Loss Prevention Checklist - Managers

Here are some of the steps managers can take to reduce the risk of theft and other forms of shrinkage. Also review the checklist for sales associates so you know how everyone in your operation can aid in loss prevention.

EXTERNAL THEFT

- [ ] **Maintain appropriate staffing.** More employees present on the salesfloor will give thieves fewer opportunities. Maintaining staffing may be challenging during a difficult economy, but a low staffing level could make you a prime target for shoplifters.
- [ ] **Shoot the outs.** Scan for out-of-stock inventory on a weekly basis. This will alert you to what areas have been shoplifted and determine shrinkage rates.
- [ ] **Have a plan for regular salesfloor maintenance.** Give employees maintenance tasks to do during downtime, such as filling, fronting, facing and dusting merchandise. The plan should create as much coverage on the salefloor as possible, which will help discourage shoplifters.
- [ ] **Post a greeter at the store front.** A greeter, which could also be the cashier, will ensure every customer is recognized and helped.
- [ ] **Maintain lighting.** Make sure there are not dimly lit areas of the salesfloor and that all lights are in working order.
- [ ] **Minimize hiding spots.** Eliminate blind areas on the salesfloor by installing mirrors in corners and remerchandising as necessary.
- [ ] **Have adequate key coverage.** Give multiple employees keys to locking cabinets or peghooks. Every employee should be able to quickly obtain a key so customers don't have to wait to purchase locked items.
- [ ] **Have a verification policy for online orders.** Create a policy where staff check the receipt and ID of anyone picking up an order in store or coming for curbside delivery. Have staff sign off on orders that leave the backroom.

INTERNAL THEFT

- [ ] **Create a positive culture.** Employees who steal often don't feel a part of the team, are disgruntled for some reason or are unhappy with their job. Create a positive culture where employees work for the best interests of the company.
- [ ] **Refine the hiring process.** Thoroughly screen new hires, including background checks. Also have a thorough onboarding process so each employee quickly starts to feel a part of the team.
- [ ] **Establish cash management policies.** Limit cash on hand and conduct regular cash drops to the safe. Also rotate cashiers and change their cash drawer assignments regularly to deter collusion.
- [ ] **Use door controls.** Keep overhead doors locked and put alarms on emergency exit doors to prevent unauthorized use.
- [ ] **Establish a trash policy.** Have a designated person remove trash at certain times of the day, use clear trash bags and flatten discarded boxes. This prevents hiding merchandise that can be retrieved later.
- [ ] **Rotate cashiers.** Rotate cashiers and change their cash drawer assignments regularly to deter collusion.
- [ ] **Establish opening/closing procedures.** Always have two people present for the opening and closing of the store. This will also help with safety.
- [ ] **Take loss prevention training.** Understand the warning signs that indicate an employee might be stealing, the different types of theft and how to respond by taking loss prevention training. NHPA's course in Internal Theft Prevention can equip you to deal with employee theft.
- [ ] **Review your return policy.** Ensure your return policy will minimize fraudulent returns and make sure all employees are trained how to properly conduct a return.
- [ ] **Managers ring up employee purchases**. If an employee wants to make a purchase from the store, require a manager to ring up the sale. This provides accountability and extra protection against fraud.

CYBERSECURITY

- [ ] **Train employees.** Have all employees take training in how to protect their personal information and identify potential threats. There are resources on **cisa.gov**.
- [ ] **Think before you click.** Don't click on unsolicited emails or text messages that ask you to update your account information. Double check email addresses and URLs to be sure they're legitimate. Scan any attachments before you download.
- [ ] **Use two-factor authentication.** Having two ways to verify your identity can help protect you from fraud and stolen accounts.
- [ ] **Think before you tell.** Don't share personal or business information online or over the phone, including usernames, passwords, credit card information, date of birth, social security number and mother's maiden name.
- [ ] **Beware of spoofing scams.** Spoofing occurs when a criminal uses an email address, sender name, phone number or website URL that looks similar to a legitimate one in order to manipulate individuals to download software, send money or share personal information, which are all common phishing schemes.
- [ ] **Beware of phishing scams.** Phishing can also take place over the phone, voicemail, email or voice over internet protocol, which is known as vishing, and can also happen through text messages, called smishing. Pharming, another type of phishing, is when a criminal installs code into your computer to redirect you to a fake website.

