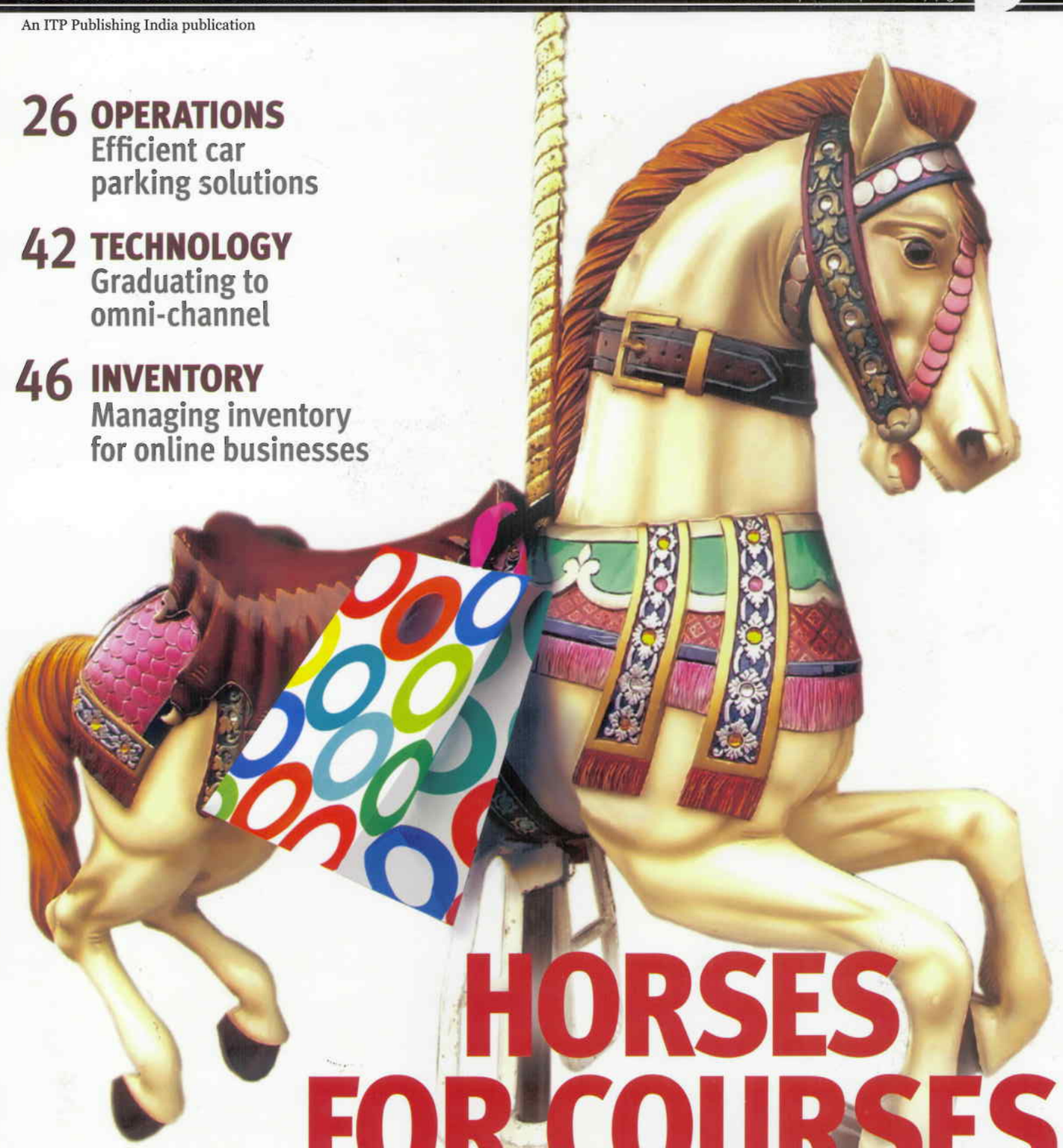
RetailToday

RIGHT FROM THE HEART OF THE INDUSTRY

JULY 2012 | VOL 01 | ISSUE 07 |₹50

An ITP Publishing India publication



HORSES FOR COURSES

Choosing the right attractions to grow footfall

Shrink rap

SHRINKAGE IS A REAL ISSUE THAT RETAILERS MUST ADDRESS. JANEES REGHELINI INVESTIGATES WHAT TO DO

"If you ask me the one most important thing top management can do to reduce shrinkage, I would have to say, 'Take an interest'."
— Peter Berlin, retail consultant.

Retailers are now more perceptive than ever to the risks involved that can lead to shrinkage. With the economic slowdown making consumers more cautious in their spending, retailers simply cannot afford anything to impact on their bottom line, prompting them to cotton on to the fact that controlling shrinkage can go some way towards helping them bolster their profitability.

