CLOSING THE G-L-B PRIVACY "LOOPHOLES"[1]

by Kevin J. Funnell and Cheryl Crandall Tangen

When the Gramm-Leach-Bliley Act ("G-L-B") was signed into law by President Clinton, he vowed that Part V of the Act, which deals with privacy obligations of financial institutions toward the nonpublic personal information of their customers and certain other "consumers," was only the "first step" in protecting the privacy of such information. The 107th U.S. Congress has seen the introduction of over one hundred privacy protection bills. Senator Paul Sarbanes, a strong privacy advocate, has assumed the chair of the Senate Committee on Banking, Housing, and Urban Affairs. Senator Phil Gramm, the ranking Republican member of the Committee and an opponent of further privacy laws in this area, recently announced that he will not seek re-election when his term expires next year. His replacement on the Committee, Richard Shelby of Alabama, another strong privacy advocate, has proven successful in steering strict privacy protections through Congress, most notably in connection with the imposition of "opt-in" requirements on states that want to sell or share personal information gleaned from motor vehicle and driver's license records. Thus, whether in this session or in sessions to come, additional privacy bills that impact financial institutions are sure to follow. If enacted, these bills would add substantially to the privacy compliance burdens of financial institutions, at a time when most institutions, the public, and Congress have not yet been given an adequate opportunity to determine how well the first step is working or whether, in fact, the first step was needed or desired by the public at all. In addition, numerous other bills, of general application, have been introduced that would limit the use and exchange of certain personal information and subject financial institutions and others to additional privacy regulation outside of G-L-B. By contrast, one House resolution, while recognizing the perception of public concern about privacy issues, would attempt to achieve some balance in privacy regulation by establishing a privacy commission to study issues relating to the protection of individual privacy and to recommend methods of achieving a workable balance between privacy protection and the appropriate use of personal information. Another source of relief, particularly in light of increased state legislative activism on privacy issues, is a House bill that would create federal pre-emption for privacy standards imposed upon financial institutions with respect to any subject matter governed under Sections 502, 503, or 504 of G-L-B.

The following is a description of the six (6) pending (as of September 10, 2001) federal bills that would amend the privacy protection provisions of G-L-B and selected other proposed federal privacy bills of interest to financial institutions. This article is not intended as an exhaustive analysis of the proposed bills; but rather is intended as an alert to financial institutions and their counsel of the existence of legislation that, if passed,

[1] This article is an updated version of the original, which was prepared for and distributed to its members by the Texas Savings and Community Bankers Association.

*Kevin J. Funnell is a partner in the Dallas office of the law firm of Bieging Shapiro & Burrus LLP. (telephone no. 972-377-7392; e-mail kjf@bsblawyers.com. Cheryl Crandall Tangen is the principal of Cheryl Crandall Tangen, P.C. and practices law in The Woodlands (telephone no. 281-296-2881; e-mail ctangen@tangenlaw.com.

may significantly (and, in most cases, detrimentally) impact how such institutions conduct their business. Informed financial institutions and their counsel are encouraged to make their views known to their elected representatives in the U.S. House or Senate. This article discusses only those laws that have been introduced as of September 10, 2001.

S. 30 ("Financial Information Privacy Act of 2001")

This bill was introduced by Senator Sarbanes (D-Maryland), the newly-anointed chair of the Senate Committee on Banking, Housing and Urban Affairs, and is the most comprehensive of any of the bills on Part V of G-L-B introduced thus far in the current session. Highlights of S. 30 follow:

1. **Sharing information with affiliates.** The bill eliminates the "affiliate" information sharing "loophole" of G-L-B. It also limits the previous exception under G-L-B that permitted the sharing of information with non-affiliated third parties for the purpose of performing services or functions for the institution so that this exception to the "opt-out" requirements applies only if the third party (affiliated or non-affiliated) uses such information solely in the performance of such services for the institution, including marketing the institution's own products or services (but not the third party's products or services).

2. **"At least as convenient" opt-out methods.** The method provided to the customer or consumer to "opt-out" of information sharing must be the same method by which the consumer or customer received the notice of his opt-out right (or another method "at least as convenient"). All sharing of nonpublic personal information about customers or consumers, even with affiliates, will require that the customer or consumer be given a convenient method to prevent (i.e., "opt-out"of) such information sharing.

