WILMER, CUTLER & PICKERING

Financial Institutions Group Newsletter

MAY 14, 2003

Financial Privacy Developments

Financial privacy is likely to be one of the most important and contentious areas of debate on both the federal and state level this summer and fall. With a few notable exceptions, since the passage of the Gramm-Leach-Bliley Act ("GLB Act") in 1999, federal and state legislatures have done little in the area of financial privacy, focusing their attention instead on issues such as anti-money laundering and terrorism financing.

The imminent sunset of the Fair Credit Reporting Act's ("FCRA") broad affiliate information sharing preemption provision and recent state actions to govern data sharing make congressional action on financial privacy this year a real possibility. The debate on FCRA extension will likely intensify over the summer as the sunset of the existing preemption provision draws nearer. In addition, California, along with several other states, is poised to adopt some form of additional financial privacy protections, either through legislation or referendum, by 2004, further intensifying calls in Washington for a national standard. Finally, the FTC rule requiring financial institutions to safeguard consumer information becomes effective this summer.

Federal Privacy Developments

Fair Credit Reporting Act Preemption

The most critical federal financial privacy legislative initiative this year is the effort to extend the FCRA provision that prohibits states from enacting laws "with respect to the exchange of information among persons affiliated by common ownership or common corporate control." Section 624(b)(2). This prohibition on state action expires on January 1, 2004, after which states would be permitted to enact legislation restricting affiliate information sharing. The financial services industry generally regards the extension of this and other FCRA preemption provisions, including those governing prescreening and furnisher liability[1], as a top priority.

[1] Prescreening refers to a marketing practice in which a financial institution requests a list from a credit bureau of persons meeting certain criteria. The financial institution can then target its product marketing toward best suited individuals. Furnisher liability means liability for those entities who provide consumer information to credit reporting agencies. The FCRA establishes certain responsibilities on data furnishers to ensure that information provided on consumers is accurate and may be relied upon in credit decisions. Section 624 of FCRA preempt state laws relating prescreening and furnisher liability.

House of Representatives. In the House, Financial Services Committee Chair Michael Oxley generally has been sympathetic to industry concerns about overly restrictive privacy measures and may support an extension of the FCRA preemption provisions. Rep. Oxley did not originally favor the consumer privacy protections in the GLB Act and has been reluctant to consider additional privacy protection measures. That said, it is not clear whether Rep. Oxley will be willing to shoulder the burden of getting a bill passed–rather than simply resisting passage of additional consumer protections. Rep. Barney Frank, the ranking Democrat on the Financial Services Committee, has indicated that the two FCRA provisions due to sunset–regarding credit reporting purposes and affiliate data sharing–may be addressed independently. Rep. Frank's approach could lead to reauthorization of preemption provisions relating to prescreening in the nearer term, with the marketing and privacy concerns relating to affiliate data sharing addressed later.

Reps. Pat Tiberi and Ken Lucas have introduced an FCRA extension bill that would remove the sunset to the FCRA's preemption provisions. This bill, H.R. 1766, also would replace section 507 of the GLB Act (which allows states to establish greater privacy protections for non-affiliate data sharing than exists under federal law) with language preempting state and local laws on non-affiliate data sharing. H.R. 1766 was introduced on April 11, 2003, and has been referred to the Financial Services Committee.

Senate. In the Senate, extension of the FCRA preemption provisions may face a greater challenge. New Senate Banking Committee Chairman Richard Shelby and ranking Democrat Paul Sarbanes have both stated that existing law is insufficient to protect consumer financial privacy. Sen. Shelby has indicated that extension of the FCRA preemption may need to be coupled with additional measures to protect consumers and announced that his committee would hold hearings on the matter starting May 15th, when FTC Consumer Protection Bureau Director Howard Beales will be the sole witness.

In March, Sen. Tim Johnson introduced a bill, S. 660, which would simply remove the sunset provision from affiliate information sharing provisions of the FCRA. Unlike the House bill, the Johnson measure does not address the GLB Act standard and would not preempt state laws that restrict non-affiliate data sharing.

