \*

(s)(1) *You* means a financial institution for which the Bureau has rulemaking authority under section 504(a)(1)(A) of the GLB Act (15 U.S.C. 6804(a)(1)(A)).

\* \* \* \* \*

**Subpart A—Privacy and Opt Out Notices**

3. Section 1016.5 is amended by revising the first sentence of paragraph (a)(1) and adding subsection (e) to read as follows:

**§ 1016.5 Annual privacy notice to customers required.**

(a)(1) *General rule.* Except as provided by paragraph (e) of this section, you must provide a clear and conspicuous notice to customers that accurately reflects your privacy policies and practices not less than annually during the continuation of the customer relationship. \* \* \*

\* \* \* \* \*

(e) *Exception to annual privacy notice requirement.* (1) *When exception available.* You are not required to deliver an annual privacy notice if you:

(i) Provide nonpublic personal information to nonaffiliated third parties only in accordance with the provisions of § 1016.13, § 1016.14, or § 1016.15 of this part; and

(ii) Have not changed your policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed to the customer under

§ 1016.6(a)(2) through (5) and (9) in the most recent privacy notice provided pursuant to this part.

*(2) Delivery of annual privacy notice after financial institution no longer meets requirements for exception.* If you have been excepted from delivering an annual privacy notice pursuant to paragraph (e)(1) of this section and change your policies or practices in such a way that you no longer meet the requirements for that exception, you must comply with paragraph (e)(2)(i) or (e)(2)(ii) of this section, as applicable.

*(i) Changes preceded by a revised privacy notice.* If you no longer meet the requirements of paragraph (e)(1) of this section because you change your policies or practices in such a way that § 1016.8 requires you to provide a revised privacy notice, you must provide an annual privacy notice in accordance with the timing requirements in paragraph (a) of this section, treating the revised privacy notice as an initial privacy notice.

*(ii) Changes not preceded by a revised privacy notice.* If you no longer meet the requirements of paragraph (e)(1) of this section because you change your policies or practices in such a way that § 1016.8 does not require you to provide a revised privacy notice, you must provide an annual privacy notice within 60 days of the change in your policies or practices that causes you to no longer meet the requirements of paragraph (e)(1).

*(iii) Example.* You change your policies and practices in such a way that you no longer meet the requirements of paragraph (e)(1) of this section effective April 1 of year 1. Assuming you define the 12-consecutive-month period pursuant to paragraph (a) of this section as a calendar year, if you were required to provide a revised privacy notice under § 1016.8 and you provided that notice on March 1 of year 1, you must provide an annual privacy notice by

December 31 of year 2. If you were not required to provide a revised privacy notice under § 1016.8, you must provide an annual privacy notice by May 30 of year 1.

4. Section 1016.9 is amended by revising paragraph (c) to read as follows:

**§ 1016.9 Delivering privacy and opt out notices.**

\* \* \* \* \*

(c) *Annual notices only.* You may reasonably expect that a customer will receive actual notice of your annual privacy notice if:

(1) The customer uses your Web site to access financial products and services electronically and agrees to receive notices at the Web site, and you post your current privacy notice continuously in a clear and conspicuous manner on the Web site; or

(2) The customer has requested that you refrain from sending any information regarding the customer relationship, and your current privacy notice remains available to the customer upon request.

\* \* \* \* \*



**[THIS SIGNATURE PAGE PERTAINS TO THE PROPOSED RULE TITLED  
“AMENDMENT TO THE ANNUAL PRIVACY NOTICE REQUIREMENT UNDER  
THE GRAMM-LEACH-BLILEY ACT (REGULATION P)”]**

**Dated:** June 29, 2016.



---

**Richard Cordray,**

*Director, Bureau of Consumer Financial Protection.*