3. **"Opt-in" for spending habits information sharing.** Absent notice to, and "affirmative consent" that has not been withdrawn by, a consumer, the bill prohibits the dissemination to **any** third party (affiliated or non-affiliated) of lists of a consumer's transactions, preferences, or interests, or a list of customers that satisfy criteria involving consumer transactions, preferences or interests (the so-called "spending habits information"), in each case where such information is derived through payment processing services (e.g. transfers by check, debit card, credit card or similar instrument). In other words, consumers will have to "opt-in" to the sharing of spending habit information derived from such payment processing services. Exceptions to the "opt-in" requirement for sharing spending habits information include some, but not all, of the general exceptions that were provided under the original version of Part V of G-L-B in connection with the "opt-out" requirements. Unlike the exceptions to the "opt-out" requirements under original G-L-B, the list of exceptions to the "opt-in" requirements for sharing spending habits information does not permit the sharing of such information with insurance rate advisory organizations or rating agencies of the financial institution, nor with a consumer reporting agency.

4. **Facilitating customer service exception.** For both “opt-out” purposes and the requirement to “opt-in” to the sharing of spending habits information, the bill adds one substantive exception, which is the sharing of information to “facilitate customer service,” such as in connection with the operation of consolidated customer call centers or consolidated account statements.

5. **Health Information.** Written notice to and "opt-in" consent from consumers must be received before an institution may disclose to affiliates or non-affiliated third parties aggregate lists containing or derived from “individually identifiable health information” or use such information in deciding whether or upon what terms it offers or continues to provide financial products or services to a consumer. In addition, the bill clarifies that G-L-B does not affect the privacy standards promulgated by the Health and Human Services Department under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Those standards, adopted late in the Clinton Administration's term of office, are the subject of much current debate. Although Representative Ron Paul introduced in March a proposed joint resolution, H.J.Res. 38, that attempts to repudiate and render null and void those standards, the resolution thus far has been stalled and the Bush Administration has refused to delay the implementation of these regulations.

6. **Restrictions on Third Party’s Reuse or Disclosure of Information.** Third parties can re-disclose nonpublic personal information received from a financial institution to another person or entity only if the disclosure of such information would be lawful for the financial institution to make directly to such person or entity. (Under current law, this limitation only applies with respect to redisclosures by and to <u>un</u>affiliated third parties.) In addition, if the third party obtains such information under one of the general exceptions to the “opt-out” provisions, the third party may only use or re-disclose such information if permitted under that exception or, if the re-disclosure is necessary to carry out the purpose for which the information was disclosed by the financial institution, under another general exception.

7. **Access to Consumer Information.** This is perhaps the most burdensome and far-reaching amendment contained in the bill. It requires access by **"consumers" (not just "customers")** to the "consumer information" that an institution has under its control, and the right to dispute the accuracy or incompleteness of such information. Institutions must correct material inaccuracies or incompleteness in such information. Institutions will be allowed to impose a "reasonable" fee for making access available. The content requirements of the privacy notice would be amended to require disclosure of this right to access and correct “consumer information.” Depending upon the implementing regulations (notably, how the regulators would define “consumer information”, since the bill and existing G-L-B do not), and the information gathering practices of institutions, this section

could impose a substantial burden upon institutions, especially as it may relate to "consumers" who are not also "customers" of the institution.

8. **Non-Compliance as Deceptive Trade Practice.** Makes violations of privacy policies a deceptive trade practice under the FTC Act. Authorizes State Attorneys General to commence actions for violations of the G-L-B privacy provisions "in addition to such other remedies as are provided by State law."

9. **Timing of Privacy Notices.** Requires the initial privacy notices to a consumer "before" the consumer becomes a customer (as opposed to "at the time" he or she becomes a customer, as is required under current law).

10. **FRCP Regulatory Consistency.** Requires the FTC to adopt regulations making the affiliate-sharing provisions of the Fair Credit Reporting Act ("FCRA") consistent with the regulations adopted by the banking agencies under G-L-B. This actually may be a good thing, depending upon how aggressively the FTC attempts to achieve consistency and whether its regulations would, in essence restrain the literal language of FCRA's current "opt-out" requirements, which are much greater than those contained in G-L-B, even if amended by S.30 to apply to information sharing with affiliates.

