



# 4 Simple Data Behaviors that Give Away Self-Checkout Fraud



Zebra  
**Prescriptive Analytics**<sup>™</sup>  
Powered by Zebra Savanna<sup>™</sup>





In this ebook we will examine:

- Why data analysis is the most effective way to identify self-checkout fraud
- 4 telltale data behaviors that indicate fraud
- How data analytics can help you identify and eliminate retail fraud



# Introduction

Self-checkout can be a great way for retailers to both speed up the checkout queue and reduce labor cost. At the same time, it's important to ensure self-checkout's risk of shrink does not exceed its benefits – a remarkably tough challenge given self-checkout's anonymity and shoplifters' determination to steal. Even the most high-tech CCTV systems and report-based solutions do little to stop the modern retail criminal's subtle, crafty schemes to bypass security protocols.

By far the most effective way to identify and stamp out self-checkout fraud is by looking to your data. Data cannot be altered, manipulated or bypassed the way CCTV footage can. By applying a data analytics solution, like prescriptive analytics, to your self-checkout data, you can identify the subtle yet telltale data behaviors that indicate fraud and automatically direct your people to take action.

Here are four data behaviors a good analytics solution can instantly recognize as self-checkout fraud:







# Four data behaviors used to recognize self-checkout fraud

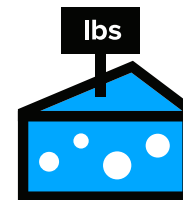
1

Cheap-item movements exceeding supply



2

Suspicious weights



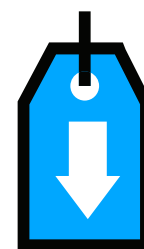
3

Low-value orders



4

Above-average markdowns





# Behavior #1



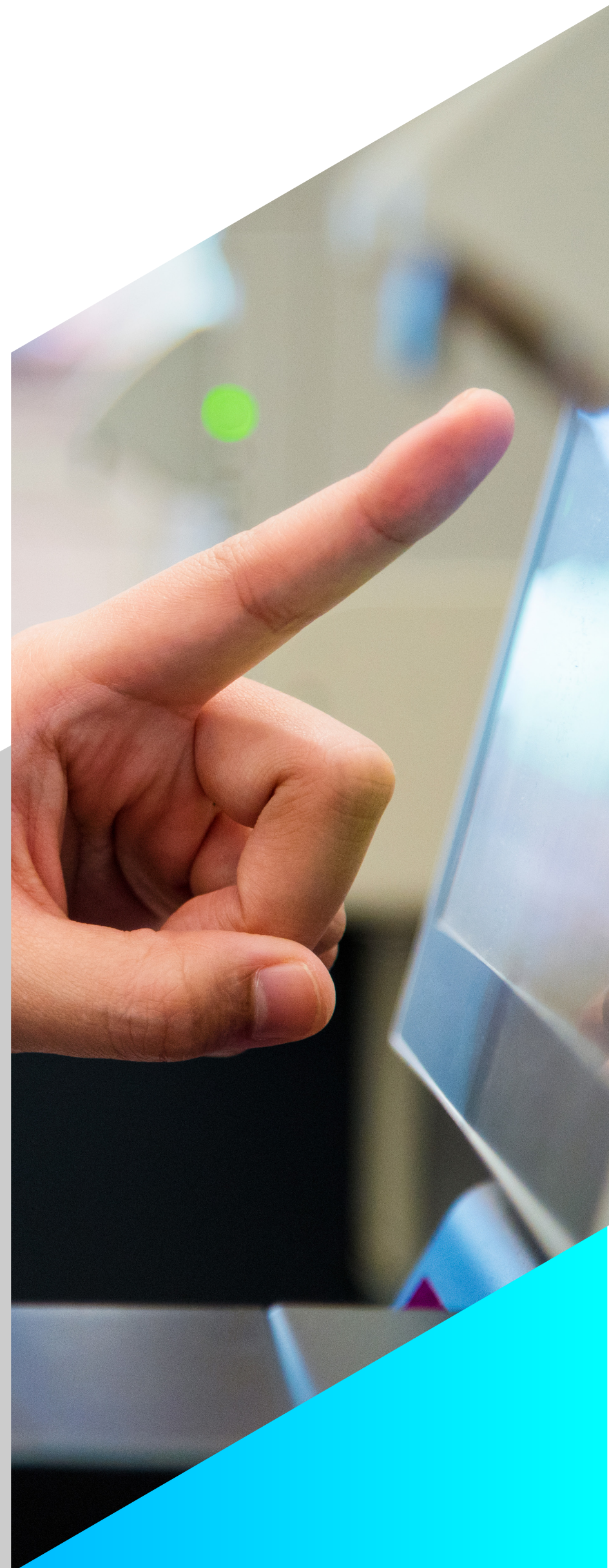
## Cheap-item movements exceeding supply

