Public Interest Comment on

The Proposed Rules to Protect the Privacy of Consumer Financial Information[1]

The Regulatory Studies Program (RSP) of the Mercatus Center at George Mason University is dedicated to advancing knowledge of regulations and their impacts on society. As part of its mission, RSP produces careful and independent analyses of agency rulemaking proposals from the perspective of the public interest. Thus, the program's comments on proposed rules to protect the *Privacy of Consumer Financial information* do not represent the views of any particular affected party or special interest group, but are designed to protect the interests of American citizens.

I. Introduction

On February 22, 2000, the Office of the Comptroller of the Currency (OCC), in conjunction with the Federal Reserve Board (FRB), Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS) proposed regulations to:

> …implement notice requirements and restrictions on a financial institution's ability to disclose nonpublic personal information about consumers to nonaffiliated third parties.[2]

The authority for this proposed rulemaking comes from Title V of the Gramm-Leach-Bliley ("GLB") Act.[3] Under the Act, Congress expressed its policy "that each financial institution has an affirmative and continuing obligation to protect the security and confidentiality of [its] customers' nonpublic personal information."[4] The law contains four major requirements:

1. All covered institutions must establish appropriate administrative, technical, and physical safeguards to protect customer records and information.

---

[1] Prepared by Jay Cochran, III, Research Fellow, Regulatory Studies Program, the Mercatus Center at George Mason University, jcochra1@gmu.edu.

[2] "Privacy of Consumer Financial Information; Proposed Rule," 12 CFR Part 573, as found in the *Federal Register*, Vol. 65, No. 35, Thursday, February 22, 2000, pp. 8770-8816. Hereinafter referred to as the "proposed rule." This comment focuses mainly on banking and related industries; however, in general, our comments also apply to rules that are concurrently being proposed by the Federal Trade Commission (for money-transfer, retailing, automotive and other non-bank credit operations), the National Credit Union Administration, and the Securities and Exchange Commission (for securities firms). State insurance commissioners will implement rules for insurers with respect to consumer financial privacy.

[3] Public Law 106-102, introduced as S.900 and formally titled, "An Act to enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, and other financial services providers, and for other purposes." The law is also known as the "Financial Services Modernization Bill."

[4] *Ibid.,* § 501 (a).

2. Institutions must clearly and conspicuously disclose their privacy policies and practices to consumers in writing or electronic form.

3. Consumers must be given the opportunity to "opt out" of any disclosures to nonaffiliated third parties before such disclosures take place; and

4. Any nonaffiliated third party receiving nonpublic personal information may not subsequently reuse or re-disclose such information unless such disclosure would be lawful if performed by the original financial institution.[5]

The law allows a number of exceptions to the general requirements. Key exceptions include disclosures necessary to carry out transactions on a customer's behalf, disclosures for law enforcement purposes, disclosures in connection with business combinations or mergers, and disclosures for auditing and insurance rating purposes.

The agencies' proposed regulations closely follow the requirements of the law. In particular, institutions covered by the rule may not disclose nonpublic information about a consumer to nonaffiliated third parties unless the institution satisfies disclosure and opt-out requirements, and the consumer has not opted out of disclosure.

II. Defining "Nonpublic Personal Information"

The proposed rule contains a lengthy discussion of the possible meanings of the phrase, "nonpublic personal information." The discussion appears convoluted, and yet the precise interpretation will have important consequences for the scope of the final rule.

In the actual law, § 509.4 defines nonpublic personal information as "personally identifiable information." That is, information must be nonpublic, AND it must be uniquely assignable to a particular individual in order to be protected under the rule.

The requirement that the protected information is nonpublic and personally identifiable can be illustrated by example. Personal information that is not identifiable might include aggregations of deposit account volumes. The basis for the aggregate data is individual account balances; however, the aggregation process eliminates linkages to particular individuals.[6] By contrast, information can be identifiable to certain individuals but the information is not in any meaningful sense nonpublic. One's home address for instance, is certainly individually identifiable, but it is not private insofar as the information is available

[5] See Public Law 106-102, Title V, § 501 and 502.