S. 536 ("Freedom From Behavioral Profiling Act")

This is one of two G-L-B amending bills introduced thus far this session by Senator Shelby. This bill would prohibit a financial institution, without written notice to a consumer and the consumer's affirmative "opt-in," from disclosing the following information to any person (although certain drafting flaws create an uncertainty as to whether "any person" is intended to cover affiliated entities):

(i) any information for the purpose of marketing "nonfinancial products" to a consumer to whom the information pertains; or

(ii) the identity of any person or entity to whom the consumer has made a payment by check or similar instrument; with whom the consumer has engaged in a credit transaction; or from whom the consumer has received any payment or transfer of funds.

The potential complications of this relatively short bill are limited only by the imagination of attorneys. For example, does this bill prohibit, absent an affirmative "opt-in," the sharing of information that is used to market both financial and non-financial products, such as solicitations for credit cards that offer frequent flyer miles for travel on a certain airline? Certainly the solicitation can be said to market that airline's travel services, which is presumably a "non-financial" product. If the literal language of the bill is followed, "any person" may be construed to include government law enforcement agencies and would, for example, preclude, absent the consumer's "opt-in," the disclosure of payment information typically sought by law enforcement agencies in

connection with drug-enforcement or money-laundering investigations or prosecutions. Similarly, the "common sense" general exceptions relating to disclosure limitations under the current G-L-B, such as disclosures required by law or judicial process or incident to the sale of the institution's assets, are arguably not available under this bill to permit the disclosure of the information described above without an affirmative "opt-in." "Any information" could easily be construed to include "aggregate" information that does not identify the consumer. What policy reasons would explain requiring the consumer's consent, via "opt-in," to the disclosure of information where the consumer's identity is not disclosed or discernable? The literal wording of this bill could cause unintended mischief.

S. 450 ("Financial Institution Privacy Act of 2001")

Although less lengthy than S. 30, this bill, introduced by Senator Bill Nelson, a newly elected Democrat from Florida who has been a privacy advocate since his days as Florida's insurance commissioner, would impose the most onerous limitations on the sharing of nonpublic personal information **by requiring across the board "opt-in," as a condition to sharing nonpublic personal information between financial institutions and affiliated or non-affiliated parties** (subject to the existing "general" exceptions that currently apply to the "opt-out" requirements under G-L-B). This bill:

1. **Opt-in.** Requires "opt-in" consent for all sharing of nonpublic personal information. Such consent must be in writing only for "health information."

2. **Definition of health information.** Includes "health information" within the term "nonpublic personal information" under Part V of G-L-B and provides a lengthy definition of "health information" as any information, including genetic or demographic information or tissue samples, collected from an individual that is created or received by a health care provider, researcher, health plan, insurer, health oversight agency, public health authority, employer, or school, that relates to past, present or future physical or mental health of an individual, health care to an individual, or payment for such health care, and that identifies the individual or from which the individual may reasonably be discerned.

3. **Cannot condition products or services on "opt-in."** Prohibits the denial of a financial product or financial service if consent to information sharing is not given. This is a major change in existing law, and would prevent the institution from offering better services and products to those who are willing to permit information sharing.

4. **Privacy Officer.** Requires each financial institution to designate a "privacy officer" responsible for compliance with the requirements of Part V of G-L-B and the institution's privacy policies. While the appointment of such an officer may make sense to individual institutions in many cases, this is an unusual interference in corporate governance matters.

5. **Civil Money Penalties.** Provides the U.S. Attorney General with the right to bring civil actions for violations of Part V of G-L-B and exact civil money penalties from the institution of not more than $100,000 per violation and from the officers and directors of not more than $10,000 per individual, irrespective of whether such violations are intentional, repeated, or comprise a pattern or practice of illegal activity. Accordingly, although the amount of the civil monetary penalties may be smaller, in some cases, than those permitted under the tiered civil money penalties that bank regulatory agencies may exact under existing law for non-compliance, a showing of intent or a pattern or practice is not relevant to the assessment or the amount of the penalty.

