

From: Thomas Eblen
Sent: Tuesday, June 22, 2004 2:47 PM
To: rfidworkshop
Subject: Fw: Spot197.htm

RFID technology could eliminate the "crime" of shoplifting from society if government will require the corporate retailers to render ordinary diligence in the conduct of their businesses.

If you read the article below (written in about 1997, I assume) you will understand that the arrests for "stealing" of persons who are permitted to exit the stores without paying are the fulcrums for the punitive civil damages that are blessed in the civil statutes of the states.

If this quiet change in the criminal law and the somewhat new civil statutes are constitutional, why has there been no public notice posted in the malls and discount stores concerning the state authorized "fine" that is paid to the corporate retailers?

The writer of this advice is warning security guards to wait until the city disposes of the arrests before trying to collect these "fines". He advises, of course, that criminal convictions are not necessary to collect civil damages. He knows that all suspects arrested and ticketed by the cities will be found guilty by the courts or diverted from the courts.

The cities assumed the responsibility for these arrests to protect the retailers because the retailers would not prosecute "first-time" suspects for the purpose of deterring future attempts. It was not cost effective for them to do so. If the prosecution failed, the retailers opened themselves to suits for false arrest and malicious prosecution.

But, our cities have made it cost effective for themselves and for the retailers to solve the problem of "shoplifting for the corporate retailers and give them a large subsidy to boot because they have closed the lower courts to any defense to a ticket for "stealing"!

The corporate retailers had law, before the change, in which they could prosecute persons for attempts to steal their property but they used the law rarely because it was not cost effective to prosecute for the purpose of "deterrence" and it was hard to show juries or the courts that they had suffered any actual loss. The courts at that time presumed that merchants had an obligation to stop all attempts to steal that they witnessed because of the manner in which retail businesses are conducted.

The retailers will not prosecute for shoplifting under these somewhat new civil laws to get these punitive civil damages because they would have to use their double-agent security personnel as prosecution witnesses and it would be obvious that the merchandise in question had been recovered and returned to stock to be sold ----- and that the store had refused to accept payment for the merchandise and had allowed the defendant to exit the store without requesting payment.

These somewhat new civil statutes were written and passed by the legislatures with the view (perhaps known only to the writers) that there would be millions of arrests, convictions, and diversions from the lower city courts and this is frightening. The tickets for "stealing" make it cost effective and profitable for the retailers to demand the punitive damages enacted into law by the state legislatures.

Because our legislators are always so happy to help the special interests, state after state over the past twenty some years have passed these new "civil recovery" statutes for "shoplifting". When the first state did it and it was so successful, it was not difficult to get other states to pass these laws to give this subsidy to the corporate retailers. If the lawmakers had any doubts whatsoever, they took comfort in the fact that "all of the other states" were doing it. Arrests for profits on this large a scale are something new to our democracy and are more fascist in nature than democratic.

RFID technology could rid us of this ugly status quo but the special interests will not want to give up their subsidy.

Carol Eblen

MO

----- Original Message -----

From: Thomas Eblen

To: Thomas Eblen

Sent: Sunday, April 04, 2004 12:32 PM

Subject: Spot197.htm

<<http://www.securitymanagement.com/library/spoticon.gif>>

Security Spotlight

By Michael Gips

In this issue:

Shoplifter Shakedown?

Open Door Policy

Fire Fallout

Ask Us

Suggestions Sought

Home on the Page

Shoplifter Shakedown?

Almost every U.S. state has enacted legislation--commonly called "civil recovery" or "civil demand" statutes--to allow retailers to forego the hassles of the legal system and simply ask shoplifters to make restitution, including some loss prevention costs. But is it appropriate for businesses to make a civil recovery demand while the suspected shoplifter is still in the custody of the security department and before even an internal determination of the validity of the charge has been made?

Civil recovery, which in most states is not tied to criminal action (that is, criminal action does not affect the ability to obtain civil recovery), is normally handled after the suspect has been released, explains Read Hayes, CPP, a loss prevention specialist. The victimized business, on its own or via an attorney or third party company, typically sends the shoplifter a letter demanding statutorily set compensation, including the value of the item stolen and damages.

