

Size Doesn't Matter

By: Gil Van Over

Did you know...size does not matter? At least to the FTC it doesn't.

The Privacy and Safeguards Rules arose from the Gramm Leach Bliley Act (GLBA) requiring financial institutions (read auto dealers) to protect consumers' personal, non-public information. The Privacy Rule has been in effect since July 1, 2001 and requires dealers to provide customers with a copy of the dealers' privacy notice.

Part of the privacy notice should read "We maintain physical, electronic and procedural safeguards that comply with federal regulations to guard your nonpublic personal information." The Safeguards Rule is that federal regulation.

As of May 23, 2003, dealers were required to comply with the Safeguards Rule. The five key provisions of the Safeguards Rule are:

1. Designate a Program Coordinator
2. Conduct a risk assessment
3. Design and implement safeguards to control the risks you identify
4. Oversee your service providers
5. Periodically audit, evaluate and adjust your program

Now comes the tricky part. The FTC has already sent inquiries to at least three dealers asking for a lengthy list of documentation to confirm that the dealer has a Safeguards Program in place. These inquiries appear to be randomly selected and do not take size into account. The letter I saw from a single point dealer asked him to provide:

- A description of the dealer's corporate structure
- A list of each type of information from or about its customers that is collected or maintained by the dealer and a copy of each form used to collect or maintain the information
- A copy of the dealer's written information security program and to certify the time period during which the program was written and implemented.
- Documentation of the security risks identified during the risk assessment process and how the dealer's plan addresses each of these risks.
- The name and title of the employee responsible for coordinating the information security program and all documents that provide the employee with direction in coordinating the program.
- Documentation of any testing, monitoring or evaluations put into place.
- Identify the name, address and phone number of each service provider that has access to the dealer's customer information and copies of each service provider's contract that requires them to implement and maintain security safeguards.
- Copies of the dealer's privacy notice, privacy policy and opt out notices provided to consumers.

Are you prepared to answer such an inquiry? The potential penalty (payable to the FTC) is \$11,000 per day for non-compliance. How many days has it been since May 23, 2003?

Gil Van Over is President of gvo3 Consulting, LLC (www.gvo3consulting.com). He assists auto dealers to design and implement a litigation defense strategy and can be reached at (312) 961-9065 or gil@gvo3consulting.com.