Asset Protection - Eyes Open for Scams

Stay Sharp - Spot the Scam!

Scammers are always finding new ways to deceive employees, but with your vigilance, we can stay one step ahead. Here's how you can clearly see the scams and help protect our stores:

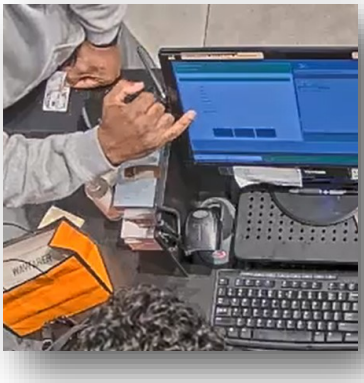
Cash Scams

- Scammers **confuse the cashier** with multiple/large bills and change requests to **underpay**.
    - **LOOK OUT**: For **large cash** purchases where customers continue to touch the money and arrange stacks of bills.
    - **See it, Stop it**: Always be the **last person to count** the money before it goes in the register and deny change requests. Take your time, and don't hesitate to **recount**. Create **distance** between **you** and the **customer**.

Phone Scams

- Scammers attempt to **manipulate employees** into providing sensitive information or funds, often through **gift cards/credit card refunds**. They could be posing as **Asset Protection** or **IT** (with register issues).
    - **LOOK OUT**: For callers stating the store is **under investigation/audit**, and that **money** needs **to be removed** from the store to make a payment/deposit. *(Remember: **No one** will **ever** call the store and ask an employee to **remove money,** or **tender** a transaction as **cash.**)*
    - **See it, Stop it**: Say "**No**" and end the call. Use resources available in the store to contact the appropriate department to verify the call. *(Remember: Make sure your call list stays updated.)*

Credit Card Scams



- Scammers trick employees into letting them **manually enter stolen credit card** numbers. This results in a chargeback, the **loss of the sale**, and creates shrink.
    - **LOOK OUT**: For **damaged cards** that **do not chip/swipe** correctly, failed **Apple Pay** attempts, or **individuals** that **say** they **work for the company** and know the systems.
    - **See it, Stop it**: **NEVER** use the **phone order** function for customers in the store. If the card cannot chip/swipe, ask for another form of payment. *(Remember: Legitimate phone orders are only for **verified customers** who are in the system.)*

Have Clear Vision

- Trust yourself; if it **doesn't feel right**, it probably isn't.
- Contact your **manager** if you have any doubt**.**
- Check **Smartly/brand communications** for policies.
- Report suspicious behavior to **Asset Protection.**

Check Scam Information on the AP Toolkit

Asset Protection