

Identity Crisis

As ID theft grows, auto dealerships become more frequent targets

Donna Harris

Automotive News

July 26, 2004

Safety first

Security experts offer dealers these tips to prevent identify theft:

Run background checks on prospective employees.

Keep transaction files in a locked room with restricted access.

Limit access to customers' credit reports to a few employees.

Don't leave customer information unattended on a desk, even for a short time.

Shred credit reports when transactions are complete.

Limit access to dealership's computer files with restricted passwords.

Don't assume a computer firewall will repel all hackers.

The thieves who struck Serramonte Infiniti in suburban San Francisco in April ignored the dealership's cash and costly equipment. But they hit the jackpot anyway.

They reached into an unlocked cabinet and stole 57 files of customer transactions. The files included credit reports, bank statements, driver's license numbers, credit card information and Social Security numbers.

Two suspects in the robbery are charged with burglary and credit card fraud. They allegedly used the stolen data to make illegal purchases at department stores.

Fifteen customers of the dealership told police in Colma, Calif., that the robbers tried to steal their identities. The crime embarrassed Sonic Automotive Inc., the nation's third-largest auto retail group, which owns the store.

Each year nearly 10 million Americans are victims of identity theft, a crime that costs them roughly \$5 billion a year, the Federal Trade Commission estimates. The FTC does not offer specific figures for dealerships. But dealers and their customers are increasingly vulnerable to thieves and computer hackers, security experts say.

Security breaches can subject dealerships to consumer lawsuits, federal and state penalties and lost sales. Dealers are attractive targets because of the personal information they collect about customers.

Financial institutions that compile similar data have made conspicuous efforts to fight identity theft. Citibank has built a popular advertising campaign around the issue. But many dealers are lagging in their efforts to safeguard their customers' sensitive financial records, experts warn.

Thieves' candy store

"When you buy a vehicle, you have to give about everything but your blood type," says Charles Dodd, CEO of the Center for Information Systems Security Research of Tampa, Fla. His computer security firm works with dealers and other businesses.

"A car dealer might have 10,000 customers," Dodd says. "For a thief, that's a candy store."

Bruce Townsend, deputy director of the U.S. Secret Service, says "there is no question" identity thieves are targeting dealerships. The Secret Service investigates ID theft cases.

"The information (dealerships) have has value," he says. "It is just as valuable as currency."

Townsend headed the West Tennessee office of the Secret Service from 1997 to 2000. At least a third of ID theft cases that crossed his desk involved dealerships, he says.

The federal Safeguards Rule requires dealerships and other businesses to protect customer information. Some states require additional measures. The FTC can fine dealers \$11,000 for each failure to comply with the rule, which took effect in May 2003.

"We think identity theft is a big problem," says Rodney Nettles, business manager of Bob Taylor Chevrolet and Bob Taylor Jeep in Naples, Fla. He says the dealerships have revamped the way they handle customer data.

They have spent \$15,000 on computer technology designed to repel fraud. Professionals monitor their networks. The stores scan rather than photocopy driver's licenses. They no longer keep transaction files on paper.

"This is a bear to keep up with," Nettles says.

Many other dealers are reluctant to acknowledge the problem of identity theft. Beth Givens, director of the nonprofit Privacy Rights Clearinghouse, a consumer advocacy group in San Diego, says customers could shun businesses that are shown to play fast and loose with sensitive information.

The Safeguards Rule does not authorize private civil suits. But legal analysts believe customers could sue dealers for negligence if they compromise financial data.

Dealers' duty

"One could easily argue that the rule establishes a duty to the customer," says Jim Ganther, a lawyer for Continental-National Service Corp. of Tampa, which supplies finance and insurance products to dealerships.

"Breach of that duty resulting in damages all adds up to negligence," Ganther says. "That's all a lawyer needs to open the courthouse doors."

Consumers have sued other businesses they allege were negligent in handling personal information, Givens adds.

Jessica Rich, assistant director of the FTC's division of financial practices, says the agency is investigating dealerships but declines to say how many. The commission soon could cite stores for violating the Safeguards Rule, she adds.