But loss prevention personnel at some businesses try to get accused shoplifters to pay this fine before they are released, presumably because their chance for recovery drops when the suspect walks out the door.

Disneyland recently changed its collection policy after facing complaints that security officers tried to collect civil recovery from detained suspected shoplifters. Park spokesman Tom Brocato explains that suspects, after being cited by the Anaheim Police Department, used to be handed a notice informing them of Disneyland's right to seek restitution. Some suspects offered to pay on the spot and the park accepted, says Brocato. He says that park policy is now to mail out the notice and not seek restitution "until the courts have come down with a conviction."

Although the typical statute, including California's, does not expressly prohibit businesses from making civil demands at the scene, Neal Tenen, an attorney and part owner of Van Nuys, California-based Civil Demand Associates, which handles the recovery process for businesses, says that he advises clients not to take money at store level for various reasons. What looks like a clear-cut shoplifting case at the moment may fall apart once a report is prepared and

reviewed, Tenen notes. For example, the report could show that an officer never saw the suspect pocket the goods or that personnel lost track of the suspect during the surveillance.

Tenen says that plaintiffs can come up with a wide variety of claims stemming from a civil demand made on the scene, depending on the circumstances, including false imprisonment, extortion, and intentional or negligent infliction of emotional distress. Tenen advises clients to give detained suspects a notice informing them that the state has a civil recovery process and that the suspect will be hearing from the store's attorney or corporate offices. Actual demand letters are sent out later. Making a civil demand after facts have been carefully reviewed, explains Tenen, reduces the chances for mistakes and consequent litigation. As for the extra cash a company might get through on-the-spot recovery actions, adds Tenen, those gains do not justify the risk. "It only takes one person to yell extortion."

Open Door Policy

The number of visitors from "sensitive" countries to U.S. Department of Energy (DOE) nuclear weapons laboratories is on the rise--and growing at a faster rate than the number of visitors from other countries--according to recent testimony presented before the House of Representatives Committee on National Security's Subcommittee on Military Procurement. Visitors from sensitive countries averaged 1,679 per year from 1993 to mid-1996, up from 513 a year during the height of the Cold War. Sensitive countries--those posing a threat to national security, supporting terrorism, seeking nuclear materials, or having regional instability--with the most visitors included China, India, Israel, Taiwan, and the states of the former Soviet Union.

Unlike during the Cold War, much of the authority to approve visitors has been delegated to the individual laboratories. The laboratories now approve all visits that do not involve high-level foreign visitors, sensitive subjects, or secure areas. The testimony (GAO/T-RCED-96-260) is available from the U.S. General Accounting Office at P.O. Box 6015, Gaithersburg, MD 20884-6015; 202/512-6000; fax: 301/258-4066; or through the Reading Room. <<http://www.securitymanagement.com/library/000292.html>>

Ask Us

One item in this month's "Spotlight" column explores gray areas in the retail civil demand process. Previous pieces have looked into university responsibility for conducting background checks of prospective students (August 1995) and an employer's ability to use a history of suspicious workers' compensation claims as a basis for rejecting an applicant (November 1995). Are there any other gray areas or fine points you'd like to see this column address? Send your questions to: Senior editor, Security Management, 1655 North Fort Myer Drive, Suite 1200, Arlington, VA 22209; 703/312-6355; fax: 703/522-5226; e-mail: smeditmg@nicom.com.

Fire Fallout

Eleven hundred guests bedded down for the night is normally a peaceful time for hotel management; but that scene can turn to pandemonium when fire strikes. A recent nighttime fire emergency in Washington, D.C.'s elegant Omni Shoreham Hotel forced the security department to put its evacuation and disaster management plans to the test.

The situation involved several simultaneous fires, strategically placed--and apparently intentionally set--throughout the hotel, forcing evacuation of all guest rooms. Despite the potential for problems, "people took it very well," says Managing Director Jose Campo. Although the hotel sustained more than \$1 million in property damage, no one was hurt.

