

Alison Clements

Retail Week Security Supplement

November 2005

A culture of zero tolerance towards employee theft is sweeping through the country's leading retail firms. Positive action to stamp out opportunistic stock theft, till-dipping and growing levels of refund fraud is being taken by the likes of B&Q, Argos, New Look and Boots.

Retailers are losing £1.7 billion a year through theft, according to figure from the British Retail Consortium, and almost a third of this sum £498 million— is attributed to dishonest staff, up from £282 million in 2003.

However, Centre for Retail Research director Professor Joshua Bamfield argues that when the cost of losses through sweet-hearting - collusion between a cashier and a third party - is counted purely as staff fraud, the percentage is closer to 50 per cent. "Collusion is a huge area of retail crime, which was overlooked for a long time, but is thankfully being better tackled today," he says. "The opportunity is there for retailers to cut these losses back considerably if the right steps towards detection and deterrence are taken."

An industry-wide push on external fraud has paid off in the past decade, but now retailers are turning their attentions to internal problems, says Checkpoint managing director David Nuthall. A starting point is for companies to improve their vetting procedures during recruitment to track serial offenders," he says. "The reality is that every major retailer has internal theft problems and they are no longer willing to tolerate it."

New opportunities for staff to perpetrate hidden crimes have emerged, thanks to the nature of modern retailing. For example, credit card technology gives internal fraudsters the scope to note down a friend's card number, key a refund request for it in-store and later share the spoils. There is no physical movement of product or cash. And dishonest staff who, according to research, tend to be part-time workers or those employed with a company for less than 12 months are - searching out new ways of helping themselves. "We have even heard of staff clocking up loyalty points on their own loyalty cards, when processing a customer's weekly shop," says ADT director of national accounts Ken Scotland.

Companies are now re-evaluating where money on protection is being spent. To see bigger savings, some are focusing more tightly on the antics of employees.

PricewaterhouseCoopers retail fraud investigation specialist Sterl Greenhalgh says retailers must understand where such problems take place in their store. "The approach needs to be much broader in scope, including an understanding of those process issues that contribute to shrinkage losses," he says. "More critical is the need to have a champion at senior management who can drive the initiative across the business.

"Retailers should also focus more on embedding awareness of shrinkage risks among their staff because this will require changes in all staff behaviour, not just at the store level," he says.

Because most staff fraud is now taking place at the electronic point of sale (Epos), retailers are investing in software that can spot irregular transactions, which spell suspicious cashier behaviour.

The War on Fraud

ORIS Consulting managing director Laurence King is working with New Look and Boots to tackle staff fraud. He says: "Technological solutions that link CCTV with Epos or enable data mining of Epos information to alert managers to till fraud are coming into their own. For example, if a member of staff is carrying out an unusual number of refunds, but the CCTV shows no product being passed back, you can take action. Similarly, if a cashier in a supermarket is clocking up fewer scans per minute than the average, managers are alerted to watch out for items being passed out for free. You might then use the CCIV to investigate further."

Loss prevention technology supplier IntelliQ markets software that speeds up employee fraud investigation. Product development director David Snocken explains that while retailers own records of billions of Epos transactions, this information is very difficult to store and understand. "We have operated a way to give them access to that data in a rapid, scalable way," he says.

Snocken says that fixed reporting across Epos data – automated searches that look for multiple refunds or excessive use of a card – can be useful as a starting point for investigations, but they only generate further

questions that need to be explored. The key is to allow loss prevention staff to drill down further into the data and get to the bottom of anomalies.

“This is essential, because what looks like fraud isn’t necessarily fraud,” says Snocken. “A multiple refund might be a legitimate return of four dining chairs. Or recurring transactional errors might suggest a need to retrain staff in procedures, rather than indicate dishonest behaviour.”

He urges retailers to take a holistic approach to investigations, looking beyond traditional shrinkage, because it often unearths wider operational problems that, when rectified, can save the company significant sums.

Scotland agrees that data mining is essential for retailers, not just in the fight against fraud, but also as a way of gaining competitive advantage during the consumer slowdown. “Profits may be down, but shrinkage is a constant, so losses take a larger percentage off the bottom line,” he says.

Investment in data mining and source-tagging programmes which catch out staff as well as customers – should be continuous, no matter what the trading environment, says Scotland. “The technology exists to make EAS tagging systems smart, so that the movements of high-value S products can be linked into data mining exercises,” he adds.

Checkpoint has just partnered with US software supplier Retail Expert to market an Epos analytical system called NaviStor. “Retailers don’t want data overload. The beauty of this technology is that a raft of analytical measures can be programmed in to deliver exception reporting that is relevant to that company,” says Nuthall. As different types of fraud evolve over time, the benchmarks and trends being used to spot unusual activities can be altered.

Now that the technology to detect internal fraudsters is readily available, retailers need to make cultural changes to support its use if savings are to be maximised, argues **King**. “Implanting a culture of zero tolerance needs to start with company-wide adherence to robust Epos procedures,” he says. “It’s no good having woolly guidelines about when tills should be opened and how refunds are processed and recorded, because this plants the seed of opportunity in the minds of the staff. To minimise temptation, all staff need to be aware that procedures are set in stone and any straying from the rules will be investigated.”

King says that inductions and training sessions must press home the culture of accountability. “The danger is that if a cashier is accidentally £10 down one day and sees that no one queries the discrepancy, the temptation will be there to take advantage in the future,” he explains.

King is also a strong advocate of properly supported systems of whistle-blowing within the company. This involves staff being given an incentive to report suspected dishonest behaviour using a confidential helpline. “Of course, it’s vital to demonstrate to the staff taking action that their advice is being followed up on, and the incentive should be there even if no fraudulent behaviour is discovered,” says **King**.

Zero tolerance means dismissing and prosecuting dishonest employees wherever possible and communicating these actions back to the staff. “My view is that we need to be totally open about how we are dealing with these people, which generates a deterrent in itself. Secrecy around what you’re doing to prevent staff fraud gets you nowhere,” says **King**.

He advises it is better to explain the lengths the company will take to stamp out theft through induction and training. “The temptation to steal is completely taken out of the equation,” he says. RW