One of the most classic self-checkout fraud schemes, this methodology involves the customer entering the PLU code for something inexpensive (often bananas at 50¢/lb) and weighing up something pricier, like a rack of lamb, a jug of olive oil or a six-pack of energy drinks. To deter this, most self-checkout registers are programmed to loudly announce “*bananas!*” whenever the customer enters the code, to alert the self-checkout attendant. But attendants can get busy, and when they do, this stopgap amounts to nothing.

Data provides a surprisingly simple indication of this fraud scheme. Numerous retailers have their analytics solutions monitoring product movements of their least expensive items sold

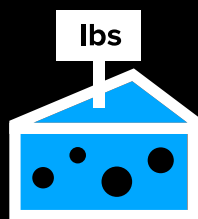


by weight, especially bananas. The right solution will instantly flag when a store, region or entire organization appears to be selling more bananas than it has in stock and alert the right asset protection (AP) investigator to follow up. If the excess quantities appear to have been purchased via the self-checkout line, this is further assurance that fraud is at play.





## Behavior #2



### Suspicious weights

Product switch-outs like the banana scheme can also be unveiled by monitoring data around item weights. The key to this analysis is identifying items whose weight seems inconsistent with the product the customer selected at the self-checkout register.

For example, consider a customer who scans a pricing sticker for beef tenderloin at self-checkout. The price added to the customer's order is just \$3. An analytics solution like prescriptive analytics will instantly identify that the store does not sell beef tenderloin in such small quantities and alert the self-checkout attendant to audit the customer's order. Chances are that when making this label, an employee or customer actually weighed a lightweight object



like a piece of fruit or a box of gloves instead of the actual product of purchase. The logic is that the customer can show any suspicious employees that the product is in fact on the receipt, and hope that the latter does not notice the suspicious weight. With data analytics on the case, the customer is much less likely to get away with the theft.