S. 324 ("Social Security Number Privacy Act of 2001")

This is the other G-L-B tightening bill introduced this session by Representative Shelby. The highlights of this bill are as follows:

1. **No sale or purchase of social security numbers.** Financial institutions are prohibited from "selling or purchasing" social security numbers or social security account numbers in a manner that would violate regulations to be promulgated by the federal functional regulators, which the bill mandates occur within six (6) months of its passage. The only guidance the bill gives in connection with the regulations that the regulators are supposed to promulgate is that the same be designed to reasonably assure that social security numbers and social security account numbers will not be used to commit or facilitate fraud, deception, or crime and to prevent "undue risk or bodily, emotional, or financial harm." The bill does not provide for any exceptions in connection with the "sale or purchase" between affiliated entities. Depending upon how such terms are defined (if at all) in the implementing regulations, the exchange of customer lists between affiliated or non-affiliated entities that include social security numbers (for identity verification purposes or otherwise) may be deemed to be a "purchase" and "sale" among them. The bill does not suggest that the regulations permit this activity if consented to, via an "opt-in" by the customer. One would hope that, at a minimum, any implementing regulations would specifically permit financial institutions to report to and obtain credit reports from consumer reporting agencies by using a customer's social security number, so that the proper person is identified.

2. **Social security number is nonpublic personal information.** Specifically includes social security numbers and social security account numbers within the definition of "nonpublic personal information."

H.R. 2720 ("Consumer's Right to Financial Privacy Act")

This bill, introduced by Representative Edward Markey of Massachusetts, is a sweeping "opt-in" bill, requiring each agency with jurisdiction over financial institutions that are governed by Section 504 of G-L-B to promulgate regulations that prohibit such

institutions from making available nonpublic personal information to **any affiliate or other person** that is not an employee or “agent” of the institution unless the consumer has affirmatively consented to the transfer of such information and has not withdrawn his/her consent. It also provides that a financial institution, in complying with the opt-in requirements, may provide an “opt-in” consent form, which would permit a menu of opt-in options; e.g. consenting to the sharing of such information with both affiliates and non-affiliates, consenting separately with respect to affiliates and non-affiliates generally, consenting separately with respect to specified affiliates and non-affiliates; and consenting separately with respect to specified financial and non-financial products or services. Financial services or products could not be denied to a consumer based upon his/her refusal to consent to information sharing. The exceptions to the “opt-in” requirements are the same as the “general exceptions” under existing Section of G-L-B (e.g. disclosures of nonpublic personal information required by law, specifically authorized by the customer, to protect against fraud, to fiduciaries or representatives of the consumer, to rating agencies, to or from consumer reporting agencies in accordance with the Fair Credit Reporting Act, necessary to effectuate a transaction authorized by the consumer, or in connection with a proposed merger or sale of a business unit relating to the consumers of that business unit). The bill also requires that the agencies promulgate regulations that require financial institutions that provide nonpublic personal information to others to provide customers with an opportunity to review and dispute and provide evidence challenging the accuracy of the information provided. The privacy notice requirements would also be amended to include disclosures of the consumer’s right to examine nonpublic personal information to be shared with others and the institution’s practices and policies with respect to permitting such examination rights.

Clearly, tracking the different “opt-in” selections will be a nightmare to administer. It is doubtful that most consumers will take the time to read, much less respond to, opt-in notices. Certainly, financial institutions' recent experience with the general lack of interest of most customers in privacy notices sent prior to July 1, 2001 would indicate that this would be the case. Equally unpleasant is the specter of assuming credit bureau-type responsibilities in connection with permitting consumer review and “correction” of nonpublic personal information. It is unclear how disclosure of nonpublic personal information to “dual employees” would be treated under this bill.

H.R. 2730 (“The National Consumer Privacy Act”)

This bill, introduced by Representative Pete Sessions, a Republican from Dallas, Texas, is the only ray of sunshine for financial institutions in the current crop of proposed G-L-B privacy amendments. Under this bill, a federal pre-emption is created for the privacy standards imposed under sections 502, 503, and 504 of G-L-B, except that state insurance authorities may still prescribe and enforce regulations consistent with those that are prescribed under Section 504(a)(1). It also removes the previous “carve-outs” to federal pre-emption contained in the Fair Credit Reporting Act that would otherwise permit state prohibitions or requirements that are more protective of the consumer. Particularly given the greater use of e-commerce in financial transactions, which knows no state boundaries, uniformity in financial privacy standards should be encouraged.