[6] The aggregation example therefore addresses the agencies' request for comment on whether either of their definitions would prohibit use of "information about a consumer that contains no indicators about a consumer's identity." (Proposed rule, p. 8774.) If data are not identifiable to a particular person, then that information would fall outside the boundaries of the proposed rule.

from public sources such as county land records, and telephone books.[7] Thus, both modifiers, nonpublic and personal, are required in order for information to be covered under the rule.

While the language of the law seems straightforward, the proposed rule is not. The agencies have distinguished alternative interpretations of "nonpublic personal information," designated as Options "A" and "B".

> **Option A:** The fact that the information is available from those sources [i.e., publicly available sources such as telephone directories] is immaterial if the financial institution does not actually obtain the information from one of them.[8]
>
> **Option B:** Information need only be available from a public source for it to be considered "publicly available."[9]

Needlessly complicating the interpretation of nonpublic personal information runs counter to Congressional intent that the proposed rule "use 'plain language' in all proposed and final rules published after January 1, 2000."[10] Option A not only violates the plain language intent of Congress, but goes beyond the requirements of the law's § 509.4. If Option A were to hold, it would mean that unless financial institutions actually constructed their customer name and address databases from, say, telephone books, then those data, which is otherwise public, would be covered under the rule—i.e., subject to opt out and disclosure requirements.

Except for the above complications, the proposed rule elsewhere tends to follow the plain language requirement set forth by Congress. In particular, the proposed rule uses examples throughout to illustrate where fine lines exist between permissible and impermissible behavior. This should prove helpful in establishing expectations among consumers and financial institutions regarding financial privacy rights and obligations under the law.

III. The Proposed Rule

A. Take Steps to Protect Information

There is an important though often overlooked distinction between privacy and security. The first requirement of GLB—that all covered institutions establish appropriate administrative, technical, and physical safeguards to protect customer records and information—is a

---

[7] A case closer to the borderline might involve *ownership* of particular financial accounts—as distinct from the content of the account. Is the mere fact that an individual holds, say, a particular credit card considered personal information, so long as balances, payment histories, etc. are not disclosed? The existence of the account is certainly identifiable or assignable to a particular individual, but is the fact of its *existence* nonpublic? In general, the answer would appear to be no, since one must publicly produce evidence of such account ownership during a transaction by producing a credit card or checkbook, for example.

[8] Proposed rule, p. 8773.

[9] *Loc. cit*.

[10] § 722, GLB. See also the proposed rule, p. 8788.

requirement for security. All the privacy policies and practices in the world will be ineffective if private personal information were freely available in unsecured databases. Thus, security is a necessary precondition of privacy, but it is not the same thing as privacy itself.

Indeed, the security requirements of covered institutions may go beyond those necessary to protect just consumers' privacy. Financial institutions have a proprietary interest in protecting certain kinds of information—just as they have an interest in protecting their physical assets. In other words, business interests and consumer interests concerning security are aligned rather than conflicting, and most financial institutions already have the security systems, required by this section of the law, in place.

B. Notice Requirements

The GLB Act requires covered financial institutions to

> …provide an initial notice of privacy policies and practices in two circumstances. For customers, the notice must be provided at the time of establishing a customer relationship. For consumers who do not become customers, the notice must be provided prior to disclosing nonpublic personal information about the consumer to a nonaffiliated third party.[11]

Notices may be given in writing or in electronic form if the customer agrees to electronic notification. Importantly however, oral notification is not permitted, nor, for example, are placards in a bank lobby detailing the institution's privacy policy.

In addition, the law requires that covered institutions annually notify current customers of the institution's privacy policies and practices and update them more frequently if such policies change.[12] Notification requirements terminate after twelve months have elapsed without contact between an institution and a former customer.[13]

---

[11] *Ibid*., p. 8775. This distinction between "consumers" and "customers" has to do with the disclosures. "[A] financial institution must give all 'customers' … notice of the institution's privacy policy." Proposed rule, p. 8772. A consumer only receives notification if the institution intends to disclose nonpublic personal information about them. An example of a consumer who is not a customer involves an individual who applies for a loan that is subsequently scored, but who then decides not to contract for the loan. A customer relationship by contrast, is "one that generally is of a continuing nature." (*Loc. cit.*)

[12] If an institution does not disclose information to non-affiliated third parties, no notice is required.

