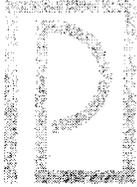


Pillsbury

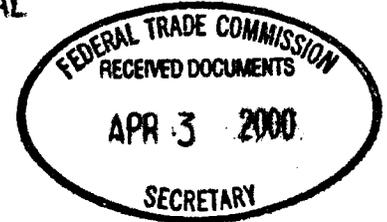


**Madison &
Sutro LLP**

Writer's direct dial number / email:
(213) 488-7320
thoren_ds@pillsburylaw.com

ATTORNEYS AT LAW
725 SOUTH FIGUEROA STREET, SUITE 1200
LOS ANGELES, CALIFORNIA 90017-5443
TELEPHONE: (213) 488-7100 FAX: (213) 629-1033
Internet: pillsburylaw.com

ORIGINAL



March 31, 2000

VIA FEDERAL EXPRESS

OCC
Communications Division
250 E Street, SW.
Washington, D.C. 20219 Attention: Docket No. 00-05

Ms. Jennifer J. Johnson
Secretary
Federal Reserve Board
20th and C Streets, NW
Washington, D.C. 20551 Docket No. R-1058

Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, NW.
Washington, D.C. 20429 Attention: Comments/OES

Manager, Dissemination Branch
Information Management & Services Division
Office of Thrift Supervision
1700 G Street, NW.
Washington, D.C. 20552 Attention Docket No. 2000-13

Secretary
Federal Trade Commission
Room H-159, 600
Pennsylvania Avenue, N.W.
Washington, DC 20580

Re: Proposed Privacy Regulations

Dear Sir/Madam:

I represent a number of banks and non-bank entities, including various Internet companies (collectively "Covered Entities") which offer products or services which appear to qualify as "financial products or services" under the proposed privacy regulations issued by the banking regulatory agencies on February 22, 2000 and by the Federal Trade Commission on March 1, 2000. On behalf of my clients, I appreciate the opportunity to comment on the proposed privacy regulations ("Proposal") issued under Title V of the Gramm-Leach-Bliley Act (GLB).

Although I recognize the difficulty of crafting regulations under broad sweep of the GLB, I have some serious concerns with the proposed regulations, and will discuss these concerns, along with other comments and suggestions, in depth below.

General Comments

Timing And Massive Operational Challenges. Most Covered Entities are unlikely to be able to comply with all of the new privacy requirements by November 12, 2000. Although the basic requirements of the regulations--which involve the disclosure of a Covered Entity's privacy policies to consumers and customers and allowing such individuals to opt out of third party information sharing--are relatively simple and direct, making the strategic decisions and implementing the requisite changes is a daunting task. Perhaps only the Year 2000 initiatives surpass the privacy regulations in the scope of their impact across business lines, products and services.

Based upon my initial analysis of what will be required if the proposed regulations are finalized, all Covered Entities would only have six months to take all of the following actions:

- Perform an in depth internal assessment of every instance in which information about a customer or consumer is collected;

- Perform an in depth internal analysis of every instance in which information about a customer or a consumer is shared with either an affiliate or a third party, including both personally identifiable information and anonymous information;
- Perform an internal review to identify where consumer and customer information in the possession of the Covered Entity is housed, who has access to such information, and who controls its release;
- Perform an internal review to identify every piece of information which has been provided to consumers and customers about a Covered Entity's privacy practices, and collection and use of such information;
- Identify what customer or consumer information collected by an entity or obtained from a third party is considered publicly available;
- Categorize the entity's entire customer base in accordance with the new definitions of consumer and customer;
- Identify which products and services qualify as being "financial products and services" triggering opt out rights and which products and services triggering opt in rights (e.g., certain medical health information);
- Determine whether any of the available exemptions apply to any of the information gathered, and document the reasons for such determinations;
- For each affected product or service, establish procedures to determine when a customer relationship begins and terminates for purposes of the GLB;
- Establish new systems and procedures to deliver annual privacy notices to customers who normally do not receive periodic notices and statements, as well as those who do;
- Review all agreements with third parties to identify the type of information currently shared (both personally identifiable and anonymous data and determine the contractual rights under each agreement to limit such sharing, and take all requisite actions, including but not limited to renegotiating the agreements and providing required notices, etc., required by such agreements to advise the third parties of the changes required by these new regulations, and then implement such changes;
- Have senior management/team meetings to determine whether the new regulations require changes to current practices, policies and or procedures and to set the company's strategy regarding the use and sharing of consumer or customer information;

- Identify proposed changes to current practices, policies and procedures and obtain management buy-in on how such changes will be implemented;
- Determine how to segregate consumer and customer information subject to these new regulations which is collected in person, on paper, by telephone, or by computer or other electronic means;
- Identify and build the requisite systems and firewalls needed to keep financial and insurance information segregated from information that is either not subject to the regulations or is covered by an exemption. Where information is collected on website firewalls, separate paths will need to be built within the website to segregate information subject to opt-in requirements (e.g., medical information), from information subject to opt out requirements, from information which is not covered by the regulation at all. Given the time and costs involved with making significant revisions to websites, and building different information paths within a website, this will be an extremely difficult, time-consuming and expensive task;
- For companies that operate in more than one state or operate over the Internet, build in an overlay which recognizes the different requirements in different states (e.g., California may enact opt in requirements for all financial information, which will mean that distinct practices, policies and procedures will need to be set up for information obtained in California).
- Develop and roll-out new forms, policies and procedures;
- Prepare new privacy policies and statements and provide them to all customers and consumers as required;
- Set up systems to respond to customer inquiries and complaints about privacy related matters, and prepare and provide scripts to customer service providers and telephone centers to advise customers and consumers of the Covered Entity's information sharing practices;
- Determine how to obtain and maintain address and other identifying information on all consumers who attempt to do business with the Covered Entity, but who do not become its customers, to ensure the continued ability to contact such consumers at a later date to advise them of any change in the Covered Entity's plans to share their information;

