

Financial Privacy Please: The Gramm-Leach-Bliley Act

The privacy of your personal financial information held by companies with which you do business is not just a matter of an increase in junk mail solicitations from such companies. The less private and secure your personal financial information is, the more likely you are to be a victim of identity theft.

Which appears more difficult to remember: the Gramm-Leach-Bliley Act or the Financial Services Modernization Act? Whatever you call it, when it comes to protecting the privacy of consumers, the law is a confusing amalgam of guidelines that help the financial industries much more than they do consumers. Although trumpeted by some politicians as a law that helps to protect consumers' privacy, the Gramm-Leach-Bliley Act, a federal law, does little to achieve that end. Rather, its intention all along was to legalize the ability of banks, insurance companies, and investment companies to merge or more effectively do business together.

The four main parts of the Gramm-Leach-Bliley Act that directly apply to consumers deal with disclosure of companies' privacy policies, opting out of providing information to nonaffiliated third parties, nondisclosure of personal account information, and setting standards to protect security and confidentiality of consumers' private information.

You might remember receiving the first annual disclosure of the privacy policies of the financial companies with which you do business, such as banks, insurance companies, credit card companies, and brokerage companies. Or then again, maybe you don't because many of us just looked at these disclosures and considered them to be just more pieces of junk mail from our banks or credit card companies. Few of us took a moment to actually try to read them, and those who did often found them indecipherable. In any event, just like the swallows returning to Capistrano or your relatives returning for Thanksgiving, these disclosures are required by law to be sent to you every year.

The privacy disclosure is required by law to be a clear, conspicuous, and accurate statement of the particular company's information-sharing and privacy policy. Unfortunately, the disclosures are generally unclear and inconspicuous. They are an all-too-accurate statement of the consumer's lack of control over his or her personal financial information. The disclosure must describe the particular institution's policy in regard to the personal "experience and transaction information" that it collects, as well as the company's policy for disclosure of nonpublic personal information to both third parties and companies affiliated with the particular institution. Experience and transaction information consists of extraordinarily personal information, such as your bank account number, how much money you have in your bank account, what you have purchased with your credit cards, how much life insurance you have, and your Social Security number. It even includes information that you might have provided to the company without even knowing that you had done so through the placement of "cookies" in your computer by a company with which you have done business online. In the world of computers, cookies are pieces of text that permit a website to store information on your computer's hard drive and then retrieve it later without your being aware that the process is occurring. Through the use of cookies, a company operating a website you visit is able to trace everywhere you have gone on the Internet. If you want to see what particular cookies are on your computer, you can go to C:\Windows\Cookies. This applies to most PCs. You also can delete cookies from your computer if you want to.

Prior to the enactment of the Gramm-Leach-Bliley Act and unbeknown to many consumers, financial institutions such as banks and brokerage houses had been sharing consumers' personal experience and transaction information not just with companies with which they already were affiliated in some fashion, but with telemarketers as well. The Gramm-Leach-Bliley Act still permits these financial institutions to share this sensitive information with affiliated companies, even if you request that they not do so. An affiliated company is one that is either owned or controlled by the company with which you do business. The Gramm-Leach-Bliley Act also permits financial institutions to share your personal information with other companies that have joint marketing agreements with the company with which you are doing business. An example of a joint marketing agreement is a program by which your bank agrees to endorse or offer insurance policies issued by another company. As a bone thrown to consumers, the law now prohibits the sharing of this information with telemarketers. By the way, if you have not yet signed up for the National Do Not Call List to stop annoying calls from telemarketers, you might want to do so. You can register for the list, which is operated by the Federal Trade Commission, by going to their website at www.donotcall.gov or by calling them at 1-888-382-1222. The process is quick, easy, and rewarding.

Perhaps most important to consumers, the disclosure must also provide consumers with a way to exercise the right to opt out of the sharing of nonpublic personal information with nonaffiliated companies.

Some sharing of information is allowed regardless of whether you choose to opt out, and in some instances this rule makes sense. Private information may be shared with third parties necessary to service your account, with credit-reporting agencies, and to comply with investigations by state and federal regulatory agencies. In other instances, your information is shared with companies because they are affiliated in some way with the company with which you are doing business, regardless of whether you have chosen to opt out of information sharing. These situations exemplify the consumer's weakness and the strength of the lobbying of the financial industries.

Rubbing salt in the wounds, some financial institution executives have even had the gall to suggest that the reason so few people have chosen to opt out of information sharing is that consumers appreciate the "benefits" of having their personal information shared with other companies. Those so-called "benefits" include having your privacy compromised and becoming more susceptible to identity theft. The truth of the matter is that the reason relatively few people have exercised their limited power to opt out of information sharing is that either they did not understand the disclosure form sent to them or they just threw it away, considering it to be merely junk mail.

One of the better provisions of the Gramm-Leach-Bliley Act is its prohibition from sharing account numbers or other identifying numbers with nonaffiliated telemarketers, direct mail marketers, or e-mail marketers.