# Behavior #3



## Low-value orders

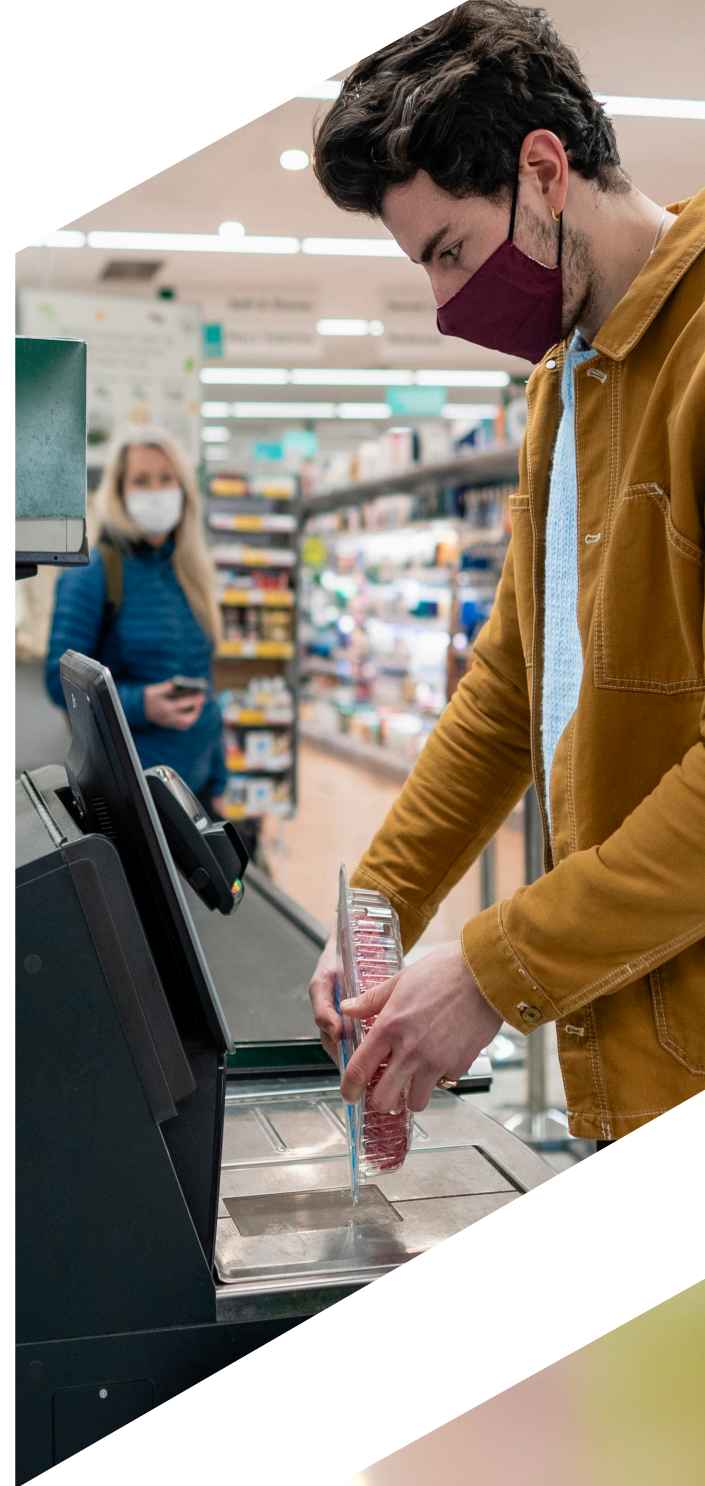
Self-checkout orders of less than one dollar are exceptionally rare, making them a prime indicator of fraud. What typically happens is a customer pays for a single, inexpensive item at self-checkout, then simply bags a full cartload of groceries before walking out of the store. In their mind, the fact that they are walking out with a receipt will help them avoid notice.

Many retailers are using prescriptive analytics to monitor self-checkout transactions for low-value orders, typically less than one dollar. Any order meeting the retailer's specified criteria is sent to the appropriate AP manager for investigation.

A regional American grocery chain recently used a similar logic to capture a self-checkout thief. Specifically, they configured their prescriptive analytics solution to flag multiple self-checkout

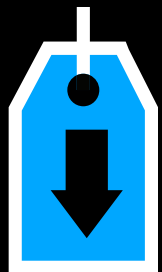


orders of less than a dollar, all on the same tender card, at the same store, and for the same item. The solution quickly flagged a customer who was ringing up 25¢ packets of Kool-Aid at self-checkout, and then simply walking out with hundreds of dollars in unpaid diapers, soda and snack foods. Thanks to the timely alert, he was caught and now faces felony theft charges.





## Behavior #4



### Above-average markdowns

For many retail criminals, the prospect of getting 50% off an item is irresistible. Thus many turn to markdown stickers, especially those placed on seasonal candy, as a means of getting illegal discounts. Often it's as simple as carefully peeling the stickers off designated items and placing them over more expensive items' barcodes. Naturally, to avoid suspicion at the register, these illegal markdowns will be rung up via the self-checkout line.

You can make this work in your favor by setting an analytics solution to monitor markdowns going through self-checkout. The right solution will determine the average value and frequency of these markdowns at each store and at various times of day. From there, it's easy for the solution



to identify when the value or frequency of self-checkout markdowns exceed the average, and alert the right person to investigate.

Some solutions, like prescriptive analytics can even correlate the excessive markdowns with other findings, such as when certain self-checkout attendants are on duty, when managers are on vacation, or when specific products are on sale. This added precision saves significant investigative time, helping you resolve more cases, more quickly.







For more information on using prescriptive analytics to identify retail fraud, visit [www.zebra.com/prescriptiveanalytics](http://www.zebra.com/prescriptiveanalytics) or email us at [inquiry4@zebra.com](mailto:inquiry4@zebra.com).

# Zebra Prescriptive Analytics™

Powered by Zebra Savanna™

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corp., registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2020 Zebra Technologies Corp. and/or its affiliates. All rights reserved.