The National Automobile Dealers Association advises dealers on complying with federal privacy rules. NADA recently sponsored a two-hour conference call with FTC privacy experts.

"Identity theft, through whatever means, continues to be a significant concern for dealers," NADA lawyer Paul Metrey says.

Big dealers not immune

Sonic says Serramonte Infiniti contacted police and notified customers whose information was compromised after the April robbery. Sonic spokesman Bill Steers declined to discuss why the dealership had kept customer files in an unlocked cabinet. Dealership executives refused to comment.

Serramonte Infiniti now keeps those files in a locked, windowless room, Steers says. Only a few employees have access to that room. The dealership also changed locks on its building, file cabinets and employee desks. It installed a security camera system.

All Sonic dealerships comply with the Safeguards Rule, Steers says.

"Sonic recognizes the critical importance of protecting our customers' personal information," he says. "Our dealerships have implemented rigorous procedures and controls to safeguard customer information."

Asbury Automotive Inc. of New York, the nation's fifth-largest auto retailer, also endured a recent alleged incident of identity theft at one of its dealerships.

A former salesman at Holler Mitsubishi and Asbury-owned Coggin Honda in Orlando, Fla., was among 15 suspects charged in June with participating in an identity theft ring. The ex-employee allegedly tapped dealership records, providing financial data that enabled other members of the ring to make illegal purchases with false documents.

Holler Mitsubishi executives did not respond to repeated phone calls.

Coggin Honda's customer records remained intact, says Allen Levenson, Asbury's vice president of marketing. But thieves used stolen identities to buy seven used vehicles from the dealership through the indicted salesman, Levenson adds. A police investigation enabled the store to recover all of the vehicles.

Levenson says Asbury couldn't have anticipated the thefts. The salesman had no police record. He passed background checks and a drug test before he was hired.

"You can only go so far," Levenson says.

Inside threat

Other dealers have failed to identify job candidates' police records. A Phoenix dealership did not perform a background check before it hired a salesman with a criminal record. The employee later stole a customer's identity.

The customer was furious with the store, says Jordana Beebe, a spokeswoman for the Privacy Rights Clearinghouse. But the dealership shrugged off the incident, she says.

Even if a thief is not on a dealership's payroll, employees remain the chief source of vulnerability to identity theft, experts say.

"Employees are the biggest risk," says Brian Bentz, a partner with the Dixon Hughes accounting firm in Memphis, Tenn. The firm has 2,000 dealer clients.

Bentz says he urges clients to restrict access to sensitive information to guard against dishonest or careless employees. He cites a case in which a dealership employee left customer files on a desk while he got coffee. Someone walked in off the street and walked off with the information.

Employees have left copies of customers' credit reports on top of a photocopier, Bentz says. Or they tossed sensitive data in the trash without shredding it, an oversight that led to identity theft.

"Dealers have a better awareness and understanding of how rampant identity theft is" because of the Safeguards Rule, Bentz says. "But is everyone where they need to be? No. To change policies and procedures overnight is not easy."

The FTC's Rich concedes that "there is no such thing as perfect security." But she says dealerships need to install reasonable policies and procedures.

Computer scare

Computer hacking can pose a greater potential threat for identify theft at dealerships than a physical break-in. Hackers can penetrate files from a remote location. A dealership may not even know its data are compromised.

"I witnessed a horror story with my own eyes," Ganther says. He visited a Florida dealership to assess its computer network's compliance with the Safeguards Rule.

"While I was there, I saw the (security) consultant's laptop indicate a hack attack was under way," Ganther says. "A signal was coming in through the dealer's high-speed T1 line, and sweeping across every computer on the network every six seconds."

Dealership managers watched the attack but could not stop it, he says.

Ganther refuses to disclose the dealership's name and location. He says the store's general manager thought such an attack was impossible because it had spent \$13,000 on a computer firewall.

Alan Andreu, president of Dealership Defense, a Plant City, Fla., software security firm, says firewalls can give dealers a false sense of security. They still must monitor their systems for potential hackers, he adds. Andreu sells software that assesses network security and alerts dealerships to intruders.

"If the firewall is improperly configured, it is next to useless," Andreu says. "It is nothing more than a box with lights on it."