Non- G-L-B Privacy Bills

H.R. 1478 ("Personal Information Privacy Act of 2001")

This bill, introduced by Representative Gerald D. Kleczka from Wisconsin, would essentially bring the credit reporting industry to its knees, severely impede credit underwriting, and restrict the ability of financial institutions to offer "pre-approved" credit. The following provisions are among the more notable and damaging to lenders and other users of consumer reports:

1. **Prohibits use of social security numbers without individual's affirmative consent.** The bill amends the Social Security Act to prohibit the sale, exchange, or conveyance of any individual's social security number without the express written consent of the individual, given after a notice is provided to the individual that describes all purposes for which the number will be utilized and prohibits any person from using an individual's social security number (or derivations thereof) for purposes of identifying such individual, absent such informed written consent of the individual. The bill provides for civil monetary penalties for violation of this section in the amount of $25,000 for each violation; $500,000 if the violations constitute a "general business practice;" and further provides for a private right of action entitling aggrieved parties to attorney's fees and costs, actual damages, and liquidated damages of $25,000 or, for willful violations, $50,000.

2. **Severely limits the ability to obtain consumer reports for transactions that are not initiated by the individual.** The bill would essentially bring all "pre-approved" credit offers to a screeching halt. It would amend the Fair Credit Reporting Act so that consumer reporting agencies could provide consumer reports requested in connection with credit or insurance transactions that are not initiated by the consumer only if the consumer provided express written authorization for such report. The consumer must be provided with a notice, prior to providing his/her authorization, that discloses what specifically is being authorized and the "potential positive and negative effects" such authorization will have on the consumer. The bill requires that the FTC and the Federal Reserve Board promulgate regulations that govern the form and content of such notice.

3. **Limits on sharing transaction or experience information.** Subject to certain exceptions described below, the bill would further amend the Fair Credit Reporting Act by prohibiting any person "for the purpose of marketing such information" (whatever that means) from transferring to any other person (other than affiliated parties), any experience or transaction information that person has with respect to a consumer, absent the express written consent of the consumer. "Transaction or experience information" is defined as information relating to one or more transactions between the consumer and a person doing business with the consumer, including any part of the transaction, brand name involved, or any

quantity, or category of merchandise involved in any part of the transaction. Accordingly, reporting the consumer's payment history seems to be covered and, absent the consumer's express consent, such information may not be provided. Exceptions include information provided pursuant to valid legal process, information required for licensure or registration by a government agency, information required in connection with real estate transactions, information required in connection with perfecting a security interest in personal property, and information relating to the amount of any transaction or credit extended in connection with a transaction with the consumer.

H.R. 347 ("Consumer Online Privacy and Disclosure Act")

This bill, sponsored by Representative Gene Greene, a Democrat from Houston, Texas, would restrict the ability of an operator of a Web site or online service to collect, use, or disclose personal information and would prohibit attaching or permitting a third party to attach a persistent "cookie" as a means of developing a personal profile of an individual, unless the operator clearly discloses such practices and provides the individual an opportunity to "opt-in" for such attachment. The bill directs the FTC to promulgate regulations relating to the format and content of a disclosure notice regarding the operator's collection and sharing of personal information and requiring a convenient means by which individuals could "opt-out" of the operator's sharing of personal information. Violations of implementing regulations would be a deceptive trade practice under the Federal Trade Commission Act. Enforcement of the regulations would, in connection with banks, be administered by the appropriate bank regulatory agency. Notwithstanding the enforcement authority provisions, the regulations to be enforced would be those to be promulgated by the FTC, thus potentially exposing financial institutions that engage in internet banking to two tiers of regulation and possible multiple privacy disclosure requirements. The bill does not mandate that the FTC promulgate regulations consistent with the G-L-B privacy regulations.