There are number of areas in which shrinkage can occur, and it is one of the biggest indicators that fraud exists within a company. Fraud might exist on a global level, but other countries have developed a thorough understanding and a concrete learning curve in how to control it. Meanwhile, Indian retailers have only recently woken up to the reality of fraud, according to Arvind Gangoly, director of operations and infrastructure, at Schedulers Logistics India.

He says that grocery retail in particular is vulnerable to shrinkage, attributing this to the fact that most items that are stolen can be consumed personally or easily disposed off.

Another contributing factor comes from within, with shop-floor employees often paid low wages and working long hours. This creates an ideal mental make-up to pilfer, especially when attractive and expensive items are on display within easy reach, Gangoly explains.

According to Rohit Mahajan, partner and co-head of KPMG Forensic Services, retailers must look out for inventory shrinkage. This refers to inventory loss due to employee theft, cheating by vendors, supply-chain fraud and consumer shoplifting.

Gangoly says, "My experience is that this easily accounts for 40 per cent of total shrinkage coming from theft. However, contrary to the general belief that customers are thieves, I am of the belief that most problems lie in-house. Retail shoppers in grocery are mostly housewives, and by nature they are not

According to Mahajan, companies are investing in sensors, CCTVs, radio-frequency identification devices (RFIDs) and IT solutions. Companies are also increasingly taking legal action against employees committing fraud, he says. "Robust internal control mechanisms and an effective fraud response plan can significantly contribute towards detecting and preventing fraud. Moreover, a stringent tone at the top that exudes zero tolerance to fraud and misconduct also acts as a strong deterrent for employees and third-parties, thereby decreasing the incidence of fraud."

Companies are increasingly using data analytics to identify unusual or irregular transactions and red flags. Most companies now have whistle blower policies and ethics helpline protocols so that issues and grievances can be appropriately escalated by employees and third-parties.

Companies can also invest in specialised fraud awareness training modules for personnel, employee handbooks and codes of conduct, a centralised ethics hotline, background checks and due diligence on hiring and partnerships.

Vohra from Control Risks believes that a retailer needs to acknowledge the different challenges in the market and work out a proportionate strategy, depending on the complexities of its environment, its corporate structure, operations and technological standards. "You need to have proportionate measures and policies in place, and also have the right communication made to all the employees and stakeholders regarding your policies."

She adds that, in terms of security risks, retailers should also acknowledge the extent of this to their operation to avoid any kind of business interruption. They will need to develop proper crisis management plans and comprehensive business continuity.

Mahajan says that during one of KPMG's investigations into inventory shrinkage found at one of the outlets of a leading retail company, the consultants observed that outlet managers had colluded with delivery van drivers who were delivering goods from the company's central warehouse to its outlets. Goods sent from the warehouse had been partly offloaded along the way by the van driver. Only a portion of the goods was thus being delivered to the outlet, and those that had been offloaded were later sold to local stores at a huge discount. "The fraud remained undetected for a long time because 100 units were loaded onto the delivery van for delivery at the outlet but then 20 units were offloaded in transit and only 80 units arrived at the outlet. However, the outlet manager confirmed receipt of 100 units."

In another of their investigations, Mahajan observed that the cashier used the "void line" option on the cash register at the outlet for siphoning off cash. Under this option, all goods purchased by a particular customer are entered into the system and money is collected from the customer. "However, after entering all the items in the cash register, the void button was pressed. As a result, even though a bill was generated listing all the purchases, the bill total was zero. The net effect was that the bill would be cancelled in the system. So in this way the sale was not captured in the cash register," he explains.

Recently, Control Risks was engaged by one the largest retail chains in the world to investigate an employee in the chairman's office. "During our briefing session, we understood that the employee in question might have been receiving kickbacks for certain real estate transactions. Following our investigation, we confirmed wrongdoing by the employee and also highlighted two other areas of concern. First, we found that employees

1 Rohit Mahajan.

2 Radhika Vohra.

FRAUD IN A CASHLESS SYSTEM

— Ramesh Krishnamoorthy, head of the fraud and risk control unit at Prizm Payment Services

As the retail industry gears for the next level of growth, with the increase in adoption of electronic payments there is bound to be a shift towards cash-less systems, which have many advantages including lower transaction costs and ease of accounting. Many players in retail industry are adopting strong enterprise-wide risk management and security practices.