[13] *Ibid*., p. 8776.

C. Opt Out Choice

Consumers, under the law, have a right to opt out of disclosure at any time.[14] Moreover, following notification of the institution's policies and practices, institutions must allow consumers a reasonable time to exercise their opt out rights before making a disclosure. Because of the wide variance among institutional practices however, the proposed rule does not specify how quickly an institution must "effectuate a consumer's opt out election."[15]

The agencies have sought specific comment on whether joint account holders must both agree to opt out for an institution to honor an opt out request, or whether an opt out request by one of the joint parties (a) covers the entire account, (b) covers only the opting out party's information, or (c) does not apply at all?

We suggest that for clarity, as well as symmetry, an opt out request on a joint account be treated similarly to institution's rules governing withdrawal requests from a given joint account. For example, if consent of both parties is required to withdraw money from a joint account, then until such time as both parties agree to opt out, the institution may treat an opt out request of one party as if no request had been made. Conversely, if either party to a joint account may make withdrawals on just one signature, then either party may effect an opt out request and have it treated as binding on the entire account.

D. No Reuse of Information by Third Parties

Third parties who receive nonpublic personal information may not subsequently re-disclose that information to others. As the proposed rule states, the Act places the receiving institution "into the shoes of the institution that disclosed the information for purposes of determining whether re-disclosures by the receiving institution are lawful."[16] That is, if disclosure were illegal for the originating institution without consumer consent, then subsequent disclosure by the receiving third party would be similarly illegal.

In addition, under §__.4 of the proposed rule, financial institutions must "enter into a contract with the third party that requires the third party to maintain the confidentiality of the information…at least to the same extent as is required for the financial institution that

---

[14] Elections to opt out would not preclude financial institutions from complying with lawful requests for information pursuant to court orders, law enforcement, etc. In addition, institutions may

> …disclose nonpublic personal information about a consumer to a nonaffiliated third party for the purpose of the third party performing services for the institution, including marketing financial products and services under a joint agreement between the financial institution and at least one other financial institution. In this case, a consumer has no right to opt out, but the financial institution must inform the consumer… [Proposed rule, p. 8777.]

[15] *Ibid.,* p. 8779.

[16] *Ibid*., p. 8780.

discloses it[.]"[17] From this information, it seems the proposed rule makes the conditions for protection and re-disclosure understandable without being unduly prescriptive.

IV. Costs & Benefits of the Rule

A. Agencies' Regulatory Impact Analysis

As part of the rule proposal process, the Department of the Treasury and the agencies with whom it is working to implement financial privacy standards have conducted a regulatory impact analysis. The analysis consists mainly of estimates of compliance burdens in the form of information collection requirements. While this approach may be helpful in establishing a first approximation of the regulatory burden, it is subject to a number of drawbacks, not the least of which is the fact that it relies heavily on an average figure for a highly skewed distribution—i.e., the distribution of deposit accounts among institutions. In their analysis, the agencies assume an annual compliance burden per institution of 45 hours.

In addition, the agencies did not attempt to monetize their estimates of time burden. Therefore, in Appendix II, Mercatus assigns a dollar figure to the agencies' hourly estimates by using a composite wage rate based on average hourly payroll costs at the regulated institutions. Table 1 summarizes the results of that analysis. We also take the additional step of determining the discounted present value of these cost estimates, assuming they recur into the indefinite future. We use the OMB standard of seven percent to derive this result.

TABLE 1
SUMMARY OF COMPLIANCE COST ESTIMATES FOR FINANCIAL PRIVACY REGULATIONS
(All Dollar Figures in Millions)

Regulator	Annual Costs	Discounted Present Value of All Costs
OCC	$ 1.9	$ 27.2
Federal Reserve	7.7	110.4
FDIC	4.4	62.9
OTS	0.8	12.1
TOTAL	**$14.9**	**$212.7**

Based on these simplified cost estimates and the discounting methodology, we suggest that the proposed rule to protect customers' and consumers' financial privacy will cost at least $14.6 million per year, or a total of $212.7 million over the indefinite future.[18]

[17] *Ibid*., p. 8779.