- Train a vast number of personnel on the collection, handling and protection of consumer information. and teach them about what they can and cannot disclose to affiliated entities and third parties;
- Provide training on the absolute prohibition on sharing of any financial institution account numbers, or access number or code for a credit card account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer;
- Provide training to all marketing personnel and business development personnel informing them of the new limitations on collecting and sharing consumer and customer data;
- Perform appropriate financial analyses of the fiscal impact on the Covered Entity of the changes in its practices or the discontinuance of the sharing of either anonymous or personally identifiable information with third parties and, in some instances, affiliated parties;
- For public companies or companies in the process of going public determine the ramifications of these new restrictions and limitations on the valuation of the company, especially if there are alliances or significant advertising revenues which will be cut off or negatively impacted by these new regulations;
- Determine what information is currently shared with controlled or controlling entities which are not financial entities and may be unaware that they will be subject to these restrictions and advise such controlling or controlled entities of the new limitations and requirements applicable to customer and consumer information shared with them;
- Reassess, improve and implement (and for some banks establish new) policies to protect the confidentiality, security and accuracy of information;
- Develop new policies to oversee or monitor third partys' compliance with privacy standards;
- Establish a centralized database program and reporting system to implement and maintain the opt out and opt in requirements;
- Set up a mechanism to address any new or additional state law requirements.

In practice, Covered Entities will have to complete preparations at least one month before November 12 because of the 30 day opt out lead time and to conform to statement mailing schedules.

Underlying each of these new tasks are concomitant programming changes and testing that must be made (particularly in the area of complying with opt out requests), preparation of training materials, provision of legal services, preparation and implementation of compliance and audit procedures, and associated record keeping. Additionally, the end of the year is perhaps the worst implementation period because of year end reporting and heightened business activities.

I believe it would be appropriate for the Agencies to comply with the GLB timing requirements by making the regulations effective in November, but to phase in certain requirements during a transition period. For example, for a period of 12 to 18 months, the initial disclosure requirement should apply only to new customers. During the interim, Covered Entities could post privacy procedures at offices and on their websites until existing customers are phased in.

The regulations should also make clear that the customer base may be given the initial disclosure in stages rather than all at the same time, which could create an operational logjam for Covered Entities and a significant challenge to the postal service. Staggering the initial notice would also avoid an annual rush of year end notices and relieve consumers from receiving multiple notices from different institutions all at once.

Third Party Agreements. Covered Entities should be allowed to include privacy provisions in their agreements with third parties or make changes to the information sharing/confidentiality provisions in those agreements as they are renewed or entered into rather than immediately. As a matter of general contract law, a contracting party has no obligation to assume a new obligation or covenant with respect to an existing contract. Covered Entities subject to these new regulations, some of whom may have hundreds of affected contracts, are likely to have to offer new consideration (concessions) to obtain these contract modifications, an expensive and time-consuming endeavor for which there is no assurance of success. Alternatively, such entities could change service providers, which would be even more costly and monumentally disruptive to business. For these reasons, I strongly urge that the Agencies adopt some form of transition period.

Uniformity. It would be very helpful if the Agencies issue uniform final rules. Uniformity is mandated by the GLB for good reason. As the Agencies know, variations in regulatory standards have important competitive effects. But more importantly, uniform regulation of privacy standards benefits consumers in the same way as APR and finance charge disclosures do.

Uniformity of federal regulations would be especially welcomed given the prospect of inconsistent state laws that Covered Entities are almost certain to face. This issue is important to all such entities, but particularly to those operating in more than one state and to holding companies with financial institutions subject to different primary regulators. I encourage the

agencies, including the FTC and other nonbanking agencies, to continue to cooperate in the development of uniform final regulations.

Notice To Non-Bank Entities Which Will Be Subject To The Regulations. The regulations will apply to many businesses which have little or no idea that they will be subject to a law which was enacted under the name of the Financial Modernization Act. Although the proposed regulations and the FTC's proposed regulations note that the the regulations will apply to more than just banks, I sincerely believe that an extremely high percentage of non-bank entities which will be subject to these regulations are absolutely unaware of them, and accordingly not only do not understand what they will be required to do, but also have no plans to even start addressing the implementation required. I think it is imperative that the Agencies, and especially the FTC send out notices, make announcements, hold seminars, etc., to try to advise all of these businesses of the fact that they will subject to these new regulations, help them through what is needed, and allow sufficient time for appropriate implementation.