H.R. 237 ("Consumer Internet Privacy Enhancement Act")

Sponsored by Representative Anna G. Eshoo, this bill is similar, but more web-operator friendly than H.R. 347, discussed above. Like H.R. 347, it prohibits website operators from collecting personally identifiable information from a user of the website unless the user is provided a disclosure notice and opportunity to "opt-out" of permitting the use or disclosure of such information. The disclosure notice must provide the identity of the operator of the website and any third party the operator knowingly permits to collect personally identifiable information through the website, as well as the address or telephone number and an email address of the website operator that the user may contact regarding information collection practices. Other requirements of the disclosure are very similar to the privacy notice requirements under G-L-B and implementing regulations. The notice must describe the type of personally identifiable information that may be collected, how such information may be used, sold or otherwise made available to third parties, the consequences of failing to provide personally identifiable information, security procedures that have been undertaken by the operator to protect such

information, and the description by which the user may exercise his or her "opt-out" rights. The good news about the bill is that it provides for federal pre-emption and a "safe harbor" if the website operator complies with self-regulatory guidelines that are approved by the FTC. It also delegates enforcement authority over banking entities to the applicable bank regulatory agency. Civil money penalties could be assessed for violations at $22,000 per violation, subject to a maximum of $500,000 for a related series of violations. Finally, the bill would require the FTC to contract for a study to examine causes for concern about privacy in the information age and strategies to respond to those concerns, resulting in a report and recommendations to Congress.

H.R. 583 ("Privacy Commission Act")

This bill, recently passed out of the House Subcommittee to which it was assigned (the House Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations) is a testament to the corollary of the old saw "If it ain't broke, don't fix it," the corollary being, "If you don't know whether it's broke, media hype seems to suggest it is, and you want to be seen as 'proactive' without sponsoring ill-conceived legislation, create a commission to study it." The bill is sponsored by Representative Asa Hutchinson (with Representative Kevin Brady, a Republican from The Woodlands, Texas, as one of the co-sponsors). While expressly stating that further study by the Commission is not a condition precedent to Congress' enactment of other privacy legislation, the bill would establish the Commission for the Comprehensive Study of Privacy Protection, which would be tasked with studying the collection and distribution of personal information by governmental entities (including the census), existing privacy protection efforts by governmental entities, privacy legislation pending before Congress, the collection and distribution of personal information by persons in the private sector, employer practices with respect to financial and health information of employees, redress for privacy violations currently available to U.S. residents, and the extent to which older and/or disabled individuals are subject to exploitation involving the disclosure or use of their financial information. The Commission would be required to submit a report to Congress and the President within 18 months of the final appointment of all of the Commission's members (which would consist of 17 members -- 2 appointed by the President, 2 by the Senate majority leader, 3 by the Senate minority leader, 4 by the Speaker of the House, 3 by the minority leader of the House, and 1 member to be jointly appointed by the President, the majority leader of the Senate, and the Speaker of the House).

H.R. 2135 ("Consumer Privacy Protection Act")

This bill, sponsored by Representative Tom Sawyer of Ohio, places limitations on the disclosure and collection of "personal information" by an "information recipient," which is defined as "any person who obtains personal information from or about a consumer" through a transaction in interstate or foreign commerce. Affiliates are excluded from the definition. It also establishes more stringent limitations in connection with "sensitive personal information," which, by definition, includes social security numbers and financial information. The information recipient may not disclose to any

other person "personal information" unless, the consumer consents to such disclosure either "tacitly" (which, presumably, means failure to exercise an opt-out) or affirmatively. In the case of "sensitive personal information," the consumer's consent must be affirmative (i.e. "opt-in"). Exceptions to disclosure are similar to the G-L-B general exceptions (e.g., to prevent fraud, as necessary to effectuate a transaction authorized by the consumer, for law enforcement or government regulatory purposes, as required by legal process, to collect a debt). Also excepted are any disclosures that the FTC has determined are consistent with the purposes of the act and in the public interest. In addition, "information recipients" may not require a consumer to provide, as a condition to the transaction, personal information that is not necessary to complete the transaction (social security numbers?). Finally, the "information recipient" must provide to the consumer about whom personal information has been obtained "reasonable access" to that information. Safe harbors are provided to those that implement "practices and procedures" to effectively prevent violations or follow guidelines issued or approved by the FTC. Violations are deemed to be a deceptive or unfair trade practices under the Federal Trade Commission Act. Rulemaking authority is granted to the FTC.

