WILMER, CUTLER & PICKERING

e-commerce news

December 20, 1999

Financial Privacy -- New Legislation

Over the past decade, consolidation in the financial services industry has increasingly allowed more of an individual's personal financial information to be collected and used by different companies within one corporate family. You should be aware that recent federal financial services reform legislation has attempted to address the privacy concerns that are raised by the sharing of personal financial information.

On November 12, 1999, Congress enacted the Gramm-Leach-Bliley Financial Services Modernization Act (the "Act"). The Act repealed the Depression-era Glass-Steagall Act, permitting banks, insurance companies and securities firms to affiliate with each other. The Act contains privacy protections for customers of financial institutions (found at Title V, Subtitle A of the Act).

What do the privacy provisions do? Title V places an affirmative obligation on a financial institution to disclose its "privacy policy," *i.e.,* its policies and practices concerning the treatment of non-public personal information about its customers, including what information is shared with affiliates and for what purposes.

Title V also requires a financial institution that intends to share non-public personal information with *nonaffiliated third parties* to provide its customers with the ability to "opt out" of such information sharing with third parties.

No limitations are placed on how a financial institution may share non-public personal information about its customers with its *affiliates.* Current Fair Credit Reporting Act restrictions will still apply. This was one of the most controversial features of Title V in the legislative debate, and the debate is likely to continue in 2000 with efforts in Congress to impose additional controls on interaffiliate data sharing.

What must an institution do in disclosing its privacy policy? A financial institution must clearly and conspicuously disclose its policies and practices concerning the protection of non-public information about present and former customers and disclosure of such information to affiliates and nonaffiliated third parties. In the latter case, the institution must also provide the consumer with information as to how to opt out of such sharing. These disclosures must be made when a new customer relationship is established and at least annually thereafter. The Act does not appear to require that the disclosures be made in a separate document, but that may be a subject of further regulations.

The privacy policy must also include the following information: (1) the categories of persons to whom nonpublic personal information is or may be disclosed; (2) the categories of nonpublic personal information that are collected by the financial institution; and (3) the security measures that the financial institution takes to protect the security and confidentiality of customers' personal information.

How does the opt-out provision operate? A financial institution that wishes to share nonpublic personal information may do so only if it (1) clearly and conspicuously discloses to the customer in writing or electronic form that such information may be disclosed to a third party, (2) gives the customer the opportunity to direct that such information not be disclosed, and (3) explains to the customer how to direct that such information not be disclosed. If all three conditions are met and the consumer does not assert his right to opt out, then the institution may share that customer's information with nonaffiliated third parties.

Which institutions are subject to the Act's privacy provisions? The Act applies to all institutions engaging in financial or other related activities, such as providing financial or economic advisory services or arranging, effecting, or facilitating financial transactions for third parties. Banks, thrifts, mortgage companies, insurers, credit card issuers, securities broker-dealers, and financial advisors are examples of covered service providers. Under this broad definition, it is also possible that a third-party Internet comparison service (such as *mortgage.com*), though not a financial institution itself, could be subject to these privacy provisions because it acts as an intermediary between consumers and traditional financial institutions.

Are all customers protected? The Act only covers "consumers," defined as customers of financial institutions who are individuals. Business customers are not protected by the Act's privacy provisions.

What information is covered? The Act covers all "nonpublic personal information," which includes all personally identifiable financial information provided by a consumer to a financial institution or otherwise obtained by the financial institution (including through transactions). This term is likely to include any information concerning income, buying habits, or insurance claim information, as well as underwriting, application, and account information and any other data collected sources. Federal regulatory agencies and state insurance commissions are expected to clarify the scope of this definition in regulations.

Publicly available information (such as addresses and phone numbers) is generally not subject to the Act's requirements. However, if publicly available information is compiled with any nonpublic personal information (such as personal or household income), then that compilation will become subject to the Act. For example, if a financial institution sorts a lists of its customers' names and addresses by their income, then that sorted list would become nonpublic personal information and would be subject to the Act's privacy provisions.

Are there any exceptions to the opt out? There are numerous exceptions to the opt-out requirement. For example, financial institutions may freely share information with third parties (1) if "necessary to effect, administer or enforce a transaction" requested or authorized by the consumer; (2) in connection with the servicing or processing of a financial product or service requested or authorized by the consumer (e.g., a mortgage); (3) in order to maintain or service the customer's account with the financial institution or with another entity (*e.g.,* as part of a private-label credit card program or other extension of credit on behalf of such entity); (4) with the consent or at the direction of the consumer to protect the confidentiality or security of the financial institution's records relating to the customer; (5) to prevent fraudulent or deceptive practices; (6) to persons holding a beneficial interest relating to the consumer; (7) to persons acting in a fiduciary capacity on behalf of the consumer; (8) to consumer reporting agencies, in accordance with the Fair Credit Reporting Act; or (9) to the extent specifically permitted or required by other provisions of law.

Does the Act place requirements on third parties that receive information from financial institutions? Yes. Once a third party receives nonpublic personal information from a financial institution, it is prohibited from further disclosing such information to any other person that is not affiliated with the third party or the financial institution, unless such disclosure would be lawful if made directly to such other person by the financial institution.

