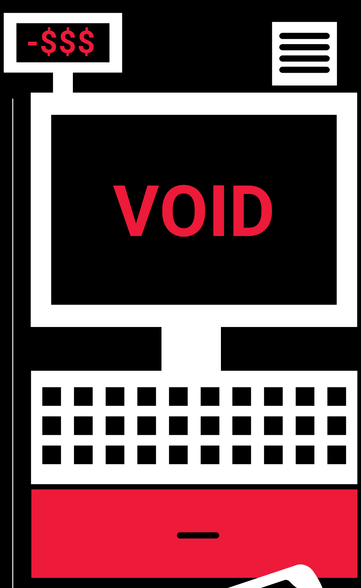
COMMON POS THEFT SCAMS



UNAUTHORIZED Discounts

Applying a phony discount, pocketing the difference

UNAUTHORIZED Voids

Issuing a fictitious void for a real transaction, pocketing the money

UNAUTHORIZED Refunds

Issuing a fictitious refund for a real transaction, pocketing the money

UNAUTHORIZED Comps

Comping items claiming customer dissatisfaction, keeping the cash

EMPLOYEE DISCOUNT ABUSE

Using personal meal discount for friends and family

SHORT-RINGING

Ringing up something less expensive to pocket the difference

NO SALE, OPEN CASH DRAWER

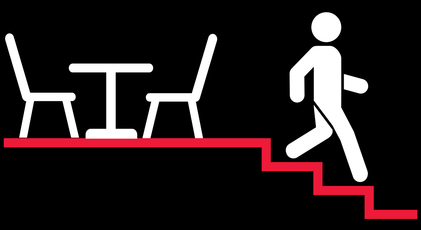
Using "No Sale" to make change, taking money from open drawer

FLOATING RECEIPTS

Reusing receipts from transactions to steal money from future transactions

PHONY WALKOUTS

Accepting payment then saying the customer walked out without paying



DETECTION VS. PREVENTION

To **fight** employee theft, **rapid detection** is critical

Nearly **one-third** (29%) of internal theft cases in the U.S. went **undetected** for **almost 5 years**

Detection of theft after the fact entails lengthy and expensive investigations to uncover, document and prosecute.

HOW CAN FINGERPRINT BIOMETRICS AT THE POS HELP?

With fingerprint biometrics, fictitious transactions can't be performed using shared or stolen credentials. Everything employees do is **irrefutably tied to their identity**, so crooks won't go undetected for long.

That's the power of biometrics.

Crossmatch.com

CROSSMATCH®
The world identifies with us.™