Specific Comments

Personally identifiable financial information. It is imperative that the Agencies recognize the extremely uneven playing field the proposed regulations create by trying to require disclosures and opt out or opt in requirements for the sharing of anonymous data that was initially derived from personally identifiable data. Virtually every business in the United States (and elsewhere) performs extensive analysis of information they have obtained from their customers. Many businesses choose to share such data with others after the personally identifiable information has been stripped out, and I believe that few, if any, consumers in the United States care about whether anonymous data initially gathered from their information is shared with others. An example of such anonymous data would include a scenario where my bank, which knows who I am, where I live, my account balances, etc., strips out my name, my social security number, my phone number, and my account number, and then advises a third party that it has a female customer who lives in Los Angeles who has bought certain types of financial products and services in the past year, and that my age is in 35 and 45 bracket. It is my impression that almost half of the data analysis and sharing done today in the United States involves such anonymous data. Nevertheless, the proposed regulations could be construed as requiring Covered Entities to obtain consent (via opt in or opt out) from their customers to share such anonymous data with others unless the initial information was either obtained from public records, or is contained in public records. Not even the European Union's Directive on Data Privacy attempts to extend its limitations and protection to such anonymous data. Despite the ability of every other business in the United States not subject to the GLB to share, sell, slice and dice the exact same information with third parties, only Covered Entities will be prohibited from doing so. Such a limitation upon a reasonable use of information which is not personally identifiable will simply exacerbate the current disintermediation of banks and other financial services providers.

In connection with this issue, the Agencies asked for comment on whether the proposed definition of "nonpublic personal information" would cover information that contains no indicators of the consumer's identity. I believe the answer is "yes" and this result is contrary to the plain language of the GLB and presumably the intent of Congress. The GLB states that nonpublic personal information is "personally identifiable financial information." If personally identifiable financial information is obtained by a bank or other entity by any of the following means, then the information is deemed to be protected nonpublic personal information: (1) if it is provided by a consumer; (2) if it results from a transaction; or (3) if it is otherwise obtained about the consumer.

While the term "personally identifiable financial information" is not separately defined in the GLB, much of its meaning is intuitive. Information is personally identifiable if it includes an identifier such as a name, address, social security number or telephone number. It is the kind of information that raises potential privacy concerns. By contrast, information that is *not* personally identifiable poses no real consumer privacy concerns and, I believe, is not and should not be subject to the GLB.

The Proposal appears to overstep the core concept of protecting only information that is personally identifiable when it extends the information subject to the regulations to "*any* information (i) provided by a consumer . . ." Section 3(o) (Alternative B, emphasis added). The agencies' slight reshuffling of the definition would make the statutory purpose of protecting information that is "personally identifiable" superfluous and meaningless.

Similarly, in Section 3(n)(2)(ii) of the Proposal, whether a list of consumers is treated as "nonpublic personal information" should depend on whether it contains personal identifiers. The result under the Agencies' interpretation is quite different. If a list or grouping of consumer information is, by definition, nonpublic personal information (because it is obtained from consumers), then there can be no list that is not protected unless it consists solely of publicly available information. But this reading would render the phrase, "derived without using any nonpublic personal information," redundant. The only obvious (and sensible) construction of Section 509(4)(C)(ii) is to read "derived without using any nonpublic personal information" as the term is defined, namely, derived without using information that is personally identifiable.

It is extremely important that the Agencies preserve this core principle that only financial information that is personally identifiable is protected. In the preamble, the Agencies listed some examples of the types of disclosures (e.g., of aggregate mortgage lending data) that are likely covered even though they raise no consumer privacy concerns. To this example I can add the sharing of aggregate (non-identifiable) data for purposes of economic forecasting, market research, calibration of credit scoring models, and academic studies. These types of disclosures pose no more consumer privacy concerns than does the submission of CALL Reports or HMDA

data, portions of which are of course available publicly. Coverage of these types of disclosures would result in the data becoming more expensive, if not entirely unavailable.

With regard to Federal Reserve's request for comments on its proposed Alternatives A and B to define nonpublic personal information I note that Alternative B is more consistent with the GLB. Publicly available information is public regardless of whether a Covered Entity actually derived the information from a public source. For the reasons stated above, and to avoid inconsistent regulation on this extremely important aspect of the regulations, I strongly urge the Agencies adopt Alternative B, but only after it is modified to exclude anonymous data, regardless of where the data is obtained or whether it is otherwise publicly available.

For the same reasons, I strongly suggest that the definitions listed in Sections 3(n) and (o) of the Proposal directly track the statutory language and be revised to include the following language:

“ . . . Aggregate consumer information however obtained by the financial institution, that contains no personal identifiers (such as name, address, telephone number, tax ID number) is not nonpublic personal information.”

It should also be noted that the proposed definition makes no attempt to give meaning to the term, “financial information,” as opposed to simply, “information.” All information collected by a Covered Entity is no more “financial” than all information given to a lawyer is “legal.” While Congress chose not to define this term, the term can only sensibly refer to information that describes a consumer's financial status or dealings, and the Agencies should similarly refrain from trying to define the term.

“Collect.” The concept of what information is “collected” and thus protected is an important one. The Proposal's definition hinges on the ability of a Covered Entity to organize and retrieve the information. I support this approach. However, I note that any information can be organized or retrieved, albeit with considerable effort and resources. Accordingly, the Proposal should clarify that it covers only information that is organized and retrievable in an automated fashion.

