

THE WALL STREET JOURNAL

MONDAY, JUNE 16, 2008 - VOL. CCLI NO. 140

MANAGING TECHNOLOGY

Stop That Thief

Losses from theft and fraud can sink a small business. Technology offers welcome relief.

By Raymond Flandez

FOR SMALL BUSINESSES, preventing theft and fraud by employees can be an uphill struggle.

Unlike their big counterparts, small companies usually can't afford a large security staff or big-ticket monitoring technology to keep an eye on things. And they often don't generate enough sales volume to make up for the losses from pilfering.

Now a new generation of security technology aims to give small businesses an inexpensive

Trouble in Store

The Situation: Theft can mean disaster for a small business, wrecking its profit margins and hurting its reputation.

The Trouble: Small businesses often can't afford the big-ticket security solutions big companies favor.

The Way Out: A host of new technologies are filling the void, giving small operators a way to protect their businesses on the cheap.

defense against unscrupulous employees. Some of these systems let business owners who are on the road check their security cameras over the Internet and get email alerts if something unusual happens, such as employees closing up shop early.

Restaurants, meanwhile, can use tableside credit-card readers to prevent cashiers from stealing customers' card numbers or inflating the tips written on bills. And grocery stores can use a combination of security cameras and software to automatically spot cashiers who try to slip free products to their friends and family.

These new products are arriving as stores face mounting losses from theft. According to the latest National Retail Security Survey, losses from "shrinkage"—which includes theft, fraud and error—

reached a new high of about \$40.5 billion in 2006. About half of that—\$19 billion—came from employee theft. Shoplifting, in contrast, accounted for about a third. (The study, conducted by the University of Florida and the National Retail Federation, was funded in part by grants from makers of security systems.)

Here's a look at some of the most innovative new security systems out there.

WATCHING FROM AFAR

For a small-business owner worried about employee theft, leaving the shop in someone else's hands can be nerve-wracking. Now a host of security providers let bosses check in on things from the road.

For instance, **Alarm.com** Inc., of McLean, Va., sells a system that allows owners to travel to a Web portal and get remote feeds from security cameras, change entry codes and trigger sensors that monitor systems such as lighting and climate control. If a problem arises with those systems—such as a power outage—you can get an alert via a text message or email.

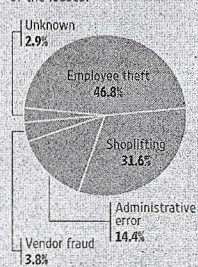
Recently, Kevin Donahue, owner of a **Planet Beach** Franchising Corp. location in McLean, was in Amsterdam on business when he received a text message from Alarm.com: The spa's alarm system had been armed at 3 p.m., before the usual closing time. He checked the security cameras online and saw the facility was dark.

So he called his manager and got the explanation: The spa had closed early because of a snowstorm.

"The greatest thing is that it gives me the ability to travel and do the things that I do," says the 34-year-old Mr. Donahue, who's also a full-time salesperson for a tech company and often travels outside the country on sales trips. "It gives me the ability to manage my staff remotely. I can call and say, 'What's going on?'" Mr. Donahue bought the sys-

Off the Shelves

In 2006, retailers lost a record \$40.5 billion to theft, fraud and error. Here's a breakdown of the losses.



Note: Percentages don't add up to 100% due to survey methodology.
Sources: The University of Florida and the National Retail Foundation

tem for under \$100 and pays a monthly fee of \$39. Alarm.com says the base price for the system is usually \$500, with a monthly fee of \$29 to \$50, although those numbers can vary by reseller and area, as well as the features customers choose.

SAFEGUARDING CARDS

Another new technology helps small businesses—particularly restaurants—protect against "skimming." In this scam, cashiers steal customers' credit-card information for use in identity theft.

About 70% of credit-card-fraud cases involve skimming, according to Trustwave Holdings Inc., a data-security and compliance-management company based in Chicago. In many cases, business owners are ultimately held responsible for their cashiers' crimes—costing them money and damaging their reputation.