S. 1399 ("Identity Theft Prevention Act of 2001")

Sponsored by Senator Diane Feinstein (D-California), this bill seems to have some bi-partisan support, given the co-sponsorship, which includes Senator Shelby. This bill would amend the Truth in Lending Act by requiring a credit card issuer that receives a request for an additional credit card within thirty (30) days of a change in address notice from the customer to notify the cardholder of the request at both the old and new addresses and provide a means of promptly reporting incorrect address changes. Also, consumer reporting agencies would be required to notify requesters if the address for a consumer provided by a person requesting a consumer report differs from the address in the agency's file. The Fair Credit Reporting Act would be amended by requiring consumer reporting agencies, at the request of a consumer, to include a "fraud alert" in the consumer's files, which notifies users that the consumer does not authorize the extension of credit in the name of the consumer unless the creditor obtains verbal authorization from the consumer at a designated telephone number or the creditor complies with any other method of preauthorization described in the notice. Credit report users that fail to comply with the preauthorization method would be in violation and subject to the existing penalties under TILA. Rulemaking authority is given to the FTC for promulgating regulations requiring consumer reporting agencies to investigate discrepancies between identifying information in the agencies' files and that provided by credit report users. The bill finally requires that electronic credit card receipts truncate the credit card number to no more than the last 5 digits of the credit card account.

H.R. 2036/S.1014 ("Social Security Number Privacy and Identity Theft Prevention Act of 2001")

This bill, sponsored by Representative E. Clay Shaw, Jr. and Senator Jim Bunning, along with many co-sponsors in both houses, heavily restricts the display, sale, and use of social security numbers in both the public and private sectors. Included

among the provisions that apply to the private sector are the following: (1) a prohibition against the purchase, sale, or display of social security numbers. “Display” is defined as the intentional placement of the number or a derivation thereof in a viewable manner on an Internet site that is available to the general public or other manner intended to provide access to such number or derivation by the general public. Exceptions include sales, purchases or displays that are necessary for national security, public health, law enforcement, in emergency situations to protect the health or safety of one or more individuals, research for advancing public knowledge, those made pursuant to the affirmative consent of the holder of the social security number, and as the U. S. Attorney General determines is appropriate. The bill further provides that, except as otherwise required under federal law, any person that refuses to do business with an individual because the individual refuses to provide or consent to another to provide his/her social security number shall be deemed to have committed an unfair or deceptive act in violation of the Federal Trade Commission Act. It also subjects “credit header” information regarding a consumer’s social security number to the requirements of the Fair Credit Reporting Act. Criminal and civil monetary penalties are provided for its violation. Rulemaking authority is granted to the U.S. Attorney General.

Conclusions

The shift to a Democrat-controlled Senate in June dramatically altered the prognosis for the passage of additional consumer privacy legislation. While Senator Gramm of Texas, the former Chairman of the Senate Committee on Banking, Housing and Urban Affairs, had publicly vowed not to permit amendments to G-L-B this session, his successor, Senator Sarbanes, is a privacy advocate who does not have the same “give G-L-B a chance” philosophy. As previously discussed, Senator Gramm's successor, Senator Shelby, is expected to align himself with Senator Sarbanes on privacy matters. If enough pressure builds to pass "something" this session, the “study” bill contained in H.R. 583 would certainly be the most innocuous and may actually result in well-considered, even-handed legislation (an oxymoron to many). Certainly, the federal pre-emption provisions of Rep. Sessions' bill would be a boon to financial institutions as well. Those with a more zealous interest in the topic may wish to suggest that they be considered for nomination to the Commission for the Comprehensive Study of Privacy Protection if H.R. 583 is passed. Certainly banks and other financial institutions have long been entrusted with information that their customers rightfully expect to be kept confidential. As such, the industry’s views on the appropriate balance between maintaining the privacy of customer information, guarding against misuse of that information, and the means of preventing identity theft without unduly interfering with the exchange of information needed to effectively service customers should be heard.