Fact that individual is/was a customer. Although I understand the concerns that underlie Section 3(o)(2)(C), which states that the fact an individual is or was a customer of a Covered Entity is itself nonpublic personal information, it should be noted that any person to whom an individual gives a personal check by definition also “knows” such information. Section (D) goes even further by covering a disclosure made “in a manner that indicates” an individual is or was a customer. Accordingly, I am concerned that the mere disclosure of a customer relationship could be deemed unauthorized even if it was made in the ordinary course of business or made inadvertently by an individual employee. For example, merchants today commonly place telephone calls to banks to determine whether there are available funds in a customer's account prior to accepting a customer's check as payment for a good or service. This practice may be

prohibited under the proposed regulations. To state affirmatively that an individual's present or past association with a bank is protected information serves only to increase the likelihood of a technical violation wholly unconnected with a breach of consumer privacy. Moreover, a prohibition on sharing such information with third parties is also likely to cause a significant increase in fraud losses due to a third party's inability to confirm the existence of an account with a bank. Such a prohibition actually plays into the hands of individuals who engage in identity theft.

Although a person's name is public information, a person's association with a bank is hardly confidential financial information. I acknowledge, however, that the GLB extends to the act of selling or otherwise disclosing a customer list, even if it contains customer names only, *for marketing purposes*. Adding proposed examples 3(o)(2) (C) and (D) might reinforce the prohibition against selling customer lists, but it would also compound the likelihood of innocent violations. Accordingly, I suggest that these examples be deleted and replaced with a purpose test, namely that disclosing a customer relationship is prohibited only if the sole or primary purpose for the disclosure is for marketing purposes.

Timing of initial disclosure. Section 503(a) of the GLB requires the initial disclosure be given "at the time of establishing a customer relationship," and not "prior to" as proposed in Section 4(a)(1). The GLB sets forth the general principle that a bank's or other covered entity's privacy policies should be one factor to be considered when a consumer obtains a financial product or service. Therefore, a privacy disclosure should be provided at the inception of the relationship, but not necessarily before. This is the same general principle underlying other consumer protection statutes such as the Truth in Lending Act (Regulation Z), the Expedited Funds Availability Act (Regulation CC), and Electronic Funds Transfer Act (Regulation E). Those laws require initial notices, but also provide specific exceptions to timing requirements. For example, Regulation CC requires the initial funds availability disclosure to be given "before" an account is opened. 15 U.S.C. Section 4004(a). But Federal Reserve rules allow the notice to be delivered a business day *later* if the bank receives a written request by mail, along with an initial deposit, to open an account. Commentary to 12 CFR 229.17 (Regulation CC). Under the Proposal, a privacy disclosure provided to a consumer credit customer could be found to be late if given before the first transaction is made, rather than before the application is approved. To create a new set of rules applicable only to the new privacy disclosure would create unnecessary and costly burdens. It would also increase the risk of technical violations, and unnecessarily complicate a transaction to the extent consumers receive multiple disclosures at different times

Privacy disclosures, unlike any previous regulatory requirement, apply to multiple business lines, including customers who normally do not receive periodic notices or statements, and even to noncustomers who are consumers. An inflexible "prior to" standard is bound to set up Covered Entities for violations, particularly in the areas of Internet, telephone and kiosk banking and other financial services. It places too much emphasis on when an individual becomes a customer and the factual circumstances surrounding an application.

The Proposal should establish a general rule that the initial privacy disclosure must be provided "at the time" of establishing a customer relationship, but clarify further that a bank or other Covered Entity is permitted to coordinate its delivery with existing notices applicable to the product or service being obtained. Where other regulations provide exceptions to general timing requirements, then delivery of the privacy disclosure in compliance with those exceptions should also be deemed timely. This allowance is reasonable because if an institution does not share the customer's information, a strict timing requirement would provide little or no additional consumer benefit. If information is shared, then the opt out procedures offer ample protection.

As to products and services for which no regulatory disclosure requirements apply, a customer is sufficiently protected if the disclosure is given any time prior to, at the time, or at a reasonable time after becoming a customer, as long as no customer information is shared before the disclosure and an opportunity to opt out is provided.

Content of initial disclosure. Section 503(b) of the GLB requires disclosure of *categories* of information collected and persons to whom information is disclosed. Use of the term "categories" was intended to allow the disclosure of "categories of information collected" and "categories of persons" to whom information is disclosed rather than simply "persons to whom information is disclosed." Unfortunately, however, the Proposal goes beyond the intent of the law by requiring the listing of the sources of information collected and examples of information disclosed, and by prohibiting the use of general terms. If the term "source" in Section 6(d)(1) means a description of each separate instance in which information is provided, such as "credit card application" or "certificate of deposit application," then this portion of the disclosure by itself could be extremely long. Explaining who has access to information and the circumstances of access (Section 6(d)(5)) is a vast undertaking, as is describing measures to protect against threats. Instead of a single page disclosure, the Proposal seems to contemplate one of multiple pages or a booklet.

