



MARCH 2008

It's Time for an Identity Theft Audit

November 1, 2008. By that date, each dealership must have in place a program approved by the dealership's board of directors that complies with the FTC Red Flag Rule. This is a major new compliance obligation, and we will write about it in future newsletters. However, before implementing a Red Flag program, every dealer should take the time to evaluate its compliance with existing FTC rules for the protection of customers' non-public information and prevention of identity theft – the Privacy Rule and the Information Safeguards Rule.

Here is a simple ten point checklist that can be used to evaluate the dealership's compliance with those important FTC requirements that are already in effect.

Privacy Rule Compliance

- 1 ___ The Company has a privacy notice form.
2 ___ Those customers who buy and finance a vehicle or lease a vehicle sign the privacy notice.
3 ___ Copies of privacy notices are maintained in deal files.
4 ___ Privacy notices are sent annually to buy here/pay here and in-house lease customers.

Safeguard Rule Compliance

- 5 ___ The Company has established a written information safeguards plan.
6 ___ The dealer has designated an employee as the information security coordinator.

7 ___ The Company has done an assessment of the risks of misuse of customer information, and the company regularly reviews and updates its Information Safeguards program.

8 ___ The dealer regularly evaluates its process of electronically receiving and sending customer information.

9 ___ All employees have signed an acknowledgment of their obligations under the Information Safeguards Policy of the dealership.

10 ___ Contractors with access to customer information have signed an Information Safeguards agreement.

see Explanation on page 2

Tool Reimbursement Plans

You've probably seen many commercials for the "easy button". Now we have the IRS "hot button". Simply adopt a tool reimbursement plan and you may press the IRS hot button.

There are a number of vendors marketing tool reimbursement plans. They are marketed as a means to provide non-wage compensation to technicians. However, tool reimbursement plans are highly technical and very closely scrutinized by the IRS. Before adopting any tool reimbursement plan, it is important that the dealership consult with its accountant. Be sure that your accountant agrees that that the tool reimbursement plan is a sound one and will pass muster with the IRS. If your accountant has a problem with the plan, do not adopt it.

1. The FTC Privacy Rule requires that a notification be given to each customer who does a finance or lease transaction. The notification must be written and must inform a customer of the uses by the dealership of the customer's information and of the customer's rights. The notice must include, where appropriate, the customer's right to opt out of release of the customer's information for purposes other than those specifically allowed by law. We have always recommended that dealers avoid the necessity of adopting complicated opt out processes by adopting a policy that the dealership will only use and release customer information in ways that are specifically permitted by law without triggering customers' rights to opt out.

2. The Privacy Rule requires delivery of the privacy notice. Customers do not have to sign the privacy notice, by law. However, it is a best practice to request signature so that the dealership can prove that the privacy notice was delivered. Sometimes customers will refuse to sign the privacy notice and will demand changes. **Never change the privacy notice.** It is a notice; it is not an agreement. It simply notifies customers of the dealer's policy. Any changes creating inconsistent policies will severely complicate compliance. If a customer will not sign, then note on the form that the customer would not sign, hand a copy to the customer, and put a copy in the



appropriate file with the notation. If the customer will not accept the copy, note that on the document and put it in the customer's file.

3. The notice must be delivered in each finance or lease transaction. (The Rule also requires delivery in insurance transactions, but that seldom occurs in a dealership unless there is a finance or lease deal.) Some dealers choose to give privacy notices to all customers. Whether the privacy notices are given only to those required by the Rule, or to all customers, make sure a copy is maintained in the customer's deal file. For those customers who do not buy who are given a privacy notice, it is a best practice to keep a copy with the credit application signed by the customer.

4. Dealers who do buy here/pay here programs or who hold in house leases (as well as dealers who hold any other sort of in house finance agreements) must annually notify those customers of the dealership's privacy policy.

5. Dealers were required to adopt and implement an information safeguard policy no later than May 23, 2003. The FTC is regularly investigating dealers and others to insure that this has been done. If your dealership has not adopted a plan, do so immediately.