PAPER SHRINK

- [ ] **Perform regular cycle counts and shoot the outs often.** Don't wait until the end of the year for an inventory checkup so you can quickly identify causes of shrink. Shoot the outs regularly to help identify theft hot spots.
- [ ] **Double check all deliveries.** Verify deliveries against purchase orders to prevent overbilling and theft by vendors. Use two employees so they can double check each other's work.
- [ ] **Establish backroom security protocols.** Establish secure receiving and unloading procedures to prevent unauthorized removal of goods. Keep a log of all incoming and outgoing shipments.

Loss Prevention Checklist - Owners

Here are some of the steps retail owners can take to reduce the risk of theft and other forms of shrinkage. Also review the checklist for managers and sales associates so you know how everyone in your operation can aid in loss prevention.

EXTERNAL THEFT

- [ ] **Post deterrent signage.** If it applies to your store policy, post clear signage stating that shoplifters will be prosecuted.
- [ ] **Establish a shoplifter response policy.** Have a clear policy that outlines how employees should respond when they see a theft. It should include how and when to confront a shoplifter and place top importance on the safety of staff and other customers.
- [ ] **Prosecute theft.** It may not always be worth it to prosecute a shoplifter, and laws in some areas have made it more difficult. Just be sure to weigh all the consequences. Prosecuting a shoplifter sends a message that theft is not tolerated at your business, it could deter future shoplifters and could also deter employees from trying to steal from you.
- [ ] **Use a camera system.** A visible camera system will first act as a deterrent to shoplifters. Install them strategically to cover all areas, including entrances, exits and high-value product sections. Use high-quality and high-resolution cameras. Inspect cameras regularly to ensure proper operation.
- [ ] **Use EAS or RFID technology.** Electronic article surveillance (EAS) and radio frequency identification (RFID) are common inventory tracking systems and effective at deterring theft.
- [ ] **Eliminate blind spots.** Merchandise the salesfloor so that there are wide, easy to navigate aisles and no blind spots. If blind areas are unavoidable, install mirrors so it's easy to see those areas from a distance.
- [ ] **Lock high-theft items.** Store high-theft items in locked cases or display behind the sales counter. You can also display models of some items like power tools on the salesfloor while storing inventory in the backroom.
- [ ] **Secure the perimeter.** Install fencing or barriers to prevent unauthorized entry after hours to storage and retail areas. Install alarms and motion detectors to alert security personnel in case of unauthorized access. Test alarms regularly to ensure reliable operation.
- [ ] **Keep thorough records.** Create incident reports of each theft and be ready to share with local law enforcement. Have a complete report with all the information an officer might need.
- [ ] **Invest in your community.** An increase in crime is often a result of deteriorating conditions in the community. Get involved in civic organizations, the local chamber of commerce or small business groups to learn how others are fighting crime and how you can address local issues that may be contributing to a higher crime rate.
- [ ] **Collaborate with other businesses.** Sharing trends or information on repeat offenders with other small businesses can help you be better prepared to face threats to your own operation.
- [ ] **Conduct regular assessments.** Seek feedback from employees and customers to identify potential vulnerabilities. Assess your risks and update your loss prevention strategies accordingly.
- [ ] **Monitor legal compliance.** Stay up-to-date with local and federal laws related to loss prevention and security measures.