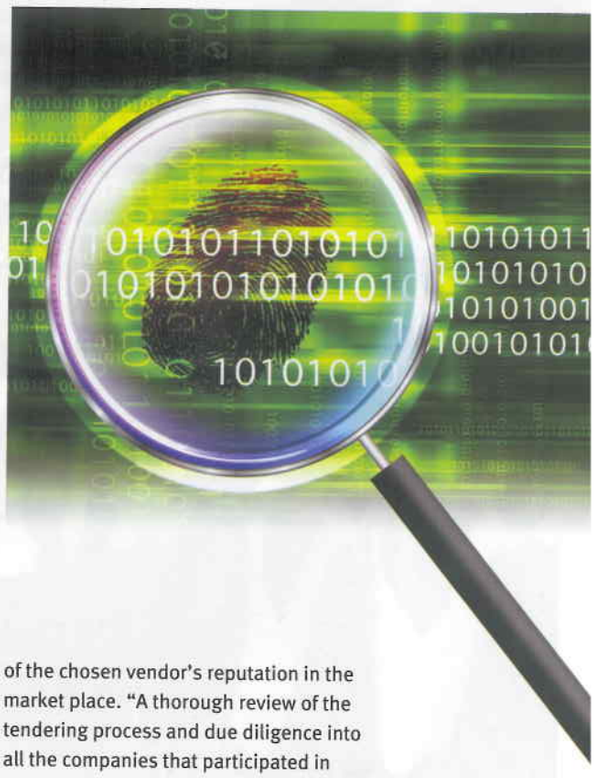
Since the growth of other industries like banking, electronic commerce, mobile commerce and e-wallets will have significant impact on the retail sector, it is important that players in the retail industry keep themselves abreast of the fraud risk or security challenges that these industries face, and work closely with them to minimise any risks.

Some examples of co-ordination with banking or the payment services industry could be PCI Compliance, procuring PA DSS-compliant payment applications, monitoring of transactions, co-ordination with fraud risk teams of banks for detection or investigation and training staff to watch out for out-of-pattern activities. This, of course, would be in addition to the strong IT security and enterprise-wide risk management controls that should be adopted by the retail industry.

The fraudsters are also getting more innovative and technologically savvy. There are many examples of ways adopted by fraudsters to defraud the customers, and one such example was the "Make a Deal" fraud in a shopping mall. The fraudsters had set up shop and had offered free mobile top-ups for Rs250 against a swipe for Rs50 on the point of sale terminal using their debit cards. The POS machine used was a skimmer and cards were skimmed along with their PINs — the fraudsters induced customers to use their debit cards and punch in the pin — and misused. While this might seem to be a simple MO, it has resulted in significant losses to customers. The fraud was detected by banks through fraud monitoring processes like online SMS alerts for transactions and transaction monitoring. Probably the process of vetting the background of such business units prior to providing space in malls will be something that can be evolved over a period of time to minimise such instances.

Monitoring of the transactions and events affecting a customer account provides business units with additional profiling capabilities and allows for early notification of suspicious activity. It also enables a more sophisticated approach to proactive fraud prevention. Resources are targeted to respond to alerts instead of "second guessing" the areas where problems might occur. This is achieved by profiling activity from the audit logs and alerting fraud professionals when unusual patterns of non-financial transactions occur.

In addition to adopting strong risk-management practices, customer and staff education on safety tips and identification of out of pattern trends is critical. This would ensure that all stakeholders in a transaction are well informed of the risks and take adequate measures to safeguard their interests leading to increased security overall.



were able to breach the company's information security controls, and second, our investigation raised questions about other employees who might have been involved in a fraud case," explains Vohra.

In another example, a leading company with headquarters in the United States was concerned about the probity of a vendor selected to procure a service for the company. "More specifically, there were concerns that the vendor was involved with another that the client had previously selected and then rejected from the tender process for non-compliance with international best practice on transaction ethics." Control Risks was asked to evaluate the company's procurement process in line with standards set out in the Foreign Corrupt Practices Act, and to establish an understanding of the chosen vendor's reputation in the market place. "A thorough review of the tendering process and due diligence into all the companies that participated in tendering revealed that two of the lowest bidders were actually founded by the same person, although on the face of it they were separate entities registered with the Indian Ministry of Corporate Affairs, but with different individuals on the board of directors. This enabled the client to take relevant action in conjunction with their legal team."

As modern retail continues to grow, there will definitely be a rise in shrinkage. With changing consumer behavior and stiff competition, fraudsters will look at devising ways to go around the system and this will lead to investing more in technology, employee education and training. Retailers must employ robust internal control mechanisms and an effective fraud response plan.

According to Gangoly: "Petty pilferage could grow into organised gangs with the necessary firepower and special skill base. Their penetration into the system in active collusion with staff cannot be ruled out. And all this can be perpetuated in a social scene whereby poverty drives people to exploit a lax law and order regime. The fact is that local police do not take this kind of pilferage seriously, especially when there are bigger issues to tackle." RT