

FINANCE & INSURANCE: Thwarting Thieves

FTC compels dealerships to guard customer information from being stolen

Harry Stoffer

Automotive News

March 31, 2003

Step by step

Here's what every financial institution, including each auto dealership, is supposed to do to safeguard customer personal information.

Name a person or persons to coordinate the safeguard program.

Identify the risks to customer information in every part of the business and evaluate methods for controlling those risks. Give special attention to:

- A. Employee training and management
- B. Information systems, including processing, storage, transmission and disposal
- C. Detection and prevention of and responses to attacks or intrusions on information systems

Design and take actions to control risks

Require service providers by contract to safeguard customer information

Test, monitor and update the program as operations change

Sources: FTC, NADA

The same law that brought us those pesky privacy fliers in all our banking, insurance and brokerage statements is creating a headache for the nation's dealerships.

Virtually every dealership in the United States must prepare a written plan explaining how it will protect the personal financial information of customers. The plan must take effect by May 23.

The goal is to guard against identity theft and other misuse of the information.

Federal officials estimate that about 750,000 cases of identity theft occur each year. Typically, someone uses another person's Social Security number, credit card number or other personal information to open accounts or charge purchases in the victim's name. It can take years to undo the damage, officials say.

Still, the new requirement for dealerships includes some tricky provisions. One is that each dealership must vouch for the security of information handed to companies that provide services.

The various provisions, collectively known as the Information Safeguarding Rule, may be news to many who are supposed to comply in less than two months.

"Candidly, that hasn't been communicated very well," says Wayne Williams, president of Williams AutoWorld, which has multifranchise dealerships in Okemos and Lansing, Mich. Williams is a former chairman of the American International Automobile Dealers Association.

Fighting crime

The Federal Trade Commission, the agency responsible for writing and enforcing the rule, says confidently that it will prevent crime and that it makes good business sense.

"When you show customers that you care about the security of their personal information, you increase their level of confidence in your institution," the FTC says in a notice to businesses.

But there also is considerable uncertainty at the FTC about what the rule means in the real world.

Laura Berger, an attorney in the FTC's division of financial practices, says the agency can't even estimate how many businesses will have to develop the security plans.

And enforcement will be through the FTC's usual means, she says. In most cases, that means consumers will have to complain that a business is out of compliance before the agency will know where to look for a violation.

The FTC is not a criminal law enforcement agency, but it can impose civil fines, get court orders and negotiate consent decrees - all of which can be costly and damaging to a dealership's reputation.

Also unsettling to those who must comply is this: There is no objective standard for what is an adequate plan. But it does appear that a plan must deal with all aspects of security, including the people who handle records, a business' computers and the networks to which they are linked, as well as the locks on the doors and cabinets where records are stored.

Security is a cultural process, Berger says.

The number of security plans that have to be developed hasn't been calculated because the rule applies to all financial institutions - broadly defined as any business that is significantly engaged in providing financial products and services to customers. Diverse

examples include check-cashing stores, mortgage brokers, property appraisers, retailers that issue credit cards and dealerships.

So, tens of thousands of security plans must be prepared just for the nation's new- and used-vehicle dealerships. They qualify mainly because of their finance and leasing operations.

Big job ahead

"It's a very significant requirement, and dealers are going to have to work hard to make sure they are in compliance," says Paul Metrey, director of regulatory affairs for the National Automobile Dealers Association.

"Our assumption is that it's going to apply to virtually everyone" in the association, he says.

NADA has about 19,800 members.

The FTC has been unable to calculate the expected cost of compliance. Metrey says estimates are easier with adjectives than with raw numbers because dealerships vary so much in size and in their levels of preparedness for the requirements.

"It is not an insignificant price tag," proportionally for any dealership, he says. He does not dispute that for larger chains it could reach tens of thousands of dollars.

NADA's management education office has prepared a guide that already has been reviewed by the FTC. It is scheduled to be available online and through the mail this month.

Karen Chapman, NADA's director of management education, agrees there is a low level of awareness about the safeguard rule among dealerships. She says her office is braced for an explosion of questions once the guide goes out and dealerships realize their obligation.

NADA also will sponsor a live online workshop April 24.

The 48-page guide, which will be available to non-NADA members for a fee, includes a sample template for dealerships to follow. But with the great variations among dealerships, "there really isn't a good one-size-fits-all," Metrey says.

The FTC calls its rule flexible, but Metrey says dealerships must do their homework and determine what would apply to their circumstances.

While supporting the goal of protecting consumer information, NADA sought some changes while the rules were being made that would have eased the burden on dealerships. NADA tried to get a later effective date and the inclusion of a commercial

reasonableness standard. It also requested an easing of some of the requirements, especially the monitoring of outside service providers.

The FTC rejected the requests.

Congress directed the FTC to write the safeguard rule for nonbank financial institutions. Other federal agencies handle banks. States regulate insurance companies.

The directive to the FTC to write a safeguard rule was part of the Gramm-Leach-Bliley Act, a 1999 law that overhauled the nation's banking system. The law also included, among other things, the requirement that financial institutions inform customers of their privacy policies - the reason those obtuse fliers are in the mail. Dealerships had to begin giving their customers privacy notices in July 2001.

Out of control?

Despite the 1999 law and other steps that have been taken by government, identity theft incidents still may be on the rise, says Joanna Crane, program manager for the FTC. "I have not heard anyone suggest that the problem has begun to decrease yet," she says.

Explosive growth of the Internet and other computer networks is a big reason.

NADA, like other business associations, worries about the steadily rising number of rules their members must follow in attempts to deal with societal ills.

At some point, when the burden is too heavy, even the government's goals will not be met, NADA's Metrey says.

Nevertheless, for the moment, he says: "We take what's been presented to us, and we just try at this point to make sure we're preparing adequately for it. Right now, it's just a matter of trying to get our people geared up and ready to put it into place."

Especially challenging is the provision that a dealership must ensure that all third-party service providers take steps to protect customer information they may get from the dealership.

Those service providers include any company doing work for a dealership that gives the company access to customer information - including computer services firms, warranty management companies and outside credit and leasing businesses.

"I do not think it is easy for a small business to do," Metrey says.

Williams, the Michigan dealer, says he sat on a bank's board of directors for 20 years and can't say how the bank, with all of its sophisticated controls, protected customer information.

So, while Williams awaits guidance on how to comply with the federal rule, he says he already has a hunch about one important step: careful hiring of employees who handle sensitive material.

Says Williams: "The key is to make sure you have someone with a high level of integrity."