Bush Administration. At a hearing held by the House Financial Services Committee on May 8th, Treasury Assistant Secretary for Financial Institutions Wayne Abernathy stated that the Bush Administration is still studying the FCRA preemption issue and developing a position.

In March, Abernathy gave a speech outlining a framework for the FCRA debate. In his speech, Abernathy stated five "basic principles of information security":

- Consumers and financial institutions have a mutual interest in the security of financial information.
- Information sharing has increased the scope financial products available to consumers.
- Identity theft is a serious and growing problem.

- Consumers need to better understand information sharing practices and more easily exercise control over sharing outside the customer relationship.
- Uniform national standards for information sharing are needed.

Abernathy's remarks in March give ammunition to those seeking to extend the FCRA preemption because it was read as an attempt to re-focus the debate from arguing about the merits of consumer privacy to discussing the mutual benefits for financial institutions and their customers in a uniform information-sharing regime.

Despite Abernathy's March speech, some pundits believe that President Bush may be sympathetic to consumers' privacy concerns. In addition, he may generally be reluctant to endorse broad preemption of state law.

State Privacy Developments

California

California State Senator Jackie Speier has re-introduced a financial privacy bill. Senator Speier has been a long-time champion of increased financial privacy for consumers and has campaigned long and hard for stronger California legislation to govern data sharing.

Her new bill, S.B. 1, would regulate the dissemination of consumers' "nonpublic personal information." The Speier bill defines nonpublic personal information as "personally identifiable financial information (1) provided by a consumer to a financial institution, (2) resulting from any transaction with the consumer or any service performed for the consumer, or (3) otherwise obtained by the financial institution."

Financial institutions would be prohibited from disclosing nonpublic personal information (1) to nonaffiliated third parties without prior written consent from the consumer (*i.e.*, opt-in), and (2) to affiliated entities without providing an annual notice to the consumer that he or she may opt-out of data sharing. Data sharing for affinity credit card programs would be permissible, but subject to a consumer opt-out.

Certain types of data sharing would be exempt from the opt-in and opt-out requirements, including those necessary to process a transaction requested or authorized by the consumer, disclosures to law enforcement agencies, sharing in cases of suspected fraud or identity theft, and other listed exceptions.

Consumers would receive an annual privacy notice on a form outlined in the bill or one substantially similar. Violators of the bill would be liable for each consumer's damages from the improper disclosure up to $2,500 per violation and up to an aggregate of $500,000 per occurrence. Those who knowingly and willfully violated the disclosure requirements would be subject to civil penalties of up to $2,500 per violation. The Speier bill would become effective on July 1, 2004.

The Speier bill passed the California Senate by a 23 to 6 vote on March 3rd. The bill now sits in the Assembly, where its prospects are uncertain. Sen. Speier's bill is the product of three years of refinements. Her original financial privacy legislation would have created an across-the-board opt-in standard for data sharing and contained few exceptions to the privacy requirements. That bill failed to gain Senate approval. In the last

term, she modified her bill to an opt-in standard for non-affiliate data sharing and opt-out for affiliate sharing, created many of the current exemptions to the sharing restrictions, and added the annual privacy notice form to the bill. The revised bill passed the Senate, but it failed to gain Assembly approval.

Proponents of the Speier bill believe that it has a greater chance to pass in the Assembly in this term because many past opponents of the legislation either were defeated in November or retired. The Assembly's Banking and Finance Committee will hold a hearing on S.B. 1 on May 19th.

The Speier bill's odds also improved this term because of the prospect of a statewide ballot initiative on financial privacy in 2004. The ballot initiative effort is headed by Chris Larsen, Chair and CEO of E-Loan. Larsen supports the Speier bill but worries the bill may once again fail in the Assembly. Therefore, to help spur the bill towards passage, he has pledged $1 million toward the drafting and promotion of a financial privacy referendum that would appear on the 2004 ballot. The referendum, released on March 12th, would permit financial institutions to share "confidential consumer information" with affiliates and non-affiliates only (a) where express prior approval (opt-in) has been received, (b) to process an approved transaction, (c) to prevent fraud, or (d) for law enforcement purposes. Larsen has stated that he will withdraw the initiative if the Speier bill is enacted.