Omni Shoreham staff hold monthly fire drills in which staff report to designated areas, telephone operators make calls, and the alarm and public address system are tested. Campo credits these monthly drills with helping the evacuation go smoothly. But he adds that the incident reinforces the importance of conducting drills with the night crew, which is smaller and has to deal with a large population of tired, disoriented guests.

Although no one got hurt in the fires, management has been looking at additional safety and security precautions. "It's quite a wake-up call," Campo says. For example, before the fire, surveillance cameras covered the lobby, certain

corridors, and access points such as guest entrances and the receiving area, but because video did not capture the culprit, the hotel is now considering adding cameras at other points.

The hotel has also emphasized security awareness to its nonsecurity staff. In addition, hotel management has been testing the hardware on exterior doors.

Because the most damaging fire originated in an unprotected storage area, management is considering protecting such unguarded areas with locking doors or gates.

Suggestions Sought

The Central Station Alarm Association (CSAA) of Bethesda, Maryland, is requesting comments on two standards recently proposed to the American National Standards Institute.

Targeted toward alarm companies, alarm monitoring facilities, municipal emergency personnel, and the insurance industry, the first standard provides information on properly processing and responding to alarm signals. The second standard is a glossary of more than 350 terms commonly used in the alarm monitoring industry.

Suggestions from security organizations, companies, government agencies, and individual practitioners are welcome. Respondents must return comments to CSAA, 7101 Wisconsin Avenue, Suite 901, Bethesda, MD 20814 by February 4, 1997.

Copies of the standards are available at the above address or through SM Online (in the Reading Room <<http://www.securitymanagement.com/library/000291.html>>).

Home on the Page

Step off the printed pages of Security Management into the magazine's virtual pages on the World Wide Web. Here's a sample of this month's diverse offerings.

Gangs.
Using data collected in a survey by the National Institute of Justice (NIJ), a group of researchers extrapolate that in 1993 there were 555,181 gang members and more than 580,331 gang-related crimes. These "reasonable" estimates, in the parlance of the authors, represent an increase of 123 percent and 1,152 percent respectively in the number of gang members and gang-related crimes since 1991. Read this Research in Brief" online <<http://www.securitymanagement.com/library/000293.html>> .

Campus security.
Find out what's new at campus police stations and security departments worldwide via SM Online's link to the University of Southern California Department of Public Safety Campus Law Enforcement Resource Page <<http://dpsw.usc.edu>> . The page offers links to more than 170 campus police and security department sites.

Retail security.
Professor Joshua Bamfield of the NENE Centre for Retail Research in Northampton, England, has written a report on the civil recovery process <<http://www.nene.ac.uk/mmb/business/bspag13.html>> and how it works in the United States and Canada.

Police technology.
From restraining foam and smart guns to projectile launchers and retractable spiked barrier strips, the Office of Law Enforcement Technology Commercialization (OLETC) explores the potential of weapons and other technologies and discusses the results of testing. Link to OLETC's home page <<http://www.nttc.edu/OLETC.html>> via SM Online.

Encryption.
What's the latest on U.S. and international cryptography policy? Recent statements on the subject by Vice President Gore, FBI Director Louis J. Freeh, and a panel of encryption experts can be found via SM Online's link to The Cryptography Project <<http://guru.cosc.georgetown.edu/~denning/crypto/>> . The site also includes papers and articles on

related topics.

Information security.

A report by the General Accounting Office found that ten U.S. government agencies had information security weaknesses, some of which have existed for years. The most common problems were poor controls over access to sensitive data and incomplete or untested disaster recovery plans. For example, annual audits since 1993 reveal that the IRS cannot ensure the confidentiality and accuracy of taxpayer data on its computers. Read the full report <<http://www.securitymanagement.com/library/96110.html>> online.

Books.

Read sample chapters of books reviewed this month and in prior issues. Spotlighted this month are chapters from Safe Schools: A Handbook for Violence Prevention <<http://www.securitymanagement.com/library/000257.html>> (reviewed in November) and The Underground Guide to Computer Security <<http://www.securitymanagement.com/library/000273.html>> (reviewed in December).