The consumer benefit of a lengthy disclosure is questionable. In most instances, the disclosure will be provided with other notices and agreements. Thus, the longer the disclosure, the less likely it is to be read. A loan applicant, after all, may have little interest in the specifics of how a Covered Entity handles information in its non-lending departments. For entities that do not share information with third parties, the value of a detailed description of what information is collected is questionable. For entities that do share information with nonexempt third parties, the critical item of information to provide is a clear and conspicuous opt out notice.

Furthermore, a detailed disclosure requirement would be costly to develop, produce and deliver. To reduce costs and complexity of compliance, most Covered Entities will attempt to use a single disclosure for all lines of business. However, the greater the detail required, the less likely use of a single disclosure is practicable, and revisions to such a document are likely to be

neverending. The more detailed the disclosure is, the more likely it is to be fodder for a plaintiff's attorney to bring suit for any alleged failure to disclose every possible detail of every aspect of the entity's privacy and information sharing practices. For whatever it is worth, of all of the privacy disclosures I have written for various entities, the ones that were best received (and even analyzed in major American newspapers) were privacy statements that were short and succinct.

If there is any doubt in the consumer's mind as to the policies of the Covered Entity, the consumer can opt out at any time, or contact the entity for additional clarification. I believe the intent of the GLB is to provide a consumer with sufficient information to make an informed decision whether to do business with the Covered Entity, and then decide whether to opt out. Therefore, the requirement to list the source of information collected and to provide examples should be eliminated.

Any mention in the initial notice of exempted disclosures under Sections 10 and 11 is unnecessary (thus Section 6(b) should be deleted). The use of general terms and general assertions is a necessity. Indeed, in light of the proliferation of disclosures consumers already receive from banks, the regulations should strongly recommend that the privacy disclosure be no longer than necessary. For clarification, the regulations should also provide detailed examples of acceptable disclosures. A short version of a disclosure will have to be permitted when given at an ATM because of the inability or difficulty to scroll down.

Annual privacy disclosure. The Agencies invited comment on the method Covered Entities intend to use to deliver annual privacy disclosures. Banks will primarily mail the disclosures with periodic statements or other notices; while Internet companies will undoubtedly post the information on their website.

With respect to customers, prior customers and consumers to whom periodic or annual notices are not required I suggest an alternative means of disclosure. The privacy interests of these consumers would be well protected if, in the initial notice, they are informed that the institution's privacy policy can be obtained at any time at the institution's website or at the Covered Entity's offices accessible to the public. This is a fair accommodation because of the expense involved in programming and other financial and environmental costs in connection with a separate mailing to such customers.

Liability for third party actions. (Sections 9(a) and 12(b)(1)). I am extremely concerned about Covered Entities' responsibilities with regard to third party use of disclosed consumer information. The Proposal should clarify what the *specific* responsibilities are with regard to third parties and should provide a safe harbor for Covered Entities from regulatory and civil liability. Although I agree it is important to try to prevent contractual third parties from breaching consumer privacy, it would not be possible for a Covered Entity to ensure that no such

breach occurs, and accordingly they should not be held liable for the acts of third parties committed in violation of contract.

I believe the GLB requires only that Covered Entities include appropriate contract provisions in their third party agreements. A contract covenant is subject to enforcement provisions that may entitle the bank or Covered Entity to obtain a civil injunction, to impose monetary damages, enforce indemnity provisions, or to terminate the agreement entirely. These potential consequences provide ample disincentives against unauthorized use of consumer information. While the Proposal does not imply a duty to monitor or audit, it would be helpful if the final regulation state that no such obligation is imposed.

Any requirement that covered parties are responsible for the acts of the third parties with whom they do business would be onerous and expensive and, more critically, would imply a level of duty that would expose them to unfair and potentially unlimited liability. A Covered Entity of any size would almost certainly be joined in any civil or class action for breach of privacy arising from the actions of its contract party. If the Covered Entity is subject to heightened regulatory obligations to supervise the offending party, then its exposure is also heightened.¹ The GLB cannot be reasonably construed to demand such a result, and the risks are sufficient to warrant clarification on this issue. Accordingly, it is recommended that the following provisions be added to the final regulations:

“A financial institution or other covered entity is not in violation of this regulation, and is deemed to have acted reasonably if its agreement with a nonaffiliated third party includes a covenant that such third party must abide by the requirements set forth in ____.”

“Nothing in this regulation requires a financial institution or other covered entity to supervise, monitor or take any other actions to ascertain a third party’s compliance with contract provisions required by this regulation. If the financial institution or other covered entity receives actual notice of an unauthorized disclosure by such third party, then the financial institution or other covered entity is not in violation of [the appropriate section] and will be deemed to have acted reasonably if it takes such actions as are consistent with its general enforcement policies applicable to other similar contracts.”

It is important to note that the GLB does not require a Covered Entity to ensure that the third party uses the disclosed information solely for contracted purposes. Section 9(a)(2)(ii). The law requires only that the third party maintain the confidentiality of information to at least

¹A similar situation arises where a bank sells servicing rights but not the loans themselves, then relies on the cooperation of the servicer to deliver annual privacy disclosures. Banks can protect themselves by ensuring that servicing rights are transferred with privacy obligations attached, but should not be held liable if the servicer either refuses or fails to comply.

the same extent that the Covered Entity does. While in most instances the effect may be the same, the imposition of an additional requirement may raise unintended issues and complexities, and for this reason alone section 9(a)(2)(ii) should be deleted.