To put these estimates into some perspective, the agencies' compliance estimates are equivalent to devoting more than 420 full time industry employees (at currently prevailing average wage rates) to the exclusive task of securing and protecting individual financial privacy every year. Alternatively, from the consumer's perspective, securing financial privacy will cost the average American household a little more than two dollars over the next several years.[19]

B. Mercatus' Regulatory Cost Estimate

Mercatus believes that the costs of complying with the privacy rule will vary directly with the number of accounts that a financial institution has at any given time. That is, the cost of annual notification, recordation of opt out requests, as well as the issuance of new notices as policies change, will be a function of the number of accounts at an institution rather than a generalized hourly burden. We expect that the largest burden will fall on deposit accounts; however, loan accounts are subject to the rule and therefore will incur compliance costs too.

Our estimating methodology appears in Appendix II. For purposes here however, we estimate that **the cost of the rule may likely exceed $223 million annually**, based on conservative assumptions regarding the unit costs of compliance incurred by individual financial institutions. Moreover, using the standard OMB discount factor of seven percent yields a long-run cost estimate for the rule of $3.2 billion.

Again, putting these estimates into some perspective, these annual costs are equivalent to devoting more than 6,300 full time industry employees (at currently prevailing average industry wages) to the exclusive task of securing depositors' and borrowers' privacy.[20] Alternatively, from a consumer perspective, financial privacy can be expected to cost the average American household roughly $32.00 over the long-run.

C. Benefits of the Proposed Rule

The benefits of increased financial privacy protection tend to be of an intangible (i.e., non-pecuniary) nature. This does not mean they are unimportant, only that they tend to be difficult to measure. We have not attempted to estimate the rule's benefits here. We merely provide an estimate of the costs so that policy makers and consumers can make a more fully

---

[18] The number of institutions regulated by each agency indicates some degree of overlap and therefore a potential for double counting. However, since some institutions may be subject to regulatory overlap and the costs involved in this estimating procedure are relatively small, this potential bias is ignored. Because the compliance estimates follow the linear methodology described in the proposed rule, we did not perform a sensitivity analysis of our estimates to changing parameters. A 10% change in estimated hours, or hourly rates will, for example, produce a 10% change in estimated costs.

[19] The number of households, 101.02 million as of 1997, appears in the *Statistical Abstract of the United States* (1997), Table 69.

[20] In terms of total industry employment, 6,300 represents a little more than three-tenths of one percent of 1997 employment in US Depository Institutions (SIC 6000).

informed decision regarding the costs of securing their financial privacy.[21] We leave it to individuals concerned to decide whether the benefits as they perceive them outweigh the costs.

V. Possible Unintended Consequences of the Rule

An implicit presumption of the law and the proposed rule is that customers and financial firms cannot come to mutually acceptable terms with respect to privacy. This may or may not be true,[22] but in any event codification of explicit privacy requirements will likely have unintended consequences, inasmuch as regulators and lawmakers cannot anticipate every possible situation under which the rules may be applied. Below, we discuss some of the unintended outcomes that may result from application of the proposed rule.

Under the rule, credit bureaus cannot disclose name and address files ("header files") to non-affiliated third parties. Because of their unique position, credit bureaus tend to have the most current data on names and addresses of Americans, since financial institutions, on a daily basis, update the bureaus with the changing information of their customers. If bureaus are no longer allowed to share even header information with non-financial institutions, this may mean, for example, that the IRS and other agencies may have to use less-reliable information in their enforcement activities. Thus, tracking down deadbeat parents, fighting tax fraud, and even ensuring that tax refunds get to the proper persons may be less efficient under the rule.