Safeguard Rules

In an attempt to provide for better security and privacy of personal information, the Gramm-Leach-Bliley Act also requires financial institutions to set up new standards to protect the confidentiality and security of consumers' personal information to help aid in the battle against identity theft and fraud. Under the safeguard rules provisions of the Gramm-Leach-Bliley Act, every company that is "significantly engaged" in providing financial services or products to consumers must develop a written plan to secure the privacy of personal customer information. This section of the law applies not only to banks, brokerage houses, and insurance companies, but also to credit-reporting agencies, mortgage brokers, real estate appraisers, tax preparers, and even ordinary retailers that issue their own store credit cards. Specifically, the plan must note and assess the risks to consumers' personal information throughout each aspect of the company's activities. The company's present security systems must be evaluated and regularly updated to respond to changes inside and outside of the company.

Due to the fact that a company's employees with access to sensitive, personal information are an always-present possible source of identity theft, companies are urged to pay particular attention to the references of employees being hired who will have access to such information. A proper safeguard plan also provides rules for locking areas and file cabinets where written records are stored, establishing and regularly changing computer passwords, and encrypting personal consumer information whenever possible.

Pretexting

The Gramm-Leach-Bliley Act also makes "pretexting" illegal. Pretexting is the term for the fraudulent obtaining of consumers' personal financial information by the use of false pretenses. Pretexting comes in many variations, such as someone pretending to be taking a survey or pretending through a website to be a financial institution with which you do business requesting confirmation of personal financial information, which when provided starts you on the road to identity theft.

Opt Out, Opt In

In the movie *The Karate Kid*, Mr. Miyagi's mantra was "Wax on, wax off." This was the mundane way that he taught young Daniel to protect himself. If you don't know what I'm talking about, go rent the video. You will enjoy it. In the world of the security of your personal financial information, the mantra is "Opt in, opt out." When the comprehensive Financial Services Modernization Act was being debated in Congress, the issue of whether consumers should be required to affirmatively opt out of having their personal information shared or whether they should be required to opt in if they wanted their personal information shared was hotly debated. Ultimately, the final score on this matter was Big Bad Financial Institutions 2 (I guess you know where I stand), Consumers 0. Not only did Congress drastically limit the circumstances in which we could prevent the sharing of our personal information, but it also, in the ultimate caving-in to the Big Bad Financial Institutions, required us to take affirmative steps to prevent the sharing of our personal information. So much for a government of the people, by the people, and for the people. But let's look at this dirty glass as half-full instead of half-empty and consider how you can opt out of information sharing. If you have neglected to take this step and opt out in order to protect yourself from identity theft and reduce the amount of annoying marketing junk mail you receive, you can still exercise your limited right to opt out of information sharing by sending a letter to the various institutions with which you deal, requesting that they not share your personal information. A copy of a form letter to opt out is included in the bonus material on www.ftpress.com/identitytheft. Generally, the disclosure that you receive from the

financial companies with which you do business allows you to exercise your limited right to opt out of information sharing through a letter or form sent back to them, by way of a toll-free telephone call, or through the Internet, if that is how you normally do business with that particular company.

Good Guys in Congress

There are some good guys from both parties in Congress trying to protect consumers' rights, and although they did not win the war when it came to the Gramm-Leach-Bliley Act, they did win some battles. Democratic Senator Paul Sarbanes was able to add an amendment to the bill while it was being considered that at least allowed the individual states to enact their own stronger laws to protect the privacy of personal information held by financial institutions. North Dakota passed such a law, which served as a model to other states so inclined to provide greater privacy protection to their citizens. In 2009, the United States Supreme Court upheld California's financial privacy law, which is much stronger than Gramm-Leach-Bliley. The California financial privacy law limits the sale of personal information by financial firms to affiliates and, quite different from Gramm-Leach-Bliley, requires consumers to opt in for information to be shared rather than requiring them to opt out of automatic information sharing as Gramm-Leach-Bliley provides.

The Bottom Line

The plain, hard fact is that the more places that have personal information about you, the more risk of identity theft you face. Much identity theft originates with criminal employees of legitimate companies stealing information to which they have ready access. And it just stands to reason that the more places your information is shared, the more places exist for identity thieves to find it. Whether these identity thieves are company employees or hackers from outside the company makes little difference to you. The result is the same. Your identity is stolen. But you can reduce your chances of becoming the victim of identity theft by merely "opting out," telling the Big Bad Financial Institutions that at least to the fullest extent that the law permits, you do not want them to share your information with anyone. The Big Bad Financial Institutions that have your information depend on all of us being too lazy to read the interminably boring, small-printed notices they send us that tell us about our rights to opt out of information sharing. They do not want us to be the victims of identity theft, but they do want to use and disseminate this information for business and marketing purposes. And when it comes to protecting our privacy or increasing their business, which do you think is their priority? So opt out. Opt out now. Okay, you can wait until you finish the book, but then opt out; go directly to opt out. Do not pass go. Do not collect \$200. Go directly to opt out.