Electronic notices. The Agencies' proposal to require customer agreement as a condition to using electronic disclosures is consistent with the Federal Reserve's Regulation E and pending electronic disclosure proposals. I ask the Agencies to adopt and publish final regulations that specifically allow the use of electronic notices, and allow their use in a multi-state context, or over the Internet. The ability to give electronic notices may become completely irrelevant if each state is allowed to adopt its own requirements related to what "counts" as a customer agreement, as an attempt to try to comply with such state-by-state requirements may simply be unworkable for a Covered Entity.

I am very concerned about any rigid requirement that customer agreement to receive electronic disclosures must be obtained in advance. There are instances in which it is not practical for prior consent to be obtained. For example, Regulation Z permits credit card initial disclosures to be provided after the credit card account has been approved and established, but prior to the first credit card transaction. Alternatively, I ask the Agencies to consider eliminating the agreement requirement altogether. If a consumer is obtaining a product or service through the Internet and has provided an email address, then very little additional consumer benefit is achieved by seeking consent to deliver a disclosure electronically. Rather, consent should be assumed so long as physical delivery of the disclosure can be provided upon request.

I also note some confusion with Sections 4(d)(4)(i)(C) and (D), which require consumers to acknowledge "receipt" of the disclosure given through a website or an ATM. As to a website, receipt might mean that the disclosure is downloaded, printed, or simply acknowledged with a click. So long as the disclosure page must be acknowledged (either by a click on a box or by proceeding to the next page) as a condition of completing the transaction, the initial disclosure requirement should be deemed fulfilled. The consumer is free to print or download the disclosure. As to other types of electronic terminals, such as ATMs, it should be sufficient that the disclosure screen appears and the user proceeds to the next screen to conduct the transaction.

Notices to joint owners. The Agencies invited comments about delivering privacy notices to account joint owners. In other contexts where disclosures are required, the Agencies have consistently concluded that notice to a single owner of a joint account is sufficient. See 12 CFR 202.9(f) (adverse action notice); 12 CFR 226.5(d) (finance charge disclosure, with exception); and 12 CFR 229.15(c) (funds availability policy). Underlying these rules is the appropriate assumption that joint owners, who often reside at the same address, will have access to the respective notices. Where joint owners do not reside at the same address, the other address(es) are often not available.

Applying the same rule here would allow Covered Entities to coordinate delivery of the initial and annual privacy disclosure with existing notice and statement requirements. As discussed earlier, the flexibility to do this could significantly reduce regulatory burden. Any conflicting requirements would require Covered Entities to alter application procedures, develop new systems, and deliver notices to individuals who normally receive no other direct correspondence with the entity.

Definition of consumer. Section 509(9) of the GLB defines consumer as an individual who *obtains* a financial product or service. The Proposal expands the definition with an example of an individual who applies for a loan *regardless* of whether it is extended. Similarly, the definition of “financial service” is extremely broad, including mere evaluation of an application. The GLB states without ambiguity that an individual who does not ultimately obtain a product or service is not a consumer. The Agencies should not ignore the plain meaning of the statute simply because they might disagree with the policy implications. The GLB’s policies were the result of careful compromises and balancing of competing interests and must not be overturned by regulatory fiat.

The preamble to the proposal states that a consumer would not necessarily become a customer simply by repeatedly engaging in isolated transactions, such as making regular withdrawals from an ATM owned by an institution with whom the individual has no account. We would add other examples such as purchasers of cashier’s checks, individuals who fail to fully complete loan applications, individuals who request but do not obtain credit card cash advances, check cashers who do not have accounts at the institution, and mere visitors to a Covered Entity’s website who do not obtain a password or otherwise take the required actions to become a customer. I believe adding these examples would be extremely helpful. Moreover, in practice, it would be impossible for a Covered Entity to treat such individuals otherwise as it would normally have no address to which to send annual privacy disclosures.

The Proposal accurately restates without elaboration the GLB reference to a consumer’s legal representative. Presumably, since “consumer” is the basis of the definition of a customer, this issue applies to customers as well. It is not evident what is intended by this definition and clarification would be helpful. Also, Section 3(e)(2)(iv) describes as an example of a consumer an individual who negotiates a workout of a loan regardless of whether the bank originally extended it. Similarly, Section 3(e)(2)(v) refers to an individual who has a loan from a bank as a consumer. The Proposal provides, as an example of a customer, a consumer who has a credit “account” with the bank. Section 3(i)(2)(1)(A). In each of these examples the described consumer must be a customer, and if any distinction is intended by reference to an “account,” that distinction is not evident.

Definition of customer. The proposed definition of customer and the examples provided are intuitive and helpful. In most instances there will be no doubt who is the customer. However, because of the breadth of this regulation, many of the finer points addressed in other regulations

regarding, for example, whether a credit is obtained for a consumer purpose under Regulation Z (see "primary purpose" tests under 12 CFR 226.2(a)(12) and 226.3(a) and associated commentary), must be observed. Other questions arise with respect to guarantors, beneficiaries and the like. To this extent, further examples of who are and are not customers would be helpful. If no further specific examples are provided, then we suggest that the regulations state affirmatively that Covered Entities may consult existing guidance in other regulations to resolve questions not specifically addressed here, and that reasonable decisions are not subject to challenge.