The general trend toward less-efficient processing can also apply to other non-financial transactions. Suppose for example that a diner suffers food poisoning at a restaurant. An efficient means of contacting other diners who may have also been exposed could involve obtaining addresses and telephone numbers from credit card information stored at the credit bureaus. Under the proposed rule, this efficient means of saving lives and preventing injuries may be curtailed.[23]

Another possible outcome of the proposed rule involves direct mail. If credit bureaus and other institutions can no longer resell header information, then the ability of direct mailers to target potential customers will be curtailed. While curtailment of direct mail for the vast majority of recipients who do not respond may be desirable for them, those who currently do

---

[21] Of course, the estimates are subject to the validity of the estimating methodology, which can reasonably be questioned inasmuch as it implicitly relies on a labor theory of value approach. That is, it does not consider capital and other non-labor costs, nor does it examine the effects of regulations on the supply of and demand for credit (i.e., on the products of the financial institutions). However, the methodology parallels the one employed by the agencies (and is consistent with the requirements of the Paperwork Reduction Act), and it does retain some connection with costs insofar as most of the opportunity costs with respect to financial privacy will in fact involve labor and the foregone services that could have been provided elsewhere.

[22] Indeed, as we have endeavored to point out elsewhere, businesses already have ample incentives to protect consumer privacy.

[23] It is also possible that under an emergency exception, the information could be disclosed. The important point however, is that the rule is unclear in such a (deliberately) nuanced situation.

respond to direct mail may see this avenue of product information closed. In other words, direct mail allows the marketing of products to be more finely tailored to the needs and desires of potential customers and the rule may curtail this ability.

If the ability of direct marketers to target their audiences accurately is curtailed under the rule, alternative means of reaching potential audiences will have to be found, and in the meantime, this reduced efficiency may lead to higher costs for customer communication. Indeed, the proposed rule in its more restrictive interpretation could have a significantly negative impact on the direct mail industry if credit bureaus and other institutions are prohibited from reselling header information.[24]

VI. Information Ownership

Most information, financial or otherwise, is jointly produced, but ownership of the resulting product is not always clear-cut. Indeed, a cloudy ownership title in information is a common thread running throughout the current privacy debates. Individual Americans seem to think they own the information about which they are the subjects, while those who collect, process, and store such information believe they own the information because they have incurred the cost of collecting and maintaining it. Moreover, the rights of use and disposal (sometimes referred to as "derivative rights") often are linked to ownership, and it is here where one gets to the core questions of privacy debates.

Who owns and who controls nonpublic personal information? The answer to this question will profoundly affect the information economy. The increasing ease with which information can be used to the detriment of its subject has of course brought the privacy issue to the fore. However, the obverse of pervasiveness is that information also enables businesses to customize product offerings and inventories to better reflect local demand, thereby conferring substantial benefits on consumers in the form of lower costs and increased variety. Drawing the line therefore between rights of information subjects and the responsibilities of information owners will be difficult, but nevertheless essential if we are to avoid impeding progress of the new information economy.

The prevailing trend in information ownership (as well as the derivative rights of use and disposal) *appears* to be that the information's possessors (i.e., those who collect and store it) hold title to the information as well as to the derivative rights of use and disposal.[25]

---

[24] Estimates prepared by Wharton Economic Forecasting Associates for the Direct Marketing Association indicate that the direct mail industry enjoyed revenues of nearly $42 billion and employed roughly 3.9 million people in 1999. In addition, if credit bureau header data were no longer available, effects may ripple through such diverse institutions and industries as public utilities (who use the data to verify identities when establishing service), universities (searching for lost alumni), and state unclaimed funds departments.

[25] Jonathan P. Tomes, J.D., points out with respect to confidentiality of health care records that, "Patients often think they own their records and thus have an ownership right to them. However, many states have statutes or administrative regulations that specify that the actual physical record is the property of the [health care] provider." [As quoted from *Healthcare Privacy & Confidentiality: The Complete Legal Guide,* (Chicago: Probus Publishing, 1994), p. 199.] We suspect that a similar state of affairs exists with respect to personal

However, such rights are qualified. Ownership rights in information may be attenuated by the subject's right of refusal—i.e., by the subject's ability to reject disclosure and to have that right respected—and by the legitimate needs of law enforcement as well as the need to have the information serve its subjects efficiently. (GLB allows banks to disclose nonpublic personal information to nonaffiliated third parties for the purposes of carrying out a transaction authorized by the customer without obtaining prior consent.)