At the local level, soon after the defeat of the Speier bill in the summer of 2002, county and municipal governments in the San Francisco Bay area began to enact financial privacy ordinances. In late-summer 2002, San Mateo County and Daly City passed financial privacy ordinances. Both ordinances follow the same basic structure as S.B. 1, but use an opt-in standard for both affiliate and non-affiliate data sharing. Both ordinances became effective on January 1, 2003. The effective date created an obvious conflict with the FCRA. A few months later, Contra Costa County passed a financial privacy ordinance using the San Mateo ordinance as a model, except that the effective date was changed to January 1, 2004 in an attempt to avoid FCRA pre-emption.

Wells Fargo and Bank of America filed suit in the Northern District of California to enjoin enforcement of the ordinances, arguing among other things that (a) the San Mateo and Daly City ordinances are preempted by the FCRA, and (b) all three ordinances are improper under the GLB Act, since the power to enact more stringent privacy standards in the federal law is given only to states. The suits have been consolidated, and the local governments have survived summary judgment motions by the banks.

Since fall 2002, four other local California governments have enacted privacy ordinances: Alameda, Marin and Santa Cruz Counties and the City of San Francisco. All four ordinances are substantively similar to the ordinance passed by Contra Costa County. The cities of Berkeley and South San Francisco and Solano County also are considering privacy ordinances.

New Jersey

Two parallel financial privacy bills have been introduced in the New Jersey Assembly and Senate. The bills, A3216 and S2245, are somewhat broader than

California's Speier bill in scope and are less refined by comparison. The New Jersey bills limit the sharing of "confidential consumer information," which includes personally identifiable information:

1) Provided by a consumer to a financial institution;
2) Obtained about the consumer from third parties;
3) About spending habits or any information resulting from transactions with the consumer or the services performed for the consumer;
4) Generated by the consumer's online movements;
5) Concerning the consumer's health; or
6) Otherwise obtained by the financial institution.

This definition is noteworthy because the term appears to cover financial and non-financial information, including health information, obtained by financial institutions.

The New Jersey bills also would prohibit financial institutions from requiring more information from consumers than, "reasonably necessary to perform the transaction, establish the relationship, administer or maintain the business relationship, collect or service a debt, protect against fraud or unauthorized transactions, or comply with applicable law."

Violations of the privacy provisions in the bills would be punishable under the state's fraud laws and subject to fines of up to $10,000 for the first offense and $20,000 for subsequent offenses.

North Dakota

North Dakota has been the most active state in the nation in the area of financial privacy in the last year. Dating back to 1985, North Dakota passed a law requiring financial institutions to obtain customer consent before sharing confidential consumer information with non-affiliated third parties. In 2000, the North Dakota Department of Banking and Financial Institutions petitioned the FTC on whether the GLB Act preempted the 1985 law. The FTC responded in June 2001 that, because the state law was not inconsistent with federal law, it was not affected.

In early 2001, the North Dakota legislature passed a law that changed the 1985 standards for disclosure of confidential customer information to non-affiliated third parties to opt-out, as under the GLB Act. A strong public reaction against the weakening of the data sharing provisions resulted in a ballot initiative in June 2002. Voters were asked whether the state should retain the newly enacted opt-out standard for non-affiliate data sharing or return to the prior opt-in standard. On June 11th, 73% of North Dakota voters favored a return to the opt-in standard.

On April 7, 2003, a new law was enacted in the state. The new law both limits the scope of the state's opt-in standard and makes clear that the standard will apply to financial institutions' joint marketing arrangements. The opt-in requirements are limited to residents or domiciliaries of North Dakota

in their relationships with financial institutions having a physical presence in the state.

Maine

A pending bill in the Maine legislature would place a financial privacy referendum on the November ballot. Like the 2002 referendum in North Dakota, voters would be asked whether the state should have an opt-in or opt-out standard for non-affiliate financial data sharing. The bill, LD 661, is currently under consideration in both houses of the legislature.