INTERNAL THEFT

- [ ] **Conduct regular cash drawer audits.** Schedule regular "surprise" audits of the cash drawer that will include all cashiers. This is one of the easiest ways to determine if an employee is stealing.
- [ ] **Conduct integrity shops.** Conduct this test if you suspect an employee is stealing. An integrity shop is when someone poses as a normal customer and uses exact change for a purchase to see if the employee records the sale properly.
- [ ] **Review employee compensation.** Employees who are paid a fair and competitive wage may be less likely to feel you "owe" them something. Receiving a competitive wage will also help them feel valued and less likely to steal.
- [ ] **Use exception-based reporting.** Reports from your POS system can provide information on all of the transactions that take place in your store, including cash refunds, no sales, voided sales, suspended sales, employee purchases and commodity group sales. This data will help you quickly spot employees who are possibly stealing from you.
- [ ] **Check for markers in the cash drawer.** Dishonest employees often keep track of cash they intend to steal by using markers or tick marks in the cash drawer. Markers can include paper clips, rubber bands and marks on the register.

CYBERSECURITY

- [ ] **Check your insurance policy.** Ask your insurance company about cyber insurance. Make sure it is adequate to cover a business of your size and will meet your needs in case of an attack.
- [ ] **Use antivirus software and keep systems updated.** Install antivirus software on every computer in the business. Process software and OS updates regularly, as updates often contain patches for known viruses.
- [ ] **Train employees.** Have all employees take training in how to protect their personal information and identify potential threats. There are resources on **cisa.gov**.
- [ ] **Limit admin access**. Limit administrator access to company machines only to those individuals who need it. Encourage them to use this access only when necessary and to have a second person verify new software downloads. Only give employees the minimum level of access they need to do their job.
- [ ] **Store data on the cloud.** Use cloud-based servers for backup of POS data and to create redundancies that will give you something to fall back on in case of a cyber attack. You may also choose to have an onsite physical server that backs up data on company computers.
- [ ] **Think before you click.** Don't click on unsolicited emails or text messages that ask you to update your account information. Double check email addresses and URLs to be sure they're legitimate. Scan attachments before you download.
- [ ] **Use two-factor authentication.** Having two ways to verify your identity can help protect you from fraud and stolen accounts.
- [ ] **Think before you tell.** Don't share personal or business information online or over the phone, including usernames, passwords, credit card information, date of birth, social security number and mother's maiden name.
- [ ] **Beware of spoofing scams.** Spoofing occurs when a criminal uses an email address, sender name, phone number or website URL that looks similar to a legitimate one in order to manipulate individuals to download software, send money or share personal information, which are all common phishing schemes.
- [ ] **Beware of phishing scams.** Phishing can also take place over the phone, voicemail, email or voice over internet protocol, which is known as vishing, and can also happen through text messages, called smishing.

PAPER SHRINK

- [ ] **Perform regular cycle counts and shoot the outs often.** Don't wait until the end of the year for an inventory checkup so you can quickly identify causes of shrink. Shoot the outs regularly to help identify theft hot spots.
- [ ] **Double check all deliveries.** Verify deliveries against purchase orders to prevent overbilling and theft by vendors. Use two employees so they can double check each other's work.
- [ ] **Establish backroom security protocols.** Establish secure receiving and unloading procedures to prevent unauthorized removal of goods. Keep a log of all incoming and outgoing shipments.
- [ ] **Review invoices for unusual items.** Double check vendor bills to make sure you're not getting billed for unusual items. Make sure you're not getting billed for something you don't normally stock.

Loss Prevention Checklist - Sales Associates

Here are some ways sales associates can prevent retail theft. Deterring and preventing theft makes the store safer and helps keep the business profitable, which can result in more opportunities and benefits for you.

THEFT

- [ ] **If you see something, say something.** If you notice suspicious behavior from another employee or from a customer, or see someone stealing, report it immediately to your supervisor.
- [ ] **Greet each customer.** Establish eye contact and greet every customer who walks in the door. Then ask what project they are working on today. This will send the message you are watching and is the first step towards discouraging would-be shoplifters.
- [ ] **Make customer service the No. 1 priority.** Shoplifters prefer to be alone and unnoticed when they do their work. Don't hover, but stay nearby and periodically check in on customers to ask if they need help.
- [ ] **Don't congregate on the sales floor.** One of the ways to deter shoplifters is to have eyes on as many areas of the store as possible. You can't do that if you spend excessive time chatting with other employees in groups on the salesfloor.
- [ ] **Maintain the salesfloor.** Spend down time maintaining the salesfloor; dust, fill, front and face merchandise. In addition to creating a more appealing shopping environment, by moving throughout the salesfloor, you'll take away the privacy of shoplifters who would rather be alone.
- [ ] **Take loss prevention training.** The loss prevention training prescribed by your managers will help you understand how to spot a potential shoplifter and what to do when an incident occurs.
- [ ] **Report opened packages.** Opened packages on a shelf or peghook may indicate a shoplifter has been at work. Report these immediately to a supervisor.
- [ ] **Report out-of-stock items.** If you notice an empty peghook or shelf, report it to your supervisor. Not only will you want to make sure the product is reordered, sometimes an empty peghook indicates theft, and reporting it will identify theft hotspots.
- [ ] **Follow store policies.** When a shoplifting incident does occur, follow store policy. The best practice is usually to observe rather than detain. Report what you observed to a manager so they can fill out an incident report.
- [ ] **Know who has the keys to merchandise locks.** Locking up merchandise helps deter theft, but don't let it become a customer service issue. Be able to produce keys to retrieve merchandise customers want to buy so they have the best service experience possible.
- [ ] **Know the hot items.** Know what items in the store are most commonly stolen. Keep a closer watch on them.
- [ ] **Verify online orders.** When a customer comes to pick up an online order, ask for a receipt and ID for verification before handing over the order.
- [ ] **Double check all deliveries.** Verify deliveries against purchase orders to prevent overbilling and theft by vendors. Partner with a co-worker so you can check each other's work.
- [ ] **Follow backroom security protocols.** Follow secure receiving and unloading procedures to prevent unauthorized removal of goods. Keep a log of all incoming and outgoing shipments.

THEFT PREVENTION FOR CASHIERS

- [ ] **Scan each piece.** Scan individual items, even if there are several of the same item. Some items will look similar and differ only by size or color. Each size or color will have its own SKU. Each SKU is tracked individually.
- [ ] **Watch the register screen.** Double check that what you are scanning matches what appears on the register screen. Price swapping is one method of stealing where thieves swap the barcode of a lower priced item and place it on a higher priced one.
- [ ] **Look in the basket.** Make sure the customer hasn't left anything in the shopping basket, either unintentionally or intentionally. One method of shoplifting is to purchase some items while leaving others in the basket.
- [ ] **Look inside items such as toolboxes.** Shoplifters may try to hide smaller items inside larger items they purchase. Instead of telling the customer you're suspicious of them, say you want to look inside to make sure they have all the correct pieces.
- [ ] **Check manual entries.** Be especially careful of SKUs you enter manually, such as for bagged goods that are picked up outside. Double check that the quantity and code are correct.

CYBERSECURITY

- [ ] **Take cyber security training.** Use training provided by your supervisor to learn to identify online threats to your personal and company data.
- [ ] **Think before you click.** Don't click on unsolicited emails or text messages that ask you to update your account information. Double check email addresses and URLs to be sure they're legit. Scan any attachments before you download.
- [ ] **Use two-factor authentication.** Having two ways to verify your identity can help protect you from fraud and stolen accounts.
- [ ] **Think before you tell.** Don't share personal or business information online or over the phone, including usernames, passwords, credit card information, date of birth, social security number and mother's maiden name.
- [ ] **Beware of spoofing scams.** Spoofing occurs when a criminal uses an email address, sender name, phone number or website URL that looks similar to a legitimate one in order to manipulate individuals to download software, send money or share personal information, which are all common phishing schemes.
- [ ] **Beware of phishing scams.** Phishing can also take place over the phone, voicemail, email or voice over internet protocol, which is known as vishing, and can also happen through text messages, called smishing. Pharming, another type of phishing, is when a criminal installs code into your computer to redirect you to a fake website.