

## So You Think You Know Privacy? Let's Talk . . .

*By Patricia E.M. Covington\**

If you thought that privacy law was limited to Gramm-Leach Bliley, you're about to get a reality check. GLB is the veritable tip of the iceberg. Just ignore the fact that icebergs are shrinking every year - because, quite to the contrary, privacy-related laws are increasing with every year that passes. When you think about the subject of consumer information privacy, it's best to step back and take a "panoramic" look at the landscape.

Understanding the complete picture is not only necessary for compliance, it's critical for not overspending when complying. It also promotes a more robust and efficient program that is more likely to achieve the laws' intended goals.

I'll start with a description of the lay of the land. Privacy-related laws can be broken down into three types: (1) don't share my information and protect what you've got (confidentiality and security related); (2) respect my privacy and don't contact me when I've said I don't want to be bothered (marketing related); and (3) don't steal from me (identity theft protection related).

The granddaddy of all privacy laws is the Fair Credit Reporting Act. How is it a privacy law, you ask? Well, for one, it says that companies that collect data about a person's credit (*i.e.* credit reporting agencies) can't willy nilly share that data (*i.e.* consumer reports) with others. This information may be shared only with persons who have a valid need under the law (*i.e.* permissible purpose). Also, persons who do obtain these credit reports can't indiscriminately share the information. If they do so, they might find themselves deemed a consumer reporting agency. And, if you have an affiliate, you can only share credit report information if you provide the consumer with an opportunity to opt out of that sharing. Finally, it contains the rules on making prescreened offers. Consumers have the right to have their names removed from the prescreening lists. So, as you can see, the FCRA has at least two types of (and really, three - we'll talk about the third one in a bit) privacy-related laws - the "don't share my information" and the "respect my privacy by not contacting me" types.

The most well known privacy law is GLB. There are two components, the Privacy Rule and the Safeguards Rule. The Privacy Rule requires companies to tell consumers what information they collect, how they share it and with whom they share it. The Safeguards Rule requires that companies actually do what they say they're doing in privacy policies. Companies must protect consumer information against unauthorized access and anticipated security and integrity threats.

Now back to FCRA. The Fair and Accurate Credit Transactions Act amended FCRA. FACTA added quite a few privacy-related laws, including: the truncation of all but the last four digits of the Social Security Number on receipts, the prohibition of selling debts that are the result of identity theft, the right of identity theft victims to obtain copies of transaction documents used in connection with identity theft, fraud alerts (initial, extended and active duty), the Disposal Rule, the Red Flags Rule and the Address Discrepancy Rule. The requirements to truncate Social Security Numbers, to not sell debts that are the result of identity theft, and to give identity theft victims copies of transaction documents used in connection with identity theft are pretty self-evident. These all are "don't steal from me" type of laws.

The Disposal Rule requires that companies properly dispose of credit reports (or any compilation of credit reports). This, of course, is to prevent the unauthorized access and use of them. Fraud alerts give consumers the right to put an alert on their credit files. If an alert is on a file, a creditor is required to verify the consumer's identity. Initial alerts are placed when someone thinks she may become the victim of identity theft (*e.g.* I lost my wallet). Extended alerts are placed when the consumer has already been victimized by an identity thief. And active duty alerts are for

individuals in the armed services and on the road. The goal of alerts is to give the creditor notice that identity theft is a real risk and it better make sure it's dealing with the *real* person and not a thief.

The Red Flag and Address Discrepancy Rules are the newest kids on the block. The Red Flag Rule requires that companies put in place an "Identity Theft Protection Program." This program must include reasonable policies and procedures to address the risks of identity theft and the safety and soundness of the dealer's business. The Address Discrepancy Rule requires that creditors confirm the identity of consumers when the address provided by the consumer is different than what is listed in the credit file. Again, all of these requirements are the "don't steal from me" kind.

FACTA does have a "don't contact me" component - it's the amendment to the Prescreening and Affiliate Sharing Rules. In addition to other requirements, the Prescreening Rule requires that the right to opt out from prescreening lists be clearly and conspicuously disclosed. The Affiliate Sharing Rule limits how information shared with affiliates can actually be used when it comes to marketing.

Other "don't contact me" laws are the federal Do Not Call laws (FTC's Telemarketing Rule and FCC's Telephone Consumer Protection Act), CAN SPAM, and Do Not Fax laws. These laws contain specific requirements regarding how and when you may contact consumers via phone, email and fax.

The states then have their own privacy-related laws. Some are mini-versions of the federal ones, and some are completely new, such as security breach notice laws. These require that consumers be notified of security breaches involving their sensitive information. The company who owns the information breached must provide the notice. In almost every case (except North Carolina and Hawaii), the security breach applies to computerized data. North Carolina and Hawaii apply it to all data, no matter the format. Thirty-four states have this type of law on the books.

The states also have Social Security Number limitation laws. These laws limit how Social Security Numbers can be used, published, and transmitted. Some states prohibit Social Security Numbers from being printed on any materials that are mailed. There are some exceptions, like for applications. At least thirteen states have this type of law.

Then there are disposal type laws. These laws are very similar to the FACTA Disposal Rule, except they apply to all records and documents that contain sensitive consumer information. They generally require that a company have reasonable policies and procedures to dispose of sensitive customer information (to prevent unauthorized acquisition and use). There are at least 16 states with this type of law.

Many states have their own safeguarding laws. These laws are similar to GLB in that companies must implement a safeguarding program to protect the confidentiality, security and integrity of consumer information. Approximately nine states have this law.

Lastly (at least for now), there are credit or security freeze laws. These laws don't require dealers to *do* anything, but instead give consumers the right to lock down their credit reports. If a security freeze is in place, creditors are "frozen out" of the credit report and can't gain access. There are usually exceptions for current creditors and law enforcement. To gain access, the consumer has to request that the credit file be "thawed." This is of interest to dealers because it inhibits the credit process and the ability to get the customer in a car and off the market.

Why is it important to know about all these laws and how they are interrelated? Well, first, it enables you to build a cohesive program -something that will comply with all the requirements and actually function better. For example, the effort you invested in to comply with the FACTA Disposal Rule will certainly help you with the state's disposal law. That effort also helps you comply with the GLB Safeguards Plan, but only if you have taken the time to document it in writing and add it to your Plan.

Many of your compliance efforts can do double duty. But, first, you need a clear picture of what you're required to do and where you're going. This will enable you to use your resources more efficiently. You won't duplicate efforts, and you'll build on existing programs when creating new ones (e.g. Red Flag Rule). In the end, you'll wind up with a stronger overall program. To top it off, you may actually prevent identity theft and fraud, which saves you even more money.

Copyright © 2007 CounselorLibrary.com LLC. All rights reserved. This article appeared in **Spot Delivery**®. Reprinted with express permission from CounselorLibrary.com.

\* **Patricia E.M. Covington** is a partner in the Maryland office of **Hudson Cook, LLP**. She can be reached at 410.865.5409 or by e-mail at [pcovington@hudco.com](mailto:pcovington@hudco.com).