Will the Act prohibit financial institutions from developing joint marketing programs with third parties? Generally no, but it will place restrictions on how joint marketing relationships can be structured. Financial institutions are permitted under the Act to provide nonpublic personal information to a nonaffiliated third party to perform services for, or functions on behalf of, the financial institution, including marketing the financial institution's own products and services or those offered pursuant to joint agreements between two or more financial institutions. However, financial institutions must fully disclose that such information will be provided to third parties and must enter into contractual agreements with the third parties that require the third parties to maintain the confidentiality of such information.

Financial institutions are prohibited from disclosing a customer's account numbers, access numbers, or access codes to third parties (other than consumer reporting agencies) that intend to use the information for telemarketing, direct mail marketing, or marketing through electronic means.

Who will administer and enforce these provisions? The Federal banking agencies, NCUA, the Secretary of the Treasury, the SEC, CFTC, and FTC (after consultation with designated representatives of state insurance authorities) are each directed to prescribe regulations to carry out the purposes of the Act, no later than six months after the date of enactment (*i.e.,* by May 2000). These agencies must consult and coordinate with each other to ensure that all regulations prescribed are, to the extent possible, consistent and comparable. This unprecedented coordination requirement will likely complicate and perhaps extend the rulemaking process.

The privacy requirements in the Act and the implementing regulations will be enforced by the Federal banking agencies, NCUA, SEC, CFTC, FTC, and state insurance authorities, with respect to all persons within their jurisdiction.

Does the Act preempt State law requirements? The Act does not supersede, alter or affect any state statute, regulation, order, or interpretation, except to the extent that such state authority is inconsistent with the Act, and then only to the extent of the inconsistency. State laws that provide greater protection are deemed not to be inconsistent with the Act, and are therefore not preempted. (This absence of complete preemption will likely lead to inconsistent legal obligations under varying state privacy laws.)

Congress took great pains to clarify the relationship between the Act's privacy provision and existing consumer protection laws, noting (a) that nothing in the Act should be construed to modify, limit, or supersede the operation of the Fair Credit Reporting Act, and (b) that no inference should be drawn on the basis of the provisions of the Act regarding whether information is transaction or experience information under the FCRA. As a result, state laws that were preempted under the FCRA, such as those that restrict the sharing of transaction and experience information, will still be preempted.

Does the Act place any requirements on the security of customer records? Yes. The Act establishes Congressional policy that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. To implement this policy, the Act requires the regulatory authorities to establish appropriate standards to: (1) ensure the security and confidentiality of customer records; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

When will these privacy requirements be effective? These requirements will be effective six months after the date the regulations promulgated by each of the federal regulatory authorities are complete. Because the rules must be issued in final form no later than six months after the date of enactment, the requirements should become effective no later than November 12, 2000, unless the regulations themselves provide otherwise.

Is there additional federal privacy legislation pending? Yes. S. 1924, introduced by Sen. Leahy (D-Vt.), would extend the opt-out requirement of the Act to information sharing with affiliates and would require financial institutions to obtain a customer's affirmative "opt-in" before sharing information with third parties. Similarly, H.R. 3320 (introduced by Rep. Markey (D-Mass.)), and S. 1903 (introduced by Sen. Shelby (R-Ala.)) would also impose an opt-in on information sharing with third parties and affiliates. However, it unlikely that action will be taken on any of these bills in the near future.

W. Scott Blackmer
Franca E. Harris

Campaign finance. The Federal Election Commission has issued a Notice of Inquiry (64 Fed. Reg. 60360) asking for comments on the application of campaign finance laws to the use of the Internet in political campaigns. Comments are due January 4, 2000.

Copyright/damages. On December 9, President Clinton signed the *Digital Theft Deterrence and Copyright Damages Act* (P.L. 106-160), a bill to increase statutory damages for copyright infringement in order to deter software piracy. The Act increases the maximum penalty for copyright infringement in a civil case from $100,000 to $150,000 per work.

Domain names/legislation. In the waning days of the session, members of Congress moved to crack down on the practice of "cybersquatting," the unauthorized registration or use of proprietary names in Internet addresses. The Anti-Cybersquatting Consumer Protection Act was included in the conference report for the omnibus spending bill (H.R. 3194). President Clinton signed the bill (P.L. 106-113) on November 29.

Domain names/litigation. On November 29, Judge Claude Hilton of the Federal District Court for the Eastern District of Virginia denied injunctive relief to Volkswagen of America (vw.com). Volkswagen had sought to stop a small Internet service provider, Virtual Works (vw.net) from using its domain name.

Privacy/EU safe harbor. As of the date of this edition of E-Commerce News, the Europeans still have three key concerns about the Clinton Administration's proposal to let companies regulate themselves through a so-called safe harbor plan. According to the Europeans, the United States needs to guarantee that its list of companies complying with the rules will always be accurate and up-to-date; that consumers will get enough choices up front about how the data being collected about them will be used; and that there are adequate mechanisms in place to punish companies that violate the rules. The Clinton Administration wants to let businesses involved in electronic commerce regulate their own privacy practices.

Tax. The Advisory Commission on Electronic Commerce met the week of December 13 in San Francisco to examine a number of different proposals, ranging from a permanent moratorium on Internet taxes to a simplified local taxation scheme that would make it easier for online merchants to collect taxes. The 19-member panel of high-tech executives and government officials has been divided over whether or not to extend state and local sales taxes to Internet purchases. Consensus did not emerge during the two-day meeting, which means that Congress will likely resume consideration of various proposals when they return in January.

E-Commerce News is a publication of WCP's EGroup.