Indeed, the entire purpose for the present regulation is to describe a line of protection for the information's subjects over which the information's possessors may not cross. A constructive role for government in this instance therefore may be to remove the cloud surrounding ownership by delineating ownership rights and responsibilities, and then allowing individuals and firms to seek their own equilibria—turning to the state for adjudication when an impasse occurs.

VII. Conclusion

Toward achieving the goal of minimal interference in the information and privacy rights of individuals, the financial regulatory agencies have shown commendable restraint. In our view, the rule in its less-restrictive form strikes a reasonable balance between efficient business operations of financial institutions (with the attendant benefits to consumers), and a growing desire for individual privacy on the part of consumers. Moreover, if our estimates are correct, the rule achieves its ends without imposing high costs on American consumers of financial products.

Unfortunately, the basic premise of the proposed rule remains animated by an implicit belief that individuals and firms cannot come to a mutually satisfactory agreement as far as privacy is concerned without government assistance. Indeed if individuals truly value their privacy, and firms desire to maximally satisfy their customers, then a meeting of the minds ought to be achievable without resort to compulsory regulations.

Our conclusion therefore is that agencies have done a reasonably good job of proposing regulations that fall within the scope of the law and that do not impose overly burdensome requirements. We estimate that the proposed rule may impose annual compliance costs of more than $220 million and long-run compliance costs of more than $3.2 billion for US depository institutions subject to OCC, FRB, FDIC, or OTS oversight.

One remaining concern, however, regards the definition of "nonpublic personal information." We strongly recommend that the rule more closely comport with the clearly expressed intent of Congress that financial information must be of both a nonpublic and personally identifiable nature to be covered by the rule. Otherwise, the rule may end up reducing the significant benefits that can potentially accrue to businesses and consumers in the modern information economy.

---

financial records. However, the crucial point is, as Tomes points out, that the treatment of the ownership question is uneven across states and thus remains uncertain.

Appendix I
RSP Checklist
GLB Financial Privacy Regulations

Element	Agency Approach	RSP Comment
1. Has the agency identified a significant market failure?	The agencies followed the law, but the law tends to imply that financial institutions lack appropriate incentives to safeguard customer privacy. **Satisfactory**	Property rights in financial information remain ambiguously defined. Congress and the agencies would do better to examine the root cause of this problem, and to address the definition of property rights directly.
2. Has the agency identified an appropriate federal role?	Financial institutions (except insurance companies) generally fall under federal purview. **Fair**	The law required action; however, Congress and the agencies have failed to demonstrate a pervasive problem that currently requires federal attention.
3. Has the agency examined alternative approaches?	The agencies have considered alternatives within the rubric of a federally imposed rule. **Good**	The agencies generally chose the least intrusive least prescriptive rules within the scope of the law when implementing the regulations. Also, the use of examples should illuminate potential gray areas in the rule.
4. Does the agency attempt to maximize net benefits?	The agencies conduct a rudimentary impact analysis. **Fair**	Benefits are not examined and costs remain unquantified in dollar terms. Our simple estimates however, indicate relatively small costs.

5. Does the proposal have a strong scientific or technical basis?	Falsifiable evidence supporting the need for the law and subsequent regulations were entirely lacking. **Unsatisfactory**	No scientific (refutable) evidence is offered in either the law or the proposed rule to support the contention that consumers are seeing their privacy *systematically* violated by financial institutions.
6. Are distributional effects clearly understood?	Distributional effects were not considered in the law or the rule. **Unsatisfactory**	Effects on non-financial industry firms were not considered. Cost/benefit analyses do not consider effects on supply of and demand for credit products resulting from this rule. Nor was any consideration given to the differential impacts on small depository institutions.
7. Are individual choices and property impacts clearly understood?	The proposal does not focus on the key issue of property rights in information, nor does it recognize the effect different regulatory approaches (including no regulation) would have on individual choices. **Unsatisfactory**	The question of who owns and controls nonpublic personal information has gone largely unresolved. This oversight will inevitably invite more regulation rather than less.

