

CAR DEALER INSIDER

Profit Making Secrets for the Competitive Dealer

Home

Search Articles

Topical Index

Past Issues

Print Current Issue

PDF Issue Archive

Conferences

Activate E-access

Subscribe Now

Privacy Policy

About Us

Contact Us

Issue Date: March 08, 2004

Beware of identity thieves; they could be your customers and employees

Cases bring added call for ramping up Safeguards Rule compliance

The situation: An undercover federal investigator approaches one of your custodians and offers \$50 for each credit application he can find in your store and hand over. Would your employee take the bait?

That's exactly the scenario that resulted in 100 credit applications winding up in the hands of a United States Postal Service inspector at a store in Indianapolis last year, reports Lyn Boucher, a USPS investigator and member of the Central Indiana Financial Crimes Task Force. The group, made up of prosecutors and investigators from several federal agencies, is one of many similar task forces across the country investigating identity theft.

"We were shocked that we could do it so easily," Boucher says. The purchase of credit applications was made during three separate visits to the Indianapolis store. The investigator was also able to purchase a set of new vehicle keys from the custodian. (Note: Investigators are not releasing the name of the store or the name of the custodian, who has been sentenced to jail time and probation, because they are cooperating in ongoing identity theft investigations.)

Background: The undercover visits to the store came as part of a larger investigation of identity theft activities in the Indianapolis area-work that led investigators to believe the custodian might be a source of consumer information identity that could be used to obtain credit cards and IDs.

The Indianapolis case is just one of a growing number of instances where dealerships are a focal point in identity theft activities. The trend typically follows one of two scenarios:

Scenario #1: Dealership employees or visitors obtain customer credit information and re-sell it to identity thieves. Experts say the going rate for an application runs \$50, but could range as high

6 signs of ID theft

Victims of identity theft have sued dealers-and won settlements-after they alleged a store was negligent in preventing a vehicle purchase made with phony ID and credit information.

Tip: If you have any doubts, don't spot deliver a vehicle, advises **Gil Van Over**, a compliance consultant with gvo3 Consulting. Tell customers you'll hold the vehicle while you get their credit approval and do additional background checks (i.e., calling numbers listed on the application for their home, job, etc.). The cooling off period often sends an identity thief elsewhere, Van Over says.

Here are six warning signs that you may be dealing with an identity thief:

1. Customer has an expired or pre-dated driver's license or identity card.



as \$500, depending on the type of customer, says Linda Foley, co-executive director of the San Diego-based Identity Theft Resource Center.

Scenario #2: Stores sell vehicles to identity thieves who use someone else's ID and credit history to obtain financing for a vehicle. Often, identity thieves seek to purchase high-ticket items like automobiles, jewelry and electronics that they can turn into cash, Foley says.

And now the bad news: In either scenario, you and your dealership could be held liable, industry

experts say. Dealership compliance expert **Gil Van Over** of gvo3 Consulting, Schererville, Ind., notes that he's served as expert witness in a case where a dealership sold a vehicle to an identity thief and wound up paying a six-figure settlement.

2. Customer doesn't know or gives conflicting answers to demographic questions (Zip Codes, addresses, phone numbers, etc.)

3. Customer insists on conducting a deal by phone, fax or email.

4. Customer has someone waiting outside and seems in a hurry to finish a deal.

5. Customer pays MSRP and purchases all F&I products without any qualms.

6. Customer's credit report contains a fraud alert. (Typically, these include instructions, such as calling a phone number, to verify a person's identity.) More consumers are requesting these alerts as fears of identity theft rise.

Safeguards Rule compliance helps prevent identity theft, liability concerns

Van Over says the Indianapolis store might have thwarted the custodian's efforts had it taken the required steps to comply with the FTC's Safeguards Rule. The Rule requires that all stores assess risks of customer information leaks and take steps to prevent them. He says some of his clients have restricted cleaning crew access to F&I and sales offices to prevent potential losses of customer information, others are making sure all customer information is locked and secured every night when their stores close for the night.

Safeguards Rule compliance experts note that many dealerships have yet to fully embrace the Rule and its provisions, which went into effect last May (see below for key compliance provisions.). The issue: Dealers view it as one more regulatory burden, and one that carries little risk of liability because the FTC lacks the resources to launch wide-scale enforcement efforts. "Despite what dealers say, they don't give a rat's rip about it," says a consultant who's conducting Safeguards Rule compliance workshops.

But there is a potential risk for non-compliance, cautions Jim Ganther, vice president and general counsel, Continental-National Services Corp. His concern: Virtually every dealership has a privacy policy that states they comply with prevailing federal laws that call for protection of customer information. He fears class-action attorneys may find Safeguards Rule shortcomings and file claims alleging stores misled consumers about the safety of their information. "That's a shoe that's waiting to drop," he says.

A quick look at the five key areas of Safeguards Rule compliance...

The FTC's Safeguards Rule is intended to protect customer privacy. Compliance consultant Mike Shanahan at K.B. Parrish & Co., Indianapolis, advises dealers to think of customer information like money and come up with processes to protect it in

all parts of your store. Here are the five building blocks of a Safeguards Rule compliance program:

1. Designate a program coordinator. The coordinator should be a senior-level manager or someone who has top management's approval to oversee the compliance program. Some stores are using controllers and COOs as program coordinators.
2. Assess risks. The most common problem, Shanahan says, is deal jackets laying out in the open on desks or fax machines. Stores are using storage cabinets and central repositories for deal documents to minimize such risks.

2 Develop a written program. The write-up should comprise all findings from your risk assessment and the measures you will put in place to protect customer records. In addition, the written program should include provisions for auditing the effectiveness of your overall record safekeeping, and obtaining written assurances from vendors that they are committed to safeguarding customer information and how they might handle any breaches.

3 Train employees. The Rule requires training of employees and obtaining their signatures on forms acknowledging they understand the Rule and your policies for safeguarding customer information.

4 Evaluate your program. The Rule requires testing of your policies and procedures—something many dealers have yet to do, says Marc Crumback, a partner with Beers & Cutler, Washington, D.C.

...plus, answers to two key Safeguards compliance questions

Question 1: Does the Rule's provisions for protecting "non-public" information include customer names and phone numbers?

The answer is "Yes," according to industry compliance experts who say you can't be sure whether a phone number is unlisted. What's more, the Rule doesn't have provisions for varying degrees of protections based on the type of customer information you collect.

Question 2: Does the Rule apply to my service and parts department?

Yes, compliance experts say. That's because the departments are part of your business, which is covered by the Rule. That means you should take steps to ensure you don't have ROs laying out in plain view, especially since some of those may include customer information that stemmed from the initial sale of a vehicle.

Categories: [Legal](#) | [Management Security](#) | [Personnel/Human Resources](#)

© 2005 UCG. All rights reserved.

Do not duplicate or redistribute in any form.

Car Dealer Insider is available for internal use only by authorized users.

Car Dealer Insider

11300 Rockville Pike, Suite 1100, Rockville, MD 20852.

Phone: 888/287/2223 Fax: 301/816-8945 Email: cdicustomer@ucg.com