As to dormant accounts, a Covered Entity should be free to declare an account dormant by whatever applicable standard it chooses to follow, and the regulations should specify that Covered Entities will not be subject to second guessing about when an account is terminated as long as the decision is made in the ordinary course of business.

Opt out notice and opportunity. I agree with the general rule that the opt out notice and opportunity must be given a reasonable time before any information is disclosed by the Covered Entity. In most instances, the Covered Entity will provide the opt out notice with the initial notice. Example 7(a)(3)(i) would allow a consumer 30 days to make an opt out decision, a period we believe is unnecessarily long. An institution that has uses for consumer information may find its value (typically as a marketing lead) will diminish quickly. A substantially shorter period of 5-10 days is sufficiently protective, especially since consumers would be permitted under Section 8(d) to opt out at any time.

Section 8(b)(1) states that an institution must provide the opt out notice within a reasonable time after entering into an oral agreement, if the customer agrees. The presumption underlying this section--that the opt out notice is normally provided at the time the customer relationship is created--is contrary to the general tenor of the Proposal. The notice must be provided some time before information is disclosed to a nonaffiliated third party, regardless of how the customer agreement was entered. The customer need not agree to a later delivery where there are no negative consequences. Accordingly, the second sentence in 8(b)(1) should be deleted.

Similarly, a consumer in an isolated transaction with a Covered Entity should not be required, as a condition of completing the transaction, to decide whether to opt out. Section 7(a)(3)(ii). The Covered Entity should be able to provide the opt out notice and opportunity either at the time of the transaction or at a later time as long as no information is disclosed before the opportunity is provided. As an alternative (and this comment would apply generally), a Covered Entity should be permitted to provide a telephone number as a means to opt out.

Section 7(b)(4) would require the initial notice to accompany the opt out notice if the latter was not delivered to the consumer originally with the initial notice. The GLB does not require this and I believe it is unnecessary. If a consumer is inclined at all to prevent the Covered

Entity from disclosing information and can do so through a simple procedure, it is hard to imagine what additional benefit is afforded by re-delivery of the privacy disclosure. My opposition to this requirement would be redoubled if the Agencies do not accept the recommendations to substantially shorten the length of the privacy disclosure.

A consumer's decision to revoke an opt out decision should not be required to be made in writing. Section 8(e). A Covered Entity should not be forced to refuse an oral request and the customer should be spared the indignity of such a refusal. Also, it is difficult to imagine an opt out decision communicated electronically that is not made without the agreement of the sender. The writing requirement to revoke an opt out decision and the agreement requirement for an electronic election should both be removed as paternalistic and unnecessary.

The opt out notice should not contain information already set forth in the initial notice. It should simply state that the consumer's information may be disclosed to nonaffiliated third parties as described in the initial notice and describe how to opt out. The example in Section 8(a)(2)(ii) should be revised accordingly.

I have extreme concerns with the apparent obligation to advise consumers who do not become customers of any change-in-terms implemented to a Covered Entity's privacy policy in order to give such consumers a new right to opt out. In many instances, the Covered Entity will simply not have any access to the consumer's current address or other information to enable it to provide such notice. It is not reasonable to believe that a Covered Entity will have an ongoing ability to locate consumers who are not customers. I note, for example, that even federal and state government agencies are unable to locate most consumers who are the owners or beneficiaries of escheated funds, and do not understand why the Agencies think that Covered Entities would be able to do so when the government cannot. Moreover, I find it frightening that there appears to be no time limitation on this obligation to advise consumers of a change-in-terms, which would effectively mean that a Covered Entity would have to go back as far in time as necessary to try to find and notify such consumers. In lieu of this requirement it would be viable for a Covered Entity to advise consumers in their initial notice that the Covered Entity may change its privacy policy and information sharing practices from time to time, that the consumer should check with the Covered Entity's offices or website as frequently as he or she deems appropriate to determine the Covered Entity's current privacy and information sharing practices, and have the Covered Entity post such changes at their website for a period of at least 30 days prior to implementing the changes into a new privacy policy or information sharing practices.

The Agencies should clarify that by allowing Covered Entities to disclose categories of information that Covered Entities reserve the right to make disclosures in the future and the parties to whom they reserve the right to disclose relieves them from having to revise policy notices later when those changes come to pass.

Implementing opt out. One of the most operationally challenging requirements of the privacy regulations will be tracking opt out decisions. To implement an opt out system successfully in an industry that is highly automated, Covered Entities are looking to the Agencies to craft thoughtful guidelines that take into account how Covered Entities actually function. I note initially that the language of the GLB on this issue is general and does not preclude the exercise of regulatory discretion.

Fundamentally, an effective opt out system simply cannot be based on the rule that an opt out decision is effective until revoked. Because of the unlikelihood of a revocation, this rule forces Covered Entities to manage opt outs that never terminate. In some respects, it would be the operational equivalent of a permanent stop payment order that is enforceable even after the customer is no longer a customer. In time, customers move on and customer information (including any opt out decision) is purged, usually long after the information has any possible value to anyone, let alone third parties. Under the Agencies' Proposal, as discussed below, each opt out decision eventually becomes a land mine hidden in a field.