Appendix II
Estimated Costs of the Financial Privacy Rule

Method 1—*Agency Estimates Based on Compliance Hours*

Under Method 1, we simply rely on the estimates provided in the Proposed Rule for number of hours expected to be spent by institutions in compliance with the rule, even though such an approach ignores significant costs. The agencies estimate that, on average, the burden per regulated institution will be 45 hours per year.[26]

The **Office of the Comptroller of the Currency** estimates that approximately 2,400 banks fall under its purview.[27] Primarily, these institutions include national banks, banks in the District of Columbia, and agencies of foreign banks. Based on data available from the Small Business Administration (SBA),[28] as of 1996, there were 2,422 national commercial banks (SIC 6021) employing roughly 847,000 people with a total payroll of $27 billion. These data yield an average hourly wage estimate of $17.64 (allowing for 2.5% average annual inflation since 1996). Therefore, using these figures and the compliance estimates in the rule, Mercatus calculates the cost of complying with the proposed rule for banks subject to OCC oversight at $1.9 million per year.

The **Federal Reserve Board** estimates that approximately 9,500 banks fall under its purview.[29] These institutions primarily include bank holding companies, state member banks, branches of foreign banks, and lending companies owned by foreign banks. Again, using SBA data, we estimate the average hourly wage at institutions subject to the Board's oversight at $18.08. Therefore, an estimate of the total annual opportunity cost of compliance for institutions subject to FRB oversight is roughly $7.7 million.

Insured non-member banks are included among the institutions subject to the jurisdiction of the **Federal Deposit Insurance Corporation**. FDIC estimates the number of such institutions at 5,764.[30] Mercatus estimates the average hourly labor cost for these banks at $16.99 and total cost therefore of $4.4 million per year.

---

[26] *Ibid.*, p. 8782. In the proposed rule, dollar cost estimates of the compliance burdens were not made. Mercatus attempts here to assign dollar figures to the compliance burdens estimated in the proposed rule.

[27] *Loc. cit.* The number of institutions regulated by each agency indicates some degree of overlap and therefore a potential for double counting. However, since some institutions may be subject to regulatory overlap and the costs involved in this estimating procedure are relatively small, this potential bias is ignored.

[28] Available from www.sba.gov. Latest data available are as of 1996. Our dollar figures are therefore increased at a compound rate of 2.5% per year to allow for inflation.

[29] Proposed rule, p. 8782. It was not possible to reconstruct from SIC data the precise number of institutions subject to Federal Reserve Board oversight due to overlapping jurisdictions of the regulatory agencies. We therefore used the data in SIC codes 6020 (Commercial Banks)—which includes State and National Commercial Banks—and 6080 (Foreign Banks and Branches).

[30] Proposed rule, p. 8783. As with the Federal Reserve estimates, SIC-level data were not aggregated according to regulatory oversight agencies. Thus, we used SIC 6022 (State Commercial Banks) to proxy FDIC banks.

Lastly, savings associations subject to the oversight of the **Office of Thrift Supervision** are estimated to number 1,104.[31] Our estimates suggest an average hourly labor rate for thrifts of about $17.03, giving an annual labor opportunity cost estimate for compliance of all thrift institutions of $846,000.

Method 2—*Mercatus Estimates Based on Total Number of Deposit Accounts*

Method 2 reflects the fact that the costs of complying with the privacy rule are likely to vary directly with the number of accounts that a financial institution has at any given time. We estimate total costs, therefore, as a function of the number of deposit and loan accounts outstanding, and the likely burden per account.

The number of deposit accounts per institution comes from the June 1999 Call Reports collected by the FDIC. However, since there are roughly 10,000 depository institutions in the US that may be subject to the rule, and the *number* of deposit accounts is not aggregated, Mercatus elected to sample major institutions around the US to derive the total number of deposit accounts. Our sample consists of 54 institutions, including almost all of the largest US financial institutions.[32] This sample represents more than half of the US deposit base.[33] The total number of deposit accounts in the US as of June 1999, therefore, is estimated at roughly 369 million accounts.