For some businesses, the solution is to let customers become their own cashiers. At **South-east Grille House** in Brewster, N.Y., servers bring a wireless gad-

get called On the Spot to their customers' tables. Patrons can swipe their credit cards on the device—which is about the size of a brick—punch in the tip amount and print out a receipt to sign, all from their seat.

Since the customer enters all the information, cashiers can't inflate the tip—and the receipts don't contain much personal data that could be stolen and used for identity theft.

The device, from **VeriFone Holdings** Inc. of San Jose, Calif., runs about \$1,000. Southeast Grille House owner Domenico Chiera says it was worth the investment. "It's fast, and the receipt has little information, so no names or numbers," says the 57-year-old restaurateur. "I like the system. It works well for us."

CHECKING OUT FRAUD

At grocery stores, thieving employees are almost as much of a problem as shoplifters. About 40% of grocery-store thefts were attributed to employees in 2006, according to the Food Marketing Institute's Supermarket Security and Loss Prevention 2007 report. One of the biggest problems is "sweethearting," in which cashiers give friends and family freebies by pretending to scan items at the register.

Many stores use closed-circuit television to watch checkout lines. But the stores often don't have the time or manpower to review the tapes, so the cameras aren't a strong deterrent. **StopLift Inc.** of Bedford, Mass., has devised a system that combines cameras with advanced software to spot sweethearting automatically. The technology can recognize when cash-

iers make unusual movements when handling items—such as placing a hand over a bar code—and determine whether the items were properly scanned.

When the system identifies sweethearting, it places blinking squares over the video to show exactly where the theft occurred. Then it gathers the incriminating clips together for owners to review.

Stores "have the cameras but they don't have the manpower to watch it," says Malay Kundu, chief executive of StopLift. "What we've done is sort of automate that."

Three **Big Y Foods** Inc. stores in Massachusetts and Connecticut have been testing StopLift's Checkout Vision Systems for the past five weeks. Mark Gaudette, director of loss prevention at the Springfield, Mass., grocery-store chain, suspects that employee theft accounts for about 38% to 40% of its total losses.

"We've got pretty much a zero-tolerance policy for any folks that steal," Mr. Gaudette says. "What we're hoping is that all these technologies will help us in loss prevention and educate all of our staff."

The stores had already been using closed-circuit television and software that scrutinizes sales data for abnormal behavior or inconsistencies at the cash register, such as excessive voids or refunds. But those measures weren't enough to stem the losses.

StopLift's system works with those tools to ferret out sweethearting. For instance, if the sales-data software shows that somebody rang up too many coupons on one order, the StopLift system can analyze video from the exact moment this happened.

Big Y is still analyzing the re-

sults. So far, Mr. Gaudette has spotted some sweetheart incidents, but he has seen few cashier errors, such as giving on hard-to-scan items ins calling the manager for help.

Pricing for the techno done on a case-by-case says StopLift's Mr. Kundu says that for a typically m-volume store, monthly subscriptions currently run about \$

Of course, buying the tems isn't the only option able for small stores. E suggest that stores could fewer part-timers—who less attachment to the b and are more inclined to and conduct more-rigoro employment screenings t out potential thieves.

Employers must also h have a code of conduct, advise. For instance, g hires talks on integrity a prevention and offer anon hotlines where employes ty managers about fellow who may be stealing.

The bottom line is th ployees must recogniz have a part to play in s theft, says Joseph LaRoc president of loss prevent the National Retail Fede "Loss prevention is really body's responsibility," he:

WSJ.com

ONLINE TODAY: One of the biggest sources of fraud store face is "sweethearting" by checkout clerks—pretending to up items but actually letting pass by free of charge. Watch security video of cashiers... sweethearting to get groceries... family and friends, free at WSJ.com/SmallBusiness.