

10 Ways Smartphones are Selling Short Your Profits

Most retailers are quick to take advantage of newer technologies, such as smartphones and tablets, to help improve areas including customer service, inventory and marketing. For example, who would have imagined a server taking your order on a small mobile device even a decade ago, or confirming in seconds if your sized medium shirt is available in another store? However as our technology gets smarter, so do the criminals who are quick to turn technology to their advantage as well.

While the vast majority of consumers and employees are honest, it only takes a few to start making a significant dent in your profits. The following examples illustrate how internal theft can occur when employees use smartphones to orchestrate a crime. This type of internal theft is most likely to occur during high-traffic times, when other employees are busy with customers or at the end of the day, when managers may be rushing to get home.



- 1 Perfect timing for a theft.** Using their smartphone, an employee can easily alert criminal partners when the ideal situation exists to commit a robbery. Maybe the manager has just opened the safe to make a night deposit, for example, or has just closed the store or restaurant for the evening. All the employee needs to do is text an outside accomplice to alert them to the ideal opportunity for a robbery.
- 2 Would you like (free!) fries with that?** Another smartphone strategy involves friends or accomplices texting an employee to ask for freebies to be included in their order. This is common in a quick service restaurant environment and especially at the drive-thru window. It can snowball into a major problem if the retailer doesn't act quickly. As one employee continues to get away with it, others will be more likely to adopt a similar practice with their friends.
- 3 Special orders on the side.** Theft can also occur when a cashier doesn't ring in the order using the main point of sale (POS) register system, but instead uses a smartphone to tally up the cost. This type of theft occurs most often at the end of the night, when an employee is closing down a register and an order can be given verbally to the kitchen. This theft is not detectable using exceptions and transaction-based reporting methods. In this case, managers will need to rely on their video surveillance to prove a crime took place.
- 4 Out of sight, out of mind.** Mobile phones can be used as a container for criminals to hide stolen cash. Bills can be hidden in a slide phone, or even tucked into the back of a phone case serving as a convenient, hidden compartment.
- 5 Bad math.** Another method of fraud involves employees who are under-ringing items and keeping a tally on their phone so they know the exact amount they can pocket at the end of the night. A \$3 drink is entered at \$1, and the employee steals the difference. The phone is used as a calculator, tallying the fraudulent transactions.



- 6** **Cooking up a little something special.** Two or more employees can use texting to secretly communicate with each other and come up with mutually beneficial “deals.” In one case, the waiter and chef were colluding to provide extras to customers, who then tipped generously. The waiter and chef split the profits.
- 7** **Labor drain.** One of the most common ways phones can rob retailers is through employee misuse during working hours or theft of time. Employees who are talking, texting, gaming or surfing the web when they should be working are a drain on their employer's bottom line.
- 8** **Inappropriate share.** The cell phone is a conduit for photos and video — but not everything is appropriate to share at work. If an employee is showing or distributing questionable content in the workplace, this can be considered harassment, which can be a major cost to an employer if it escalates to a labor dispute or lawsuit.
- 9** **Data breach.** Many employees have access to confidential company information, such as internal memos, financial records, or even the location of a safe. The cell phone can be used to share this information, and the results can be costly for the employer.
- 10** **High cost of convenience.** Mini adaptors that allow smartphones or tablets to process credit card payments can also be used to commit theft. Fraudsters hack the technology so their phone steals data from a credit card's magnetic strip. In some cases an employee will simply use the phone to snap a picture of the card number and security code to use at a later time.

Learn more about March Networks Retail Solutions

March Networks® is a leading provider of intelligent IP video solutions used by retailers worldwide to enhance security, improve store operations and reduce shrink significantly. Our Retail Solutions include centralized video management, high-performance hybrid NVRs, IP cameras, video analytics and powerful software applications purpose-built to speed retail LP investigations and strengthen case evidence.

To learn more, contact us at
1.800.563.5564 x5448 or visit us at
www.marchnetworks.com.

Keeping Your Loss Prevention Strategy Up-to-Date

Retailers can protect their assets with an up-to-date loss prevention strategy that includes a strong mobile device policy. The policy should clearly outline when and where phone or tablet use is acceptable at work, if at all. Some retailers simply advise employees to leave the devices at home. If mobile devices are not allowed at work, storage lockers should be provided so employees can keep them locked up.

Stop Shrink Faster

Retailers can use intelligent video surveillance to detect fraud sooner, stop it faster and ensure that their loss prevention policies are being followed. Clear video evidence can also play a critical role in successful prosecutions.