

August 2007

Identifying the Enemy Within

By James Ganther

Your customers aren't the only ones you have to worry about. Sometimes, your own employees can't resist the temptation. Problem is, that opportunistic employee puts your dealership at risk, too.

The fact that identity theft has been cited as the fastest-growing crime in the United States doesn't bode well for automotive dealerships. Because of the nature and amount of nonpublic, personal information dealership employees collect in the course of delivering a vehicle, dealerships are a target for identity thieves. But what happens when that thief happens to be on the payroll?

A name, date of birth, and either an address or social security number are all an identity thief needs to get started. Much of that information can be obtained from a driver's license, which is routinely collected and copied prior to a test drive. However, dealerships collect far more — and far more sensitive — information. Credit applications and reports containing account information can really make the job of a would-be ID thief much easier. Even completed F&I menus can be used to compromise a customer's data security.

Once collected, all of this information is at risk until securely stored or destroyed. And the person with the easiest access to this nonpublic personal information is almost certainly a dealership employee.

Safeguards Rule: The Five Requirements

Implementing steps to prevent ID theft is a good place to start. In fact, it is a requirement set forth by the FTC Safeguards Rule. It says all "financial institutions," including dealerships that arrange financing or leasing, are obligated to have a written customer information security program that addresses the five main areas listed below:

1. Appoint a program coordinator (commonly referred to as a compliance officer).
2. Conduct a risk assessment, including an assessment of the dealership's computer networks and DMS.
3. Design and implement safeguards to address the risks identified in the risk assessment.
4. Oversee service providers, especially outside vendors who have access to nonpublic personal information of a dealership's customers.
5. Periodically audit and revise the information security program.

Let's consider a common fact pattern. A dealership employee has legitimate access to customers' nonpublic personal information. Falling into temptation, the employee copies enough information to get a new credit card issued in the customer's name. The employee goes on an Internet shopping spree, maxing out the card with charges for a new flat-panel HDTV, iPod, and a year's supply of SlimFast meals. All deliveries go to a Mail Boxes Etc. address in a nearby town.

While watching football on the ill-gotten HDTV, the culprit orders two large pizzas from a local pizza place (the SlimFast apparently got old). Unfortunately for the ID thief, he gave away his

home address when ordering the pizza, leading law enforcement to his door.

Now for the payoff question: What happens to the dealership? Like all true legal questions, the answer is "Well, that depends." Not only will the dealership have to prove it had a satisfactory information security program in place, but it will also have to prove it trained the culprit whose behavior is frowned upon. If that's the case, then the answer is "not much." If the dealership can't prove it did both, then the dealership better start warming up its checkbook.

Remedies and Repercussions

No individual aggrieved party can sue a dealership for violating the Safeguards Rule. That's the FTC's job. But the FTC has taken the position that failing to comply with the Safeguards Rule constitutes a deceptive trade practice, and aggrieved parties can sue for that. In fact, "deceptive trade practices" are among a plaintiff lawyer's favorite words, right up there with "class action" and "punitive damages."

Until recently, there wasn't much a dealership could do after an identity theft had occurred. But a new product is making its way into the retail automobile market that could go a long way toward reducing liability in identity theft situations. That product is called identity theft remediation services.

Identity theft remediation services typically offer these types of services following a reported incident:

Assignment of a paralegal case worker to the victim

Contact all affected accounts (bank, credit cards, brokerage and investment, etc.)

Cancellation and replacement of credit cards, driver's license, passport

Guaranteed restoration of credit score to pre-incident level

While identity theft remediation services have existed for years, it has primarily been provided to customers of banks and credit card companies. Only recently have these services been modified to better fit the needs of dealership customers.

"Because dealerships typically present more opportunity for an 'inside job' than most other types of businesses, adding this kind of protection just seemed like a no-brainer," says Ryan Gomez, account manager for NXG Strategies Inc., which is working to bring a remediation program to automotive dealers. "When you've done what you can to prevent identity theft, the natural complement to that security program is a remediation program."

Products That Protect

When Gomez set out to tailor NXG's remediation program to suit automotive dealerships, he says he knew the program had to be inexpensive, easy to administer and effective. What he found was that a good program would allow a dealership to pack the cost of the program into each vehicle it delivers, whether it's paid in cash, financed or leased. The customer then receives a certificate at the time of delivery describing benefits and claims procedures. There is no registration or remittance at the time of delivery — dealerships simply pre-purchase the certificates in bulk prior to delivering the vehicles.

In the event an identity theft occurs involving a covered customer, the customer calls the toll-free number on the certificate and provides his or her customer code printed on the certificate. Once the customer's eligibility is verified, the benefits commence immediately and continue until the case is completely resolved.

While the term of coverage can be adjusted to fit each dealership's needs, three- and five-year terms are common. Gomez says his program can be less than \$6 per vehicle for three-year coverage, and less than \$10 for five-year coverage.

Despite a dealership's best efforts to comply with the Safeguards Rule and otherwise protect customer data, there is really little that can be done to thwart the criminal actions of a determined employee. Having remediation services built into a dealership's standard operating procedures shows the dealership's desire to protect customers. And that can only help reduce the dealership's ultimate exposure for such a breach.

"This kind of coverage closes the loophole for dealerships, as their concern for customers' identity security is clearly demonstrated before the loss occurs. This should reduce exposure to punitive damages," said David Robertson, executive director of the Association of Financial and Insurance Professionals and co-author of the *FTC Safeguards Rule Compliance Kit*.

Robertson also adds a word of caution: "This assumes the dealership already has a safeguards program in place. If that mandatory step has not been taken, trying to close the barn door after the horse has left probably won't do much good."