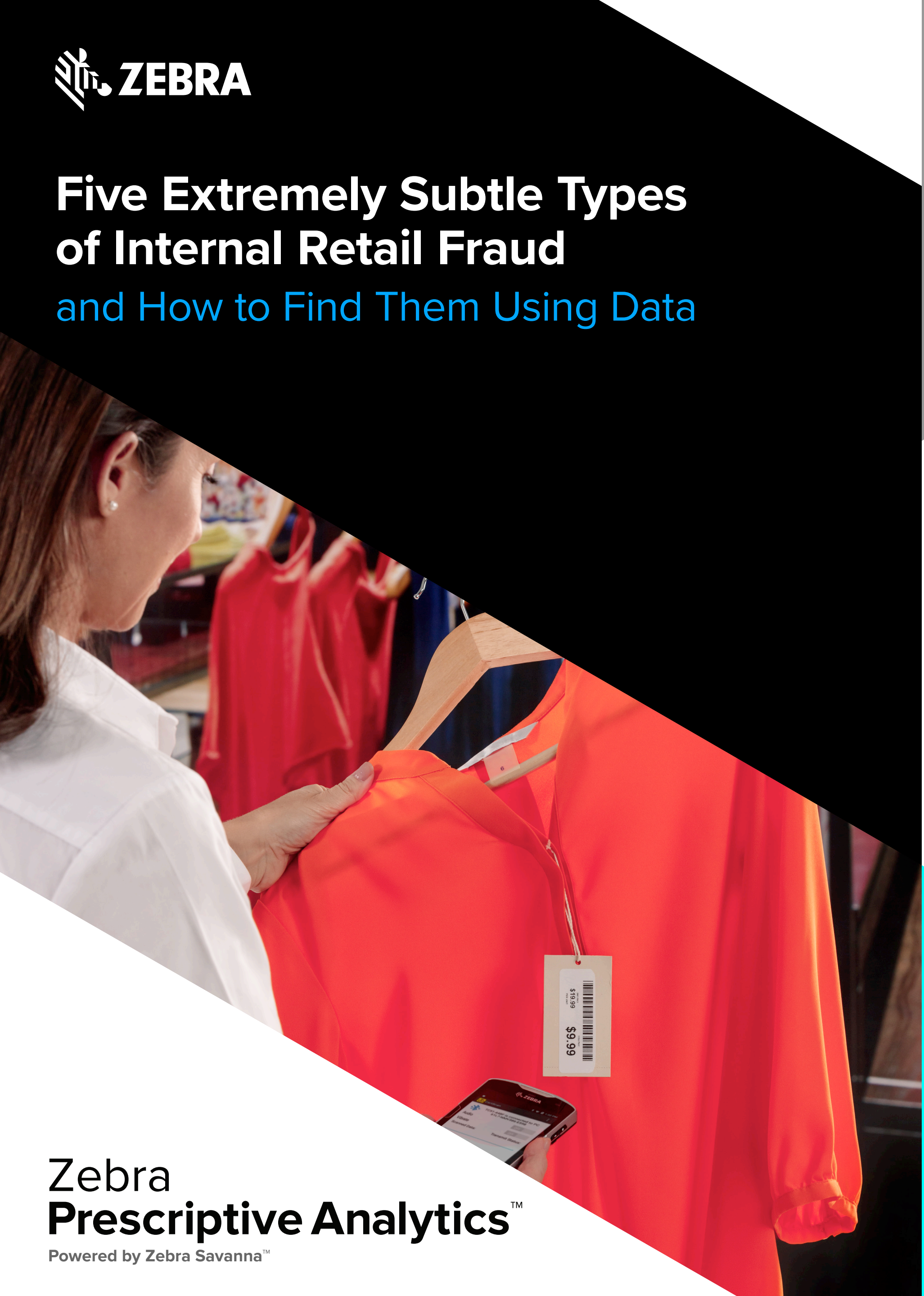
Five Extremely Subtle Types of Internal Retail Fraud

and How to Find Them Using Data



Zebra
Prescriptive Analytics™

Powered by Zebra Savanna™

In this ebook we will examine:

- Five types of internal retail fraud
- The data behaviors that reveal them
- How to identify and stop them with advanced analytics

Introduction

Fraud is no joke in the brutally competitive retail industry. With margins stretched razor-thin by aggressive pricing wars, retailers need to crack down on cash loss due to fraud, especially when it is being committed by their own employees. In addition to having intimate knowledge of retailers' security procedures (and by extension, how to circumvent them), employees have access to risky register functions and unprotected merchandise in back rooms, in the warehouses and on trucks. This insider knowledge makes it very difficult to detect internal fraud, even with CCTV and other security measures.

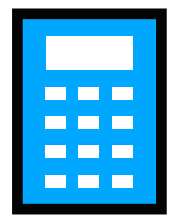
To combat this challenge, many retailers are leveraging their data to identify suspicious activity by employees. They know that data cannot be manipulated and the right advanced analytics solution, like prescriptive analytics, can identify specific behaviors that indicate fraud and other activities that erode margins. This ebook will discuss five extremely subtle examples of employee fraud and the telltale data behaviors that prescriptive analytics can identify