The number of loan accounts is not available from any published source that we could find.[34] Therefore, our estimate of loan accounts is derived as a fraction of the number of deposit accounts. At some level, the deposits and loans should be related inasmuch as banks operate as intermediaries to link savers and borrowers. However, it is expected that loan accounts will be fewer in number because of (a) reserve requirements (that necessitate holding a fraction of deposits in reserve), and (b) the fact that loans tend to be undertaken to facilitate spending that cannot be afforded out of current cash balances (i.e., average loan *dollar values* will tend to exceed average deposit *dollar values*). We therefore estimate the relationship

---

Some portion of state banks is no doubt part of the Federal Reserve System and to that extent represents double counting in the data. However, inasmuch as we are estimating labor opportunity costs, such differences should not invalidate the estimates derived from them.

[31] Proposed rule, p. 8783. SIC 6035 (Federally Chartered Savings Institutions) shows 173,441 employees with a total annual payroll of $5.4 billion.

[32] Of the top 50 financial institutions in the US as of 1999—as determined by the Federal Reserve Board and available at http://www.ffiec.gov—Taunus Corporation (number 9), HSBC North America (11), Bankmont (26), Citizens of Rhode Island (37), Compass (42), Allfirst (44), and Bancwest (45) did not have June 1999 Call Reports available at the FDIC. Amsouth (23) was also excluded because its June 1999 Call Report was unavailable. Therefore, to the remaining top 42 we added TB&C, First Citizens, First Virginia, GreenPoint Financial, First National of Nebraska, Pacific Century, Mercantile of Baltimore, Cullen/Frost, Wilmington Trust, Riggs Bank, and Mercantile of St. Louis. The choice for inclusion was based on size of the institution's deposit base (deposits of more than $3.0 billion) and/or on an institution's proximity (geographically) to one it may be replacing in the Fed's top 50 list.

[33] Our sample of 54 institutions covers 50.8% of all deposits as of June 1999 (measured in dollar volumes).

[34] Conversations with the Federal Reserve's Research Department confirmed this fact.

between deposit and loan accounts is approximately ten deposit accounts to every one loan account. Under these assumptions, the number loan accounts is estimated at nearly 37 million, and therefore the total number of deposit and loan accounts is more than 406 million as of June 1999.

We estimated the cost of notifying customers of the institution's privacy policies and practices at fifty cents per account. While this cost could arguably be higher if all paper notices were required by the rule, the option of notifying customers electronically may substantially reduce this cost. Thus, we have chosen a lower and more conservative unit cost figure. The annual costs of notification therefore are roughly $203 million.

As a benchmark to estimate the number of account owners who might elect to opt out in a given year, we rely on an estimate furnished in the Department of Health Human Services proposed rule to protect medical privacy.[35] In its proposed rule, HHS stated that as many as one in six individuals may presently be taking adverse actions, including treatment avoidance, in order to protect their medical privacy.[36] If a similar relationship holds with respect to financial privacy, perhaps as many as 17 percent of account holders might be expected to opt out of disclosures of their personal financial information over time.

It seems reasonable to assume, however, that not all individuals will exercise their rights to opt out immediately, and that there would be some degree of turnover among those who elect to opt out. Therefore, we have assumed that in any given year, financial institutions may see perhaps five percent of their account holders exercising their rights to opt out of disclosure. Further, we estimated the costs associated with recording and fulfilling the opt out request at $1.00 per request. This figure is assumed to include the costs associated with programming and maintaining account systems, on-going record keeping, personnel training, and so on. Under these assumptions, the opt out provisions of the rule can be expected to cost financial institutions at least $20 million per year.

Taken in sum, Mercatus estimates the cost of complying with new financial privacy rules at approximately $223 million per year. Assuming a seven percent discount rate gives a long-run present value cost estimate of nearly $3.2 billion to protect consumers' financial privacy.

---

[35] "Standards for Privacy of Individually Identifiable Health Information: Proposed Rule," 45 CFR Parts 160 Through 164, as found in the *Federal Register*, Vol. 64, no. 212.

[36] *Ibid*., p. 59920.