Filling Empty Heads With The Safeguards Rule

By James S. Ganther, Esq.

There is a time-honored legal activity known as "reading the tea leaves." This term refers to the art of trying to figure out what a governmental entity really meant when it published a rule before the courts have had a chance to weigh in on the issue. The term applies well to the FTC Safeguards Rule, which became law just three short years ago and is, in fact, small enough to be folded into a Lipton Flow-Thru tea bag.

When the FTC promulgated the Safeguards Rule on May 23, 2003, who knew what meaning was packed into its 786 words? What constituted compliance? In deference to this legitimate question, when the FTC began enforcing the Rule, it did not immediately apply substantial monetary fines. Rather, it entered into consent orders with the offending companies, in an effort to both force those companies into compliance and, at the same time, put the rest of the world on notice as to what the FTC considered adequate effort to satisfy the Rule.

Well, after three years, we're beginning to get the picture. And recently, after two and a half years of no-monetary-fine consent orders, the FTC has begun to levy fines — *big* fines. So we're in a position to make some judgments about what actually constitutes compliance with the Rule. Those judgments follow.

Only Letters in Early Days

A few short months after the enactment of the Safeguards Rule, the FTC fired its first shot across the bow of the retail automobile industry. On Sept. 9, 2003, the FTC sent a series of enforcement letters to certain automobile dealerships in the Eastern United States. We can learn a lot from what those enforcement letters said, and what they didn't say.

The FTC characterized the enforcement action as "a non-public inquiry" into the dealerships' compliance with the Rule. Thus, the results of those investigations have not been made public.

In its enforcement letters, the FTC requested voluminous records from the dealerships, describing their information security programs as well as detailed information about the ownership structure of each dealership. When those two requests come in consecutive paragraphs, dealer principals get nervous.

What is most interesting from the perspective of two-plus years since those letters were delivered is what they did not ask for. The letters made *no specific mention of computer security*. All of the document requests seemed to be aimed at policies, procedures and safeguards designed to protect paper records. This would soon change.

Real Risk Is in Computers

Sometime in 2004, it seems to have dawned on the FTC that the real risk to customers' non-public personal information (NPI) was the vulnerability of the computer networks in which such NPI was stored. After all, if someone picks up an unguarded deal jacket, only one identity has been compromised. If someone hacks into a dealership computer network, *all* of that dealerships' customer NPI is compromised.

In 2004, the FTC filed a complaint against Petco Animal Supplies Inc. The FTC alleged that Petco failed to safeguard its computer network. This was discovered when a "White Knight"

hacker — one who hacks for the joy of hacking, but doesn't actually steal any information — easily penetrated the Petco Web site and was able to see, in plain text, the credit card numbers of Petco's customers.

An important element of the complaint against Petco is that Petco represented to its customers that it actually took steps to protect their NPI when, in fact, it did not. This has obvious ramifications for the retail automobile industry, which also makes such representations to its customers through the mandatory privacy notice given to each customer at the time of sale.

The FTC determined that Petco violated the Safeguards Rule by "failing to implement reasonable and appropriate measures to secure and protect databases" that contain customer NPI. The FTC went on to allege, "The risk of such Web application attacks is well-known in the information technology industry, as are simple, easy to implement, and publicly available measures to prevent such attacks."

Laying the allegations against Petco alongside the terms of the Rule, Petco was being charged with failing to conduct a network vulnerability assessment and failing to design and implement reasonable safeguards to address the risks identified through the assessment. Thus, Petco violated the Safeguards Rule *even though no customer NPI was actually compromised*. A theologian would call this a "sin of omission"; Petco was prosecuted not for what it did, but for what it failed to do.

If that were not enough, the Petco case made another point with troubling implications for the retail automobile industry. Almost as an afterthought, the FTC concluded its complaint against Petco with the statement: "The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices."

Gulp.

What this means is that the FTC now considers violations of the Safeguards Rule to constitute a "deceptive trade practice," and those three words are music to the ears of plaintiffs' lawyers. Furthermore, most states' unfair and deceptive trade practices acts look to the FTC for interpretations of what amount to such an offense. This means that the federal interpretation that a violation of the Safeguards Rule is a deceptive trade practice could support a lawsuit based on state law as well.

The FTC refined what it considers adequate computer security in the Nationwide Mortgage case. In that 2004 case, Nationwide was cited for failing to monitor its computer network for "vulnerabilities that would expose customer information to attack." Thus, under the FTC's interpretation expressed in the Nationwide Mortgage case, a dealership is violating the Rule if it does not regularly monitor its network for new vulnerabilities as those become known.

In 2005, the FTC filed a complaint against Superior Mortgage Corp. While the allegations in the Superior case mirrored those in the Nationwide case, there was one new wrinkle: Although customer NPI was transmitted in encrypted format to Superior through its Web site, Superior was cited for failing to encrypt that information when it transmitted it to its lenders.

This situation is analogous to a dealership transmitting customer NPI over unencrypted links in the course of presenting a *Web-based* menu. While the FTC hasn't opined on this issue directly, it is reasonable to assume that the use of such unencrypted menu programs would constitute a violation of the Rule, with all the bad results described above. To see if the

Web-based menu you're using is encrypted, look for "https" (the "s" stands for "secure") preceding the menu Web site's URL. If it merely reads "http," find another vendor before the FTC finds you.

Also in 2005, the FTC filed a complaint against BJ's Wholesale Club Inc., a Massachusetts-based company operating 150 warehouse stores in 16 states in the Eastern United States. The FTC alleged that BJ's violated the Safeguards Rule by:

- Failing to encrypt customer NPI before transmitting it from computer to computer
- Storing customer NPI in files that could be accessed using commonly known default passwords
- Failing to utilize readily-available security measures to prevent unauthorized wireless connections to its networks
- Failing to use measures sufficient to detect unauthorized access to the networks or to conduct security investigations

BJ's ultimately settled the case against it, but the FTC's position remains: To comply with the Safeguards Rule, you'd better secure your computers, including use of an intrusion detection system.

Monetary Fines Now Assessed

Earlier this year, the FTC settled a claim against ChoicePoint Inc. for its failure to properly secure its customers' NPI and, as in the Petco matter, making deceptive claims that it actually did protect such data. What is different about the ChoicePoint matter, however, is that this time the FTC assessed monetary fines and, as promised, *big* ones. ChoicePoint was fined $10 million in civil penalties, and an additional $5 million for consumer redress. For the mathematically challenged, that adds up to $15 million that would not be covered by any insurance policy.

From reading the FTC's tea leaves over the past three years, several things become clear:

1. The world is on notice that the FTC considers lack of computer security the main threat to customers' NPI, and therefore a prime area of concern in connection with Safeguards Rule enforcement.

2. It is a violation of the Safeguards Rule to fail to conduct a network vulnerability assessment.

3. It is a violation of the Safeguards Rule to fail to continuously monitor a computer network for vulnerabilities.

4. It is a violation of the Safeguards Rule to fail to use a network intrusion detection system.

5. The FTC (and thus, state attorneys general) considers violations of the Safeguards Rule to constitute a deceptive trade practice.

6. The FTC has taken the gloves off. Fines have been levied, and we can expect more of the same in the future.