Western Massachusetts Law Tribune, March 27, 2002 at 15

Privacy Notices: Designed to Fail

By Eric J. Gouvin

In the past year you have received a flurry of letters from your bank, insurance company, mutual fund firm, pension plan, credit card issuer, and other providers of financial services telling you about their "privacy policies." You got those notices because they are required by a regulation promulgated jointly by the federal banking regulators last year which requires, among other things, that financial institutions:

– provide customers with a notice of the institution's privacy policies and practices; and

– provide customers with the opportunity to opt out or bar the institution from sharing customer information with unaffiliated third parties unless the institution has a reasonable basis to believe that the information is lawfully publicly available from certain public sources.

Maybe you do not remember those notices. They looked a lot like junk mail. You may have thrown them away by accident. If you missed those letters the first time, just wait a little while because covered financial institutions are required to provide those privacy notices to their customer once every 12 months. Next time they arrive, don't throw them away. They give you a mechanism to claim some control over how your personal information will be used. How effective they have been in that role is a story of its own.

The Gramm-Leach-Bliley Act provided long-overdue reform to an industry that was artificially segmented into increasingly anachronistic categories. The bright side of the legislation was that it finally allowed banks, insurers, securities firms, and mutual funds to associate with much less folderol than was previously required. The dark side of the legislation was that these new combined firms could create extraordinarily detailed profiles of their customers simply by assembling data about their income, assets, debts, payment histories, health, spending habits, and other sensitive information. In the information age, this data is a valuable commodity. The possibilities for invasion of privacy were not lost on consumer protection groups who urged Congress to make financial service providers obtain their customers' express consent before selling the personal information. Under this approach, customers would have had to "opt-in" before their data could be sold. The financial services industry hated that idea. They said it would cost too much to administer. The real problem, however, was that they feared too few customers would actually acquiesce to the sale of the information.

Instead, the financial services providers were successful in getting exactly the opposite approach built into the legislation. Rather than obtaining customer permission to sell the data, the companies' right to sell that data would be presumed and customers who objected would be required to "opt-out" by signing a form denying permission to sell

the information. The basic idea was that consumers could make their own decisions after full disclosure.

With the first wave of disclosures behind us, only 1 in every 20 or so consumers have bothered to send back their opt out forms. That could mean that the overwhelming majority of Americans embrace the prospect of receiving junk mail, dinnertime telemarketing calls, and email spam trying to sell them all manner of things that their personal data profile suggests they might be interested in. Of course, that's only one possible reason, and not a very plausible one at that. The more likely reason for the low response rate is that the "privacy notices" have been designed to be thrown away unread, or, if read, to mislead.

The typical privacy notice has all the readability of a software license but without the compelling storyline. It seems obvious that most consumers do not have the stomach to plow through those notices. They are full of technical jargon and are set in small type. When a hardy soul does get through the notice they typically will find that "full disclosure" of the pros and cons of opting out is weighted much more heavily on the cons than the pros. These notices suggest that opting out of the information sharing would be a very costly move – one that could deprive the customer of valuable money saving opportunities.

The way the notices have been handled in the first wave of compliance has been an elaborate sham designed more to protect the financial institutions that are selling the information than the consumers whose information is being sold. The notices cannot protect consumers unless they fully and fairly disclose what the financial companies have in their possession, what they intend to do with it, and what the customer needs to do to opt out. The disclosure cannot be full and fair unless it is also readable.

Under the law the regulators are required to review the notices this year and suggest improvements. One obvious improvement would be to require the forms be in "plain English" – something we require of lots of other consumer-related documents. Imagine a privacy notice that says:

> We have learned a lot of information about you and your household through our account relationships with you. For example, we know your annual household income, your major assets, your investments, where you work, and your Social Security number. We sell this data to other companies that want to market their products to you. Do you want us to continue doing this? Yes or no.

Further imagine this notice on the back of a pre-addressed post paid postcard and we could have the beginning of a privacy notice that would really allow customers to tell their financial institutions how they feel about sharing of financial information. Until that time, people likely will continue to allow their personal information to be used in ways they don't like because they don't really know they can do anything about it.