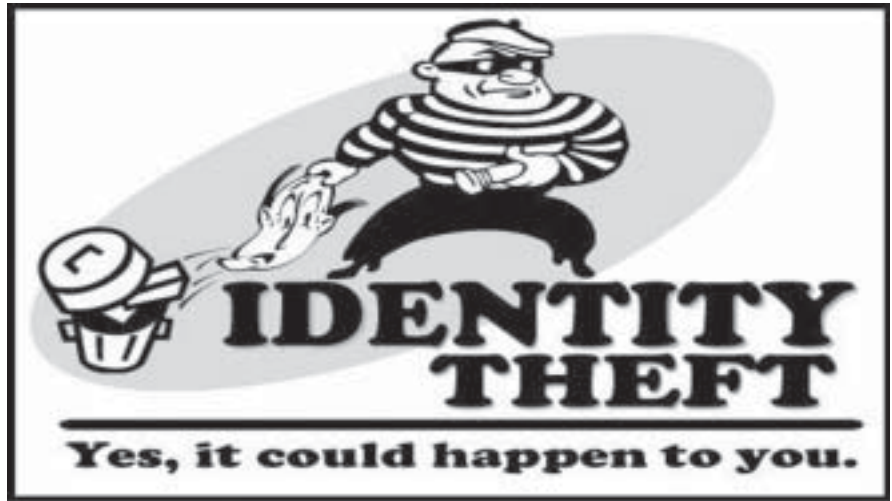
Explanation continued from page 2

6. The Rule requires an Information Safeguard Coordinator. That safeguard coordinator must be an employee of the dealership. The obligations of the coordinator can be delegated to others who need not be employees. However, the person in charge of the Information Safeguard Program in the dealership to whom people can direct questions must be a dealership employee.

7. At the time the dealership adopted its Information Safeguard Plan, an identification and assessment of the risks was required. It is important to the effectiveness of the plan that this step was taken and that evidence of the assessment was kept. Make sure the initial assessment is maintained in the dealership's records. The Rule requires that a safeguard plan be regularly evaluated and amended to insure its effectiveness. There should be a schedule of regular evaluations at least annually and preferably semi-annually. All assessments and changes must be documented. Do not discard prior versions of the plan once the plan is amended. Keep a running history of evaluations and changes in the event the dealership is ever asked to show that it complies with the Information Safeguard Rule's requirements.

8. The FTC has an ongoing requirement to report compliance with the Information Safeguard Rule to Congress. In connection with this

obligation, it regularly investigates companies, including auto dealerships. One of the key elements the FTC investigates is the electronic



processes that dealers use for transmitting and receiving customer information. All customer information should be received securely whether it comes in through email or the internet. All information should be transmitted securely whether it is by internet or another contact means. Regular and continued work with the dealership's IT vendor is necessary to be sure that protection of information transmission is state of the art.

9. Employees throughout the dealership should know of the dealership's policies and procedures to protect customer information. It does no good to adopt a plan in which the employees are not trained. All employees should be trained on the Information Safeguard plan and sign acknowledgments of their obligations.

10. Suppliers who have access to the dealership's customer information are required to sign an agreement that they will safeguard that information. This is not only the law, it is a sensible business practice. The dealership's customer information is a valuable asset that should be protected.

CHARAPP & WEISS, LLP
8300 Greensboro Drive
Suite 200
McLean, VA 22102
Phone: (703) 564-0220
Fax: (703) 564-0221
www.cwattorneys.com
Contents © 2008 Charapp & Weiss, LLP
Articles are for information only and do not constitute legal advice.

Believe It or Not, You Are in the Digital Millennium

Digital copyright laws can have significant consequences for dealers. Alarmed by declining revenues caused by the unauthorized online copying of their products, large entertainment companies have sought enhanced legal protections. Of special importance is the federal Digital Millennium Copyright Act of 1998 (“DMCA”).

The DCMA does not actually prohibit making unauthorized copies of movies, music, or software from sources on the internet—a traditional protection that has existed under other laws for decades. Rather, the D C M A criminalizes the use, creation and distribution of technology, devices, or services that circumvent anti-piracy protections commonly embedded by media distributors in DVDs and software. With the wide availability of software to defeat these protections, converting or “ripping” (converting physical media like DVDs and CDs to digital files on a hard drive or iPod) digital media is tempting. In fact, circumventing these anti-piracy protections can have serious consequences.

Many people mistakenly believe that it is permissible to make copies of media that have been lawfully purchased as long as the copies are never distributed. Doing so, though, may infringe the copyright and, if the work reproduced contains digital anti-piracy protection, such an action violates the DMCA.

Violations of the DMCA can be costly. Copyright holders are permitted to recover either their actual damages caused by violators or statutory damages of between \$200 and \$2,500 per act of encryption circumvention, plus costs and attorneys fees. In addition, DMCA violators may be prosecuted criminally and receive fines of up to \$500,000 and five years in prison for a first offense. Although media producers are often reluctant to sue individual consumers for copyright infringement and violations of the DMCA, businesses are a prime target for litigation because of the perception that they have deep pockets and few defenses. Given these legal requirements, the following are useful points to remember:



- Whenever digital media is purchased for a business, carefully read all the limitations which are included on the media itself or accompanying documents concerning the use of the product. Strictly observe these limitations.
- Do not copy or permit the copying of digital media which contain encryption or any other anti-piracy technology.
- Do not use nor copy any media that the business did not

purchase without the specific permission of the copyright holder.

- Permission to copy, distribute, or perform protected media may often conveniently be obtained from the Copyright Clearance Center (www.copyright.com), which serves as a central clearing house for forwarding copyright royalties to many copyright holders.
- Employees must be trained to understand these basic copyright rules.

Knowledge of and compliance with these rules is more important than ever because media producers often offer large financial rewards to individuals who report illegal copying by a company.