

October 2005

PRIVACY

Make It an Organizational Priority

You can't pick up a newspaper or turn on the news without hearing about another breach of private consumer information. As a result, consumer identity theft fears have escalated and regulators are reacting. Currently, regulations are being drafted to hold companies more accountable for failing to secure the data they collect and store about their employees and customers.

As is typical in the area of consumer protection, the regulatory charge is being led on the state level. A state-by-state regulatory structure has emerged since 2003, when California passed one of the first laws requiring notification of data theft or loss. Since 2003, 17 states have enacted similar laws, including Arkansas, Georgia, Montana, North Dakota and Washington. Ohio has not yet enacted a law; however, On August 2, 2005, the Ohio House passed [House Bill 104](#) and companion data breach legislation is pending in the Senate.

Congress has been active in this area as well. Under one of several recent Congressional proposals, companies that experience loss or theft of data on more than 1,000 people would be required to notify the affected persons or face fines of up to \$11 million per incident. Additionally, the bill would bar businesses, schools and companies from using Social Security numbers on identification cards and other forms of identification. S. 1408, 109th Cong. (2005).

Whether it is state or federal legislation, businesses that collect and maintain personal information can be assured that in the near future a government entity will be placing greater security and privacy requirements on procedures associated with the collection and storage of personal information. State and federal regulations in this area generally share three common points. They require companies to:

- notify consumers nationwide if certain types of breaches occur
- set minimum standards for security
- impose stiff civil and/or criminal penalties for violations

In the meantime, protect your company by reviewing your privacy policies and ensuring you have adequate security procedures in place. If you think your dealership's privacy policies and procedures may not be up to snuff, here are some suggestions:

- **Data Security** – develop policies and procedures and conduct training regarding data security to include:
 - Requiring employees to log off of unattended computers.
 - Implementing a password protocol and requiring that passwords not be shared or disclosed to unauthorized individuals.
 - Installing and routinely running anti-virus software and updating your operating system on a regular basis with the latest security patches, updates and drivers. This will ensure your computer is up-to-date and will help prevent against viruses and other security breaches.
 - Maintaining the confidentiality of all data, keeping in mind the privacy of all individuals.
- **Document Destruction** – dispose of confidential information in a secure manner.
- **Facility Security** – ensure that no unauthorized individuals have access to facilities.
- **Outsourcing/Subcontractors** – inquire about their security protocols and if they meet standards, insist on strict compliance.
- **Employee hiring** – conduct background screenings and have employees sign privacy statements.

Most importantly, hire a compliance officer or assign compliance officer duties to a current employee. Stay current on privacy regulations and revise and adopt your privacy policies and procedures accordingly.