It helps to appreciate the magnitude of the risks of the "effective until revoked" rule by observing its general effect 10 years from now: the pace of change in the industry has remained brisk and customers have moved about freely. Consider the following situations: (1) a customer opts out, leaves the Covered Entity, and then returns 10 years later without reaffirming a desire to opt out; (2) a consumer opts out when obtaining a loan but obtains a deposit account at the same bank 10 years later; (3) a customer opts out as Joan Smith, leaves the Covered Entity, and returns 10 years later as Joan Jones; (4) Covered Entity A, where John Doe has opted out, is purchased by Covered Entity B, where John Doe is also a customer but has not opted out.

I recommend a rule that an opt out decision must be subject to expiration and, in certain circumstances, to reaffirmation. A decision should expire when an individual is no longer deemed to be a customer for purposes of delivering the annual notice under the Proposal. The risk that personally identifiable information about former customers will be shared is virtually (if not entirely) nonexistent because few, if any, Covered Institutions share personally identifiable information about former customers. Also, if an individual who has opted out becomes a noncustomer and then a customer again, that decision to opt out must be reaffirmed. These are reasonable compromises. With each passing year the number of such incidents will expand exponentially and the only reasonable alternative for any Covered Entity would be to cut off the flow of consumer information.

Exceptions. The GLB itself does not clearly distinguish the Section 502(b)(2) exception (that includes joint marketing agreements) from the key general exception under 502(e)(1), which is generally understood to refer to third parties on whom Covered Entities rely for core processing and other services. Section 502(b)(2) information sharing is subject to heightened disclosure requirements. I believe the unfortunate use of the phrase "services for or functions on behalf of the bank" in this section was not intended to cover the 502(e)(1) processing exception, which

poses minimal privacy concerns. The regulations should state clearly that the heightened requirements set forth in Sections 9 and elsewhere apply only to disclosures incident to marketing activities and not to Section 10 services and processing activities.

The Section 11(a)(ii) fraud exception should clarify that a disclosure is permissible to protect against fraud, unauthorized transactions, claims or other liability *as applied to customers* as well as the Covered Entity. It makes little sense to draw a distinction turning on whether the Covered Entity or a customer is the victim, especially when so often the Covered Entity ends up absorbing any monetary loss. This clarification would also make certain that a disclosure is permissible under a law that permits a Covered Entity to report potential incidents of financial abuse of the elderly. Such a law is currently pending in the California legislature.

I also ask that the Agencies establish the general rule that a consumer's consent to disclose under Section 11(a)(1) is effective no matter how expressed, and to provide examples. For instance, during an in-person or Internet interactive transaction a Covered Entity should not be required to obtain a written consent to ask whether a consumer would like to obtain preapproval for another product. Oral consent should be permissible from a telephone customer. In an Internet environment, a click on a box on the screen could be an effective consent. In general, the rules must be made flexible enough so that a Covered Entity is not unreasonably impeded from pursuing marketing opportunities. These opportunities, for the most part, benefit both the institution and the customer.

The "dual employee" exception to the definition of nonaffiliated third party, which we support, is an attempt to create a practical distinction where the legal distinction is, unfortunately, anything but clear. Greater clarification is necessary. The Proposal would deem a disclosure to a dual employee an internal one but not a disclosure directly to the other employer. We support this general rule but suggest that the Agencies explicitly negate the legal fact that the employee's receipt of information is ascribed to the other employer. When the disclosure is made *directly by the consumer to the employee*, the regulations should clarify that any sharing of information within either employer is deemed internal and therefore neither subject to the opt out rules nor the consent exception.

Finally, the regulations should provide specific examples of disclosures that do not fall squarely within the exceptions. Without suggesting any particular order of importance, these include disclosures made in conjunction with collection activities, automobile repossessions, to appraisers, to flood insurance providers, to tax service providers and consumer credit counselors. These are the types of disclosures that are not clearly "necessary" to provide a product or service but are nevertheless integral to transactions or to Covered Entities' legitimate interests.

Concurrent state regulation. We understand that the GLB explicitly contemplates state legislation of privacy and that the Agencies have no authority to offer significant relief in this area. As difficult as it will be for Covered Entities to comply with the federal rules, it is the

specter of state legislation that in many ways is more daunting if only because of the difficulty of complying with multiple, conflicting requirements. Because Congress has spoken on this issue we will not dwell on it here. We ask only that the Agencies take every opportunity to provide certainty in the regulations. It would be helpful, for example, in connection with an FTC determination that a state law is not inconsistent with the GLB, that the declaration clarify that compliance with a particular state provision also constitutes compliance with the federal regulations.

Disclosure of account numbers. The Proposal properly restates the GLB prohibition against the disclosure of account numbers and the like for marketing purposes. The Agencies should clarify that a consumer may consent to such a disclosure. Also, account numbers are often encrypted when transferred along with other information, and this practice should be exempted from the prohibition.

I appreciate this opportunity to provide comments to this important regulation and urge the Agencies to carefully consider my suggestions. If you should have any questions, or if I may be of further assistance, please do not hesitate to call me.

Sincerely,

A handwritten signature in black ink that reads "Deborah Thoren-Peden" with a small mark at the end.

Deborah Thoren-Peden