Preemption and Enforcementof State Privacy Enactments

Even if individual states continue to enact privacy measures, national banks and thrifts (and their federal regulators) may assert that, notwithstanding the GLB Act's allowance for state regulation of non-affiliate data sharing, state privacy measures are either preempted or enforceable only by the OCC or OTS. In a recent string of issuances and court briefs, the OCC and OTS have asserted that many state laws and regulations, particularly in the area of consumer protection, are preempted to the extent these measures apply to national banks and federal thrifts because the two agencies are given exclusive regulatory authority over such federally chartered institutions. Even when such state laws and regulations are not preempted, the agencies have argued that the state requirements may only be enforced by the federal regulator.

FTC Safeguards Rule

The FTC's Final Rule on Standards for Safeguarding Customer Information ("Safeguards Rule") becomes effective on May 23, 2003. The Safeguards Rule was published on May 23, 2002 (67 Fed. Reg. 36,484) and is designed to meet the FTC's requirements under Title V of the GLB Act, which mandated that certain federal regulatory agencies develop standards for the protection of sensitive information for financial institutions. Under the rule, financial institutions are required to develop, implement, and maintain "reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of consumer information."

The Safeguards Rule is applicable to financial institutions regulated by the FTC, including check-cashing businesses, data processors, mortgage bankers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, courier services, and retailers that issue credit cards to consumers. The FTC Safeguards Rule mirrors rules issued by the federal banking regulatory agencies and the National Credit Union Administration under Title V of the GLB Act.

The Safeguards Rule defines "customer information" as "any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of [a financial institution] or [its] affiliate." In the preamble to the final rule, the FTC stated that where information is disclosed to other financial institutions, such as credit reporting agencies and ATM operators, those institutions will be covered by the rule.

The rule states that the safeguards must be "appropriate to the size and complex-

ity of the entity, the nature and scope of its activities, and the sensitivity of any consumer information at issue." Although the Safeguards Rule is designed to be flexible, certain steps are required for all covered financial institutions:

1) At least one employee must be designated to coordinate the institution's information security program.

2) The institution must "identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks."

3) The institution is required to "design and implement information safeguards to control the risks [identified] through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures."

4) All service providers must be overseen to ensure that the service providers are capable of maintaining appropriate safeguards for customer information.

5) Each financial institution must "evaluate and adjust [its] information security program in light of any materials changes to [its] business that may affect [its] safeguards."

Provisions of the Safeguards Rule affecting financial institutions' contracts with nonaffiliated third-party service providers will not be effective until May 23, 2004, if such contracts were in place prior to April 23, 2002.

Philip D. Anker	+1 (202) 663-6613	Franca Harris Gutierrez	+1(202) 663-6557	James H. Mann	+1 (212) 230-8843
Gregory A. Baer	+1 (202) 663-6859	Wilhelm Hartung	+44 (20) 7872-1075	David Medine	+1 (202) 663-6220
Ursula Bass	+1 (202) 663-6203	Stephen R. Heifetz	+1 (202) 663-6558	Eric Mogilnicki	+1 (202) 663-6410
Clare D. Bracewell	+1 (202) 663-6944	Michael Hershaft	+1 (202) 663-6427	Matthew P. Previn	+1 (212) 230-8878
Russell J. Bruemmer	+1 (202) 663-6804	Kirk Jensen	+1 (202) 663-6182	Jessica E. Singer	+1 (202) 663-6133
J. Beckwith Burr	+1 (202) 663-6695	Satish M. Kini	+1 (202) 663-6482	Daniel H. Squire	+1 (202) 663-6060
David M. Capps	+44 (20) 7872-1080	Michael D. Leffel	+1 (202) 663-6784	Natacha Steimer	+1 (202) 663-6534
Ricardo R. Delfin	+1 (202) 663-6912	Christopher R. Lipsett	+1 (212) 230-8880	Todd Stern	+1 (202) 663-6940
Simon Firth	+44 (20) 7872-1036	David A. Luigs	+1 (202) 663-6451	Manley Williams	+1 (202) 663-6595
		Martin E. Lybecker	+1 (202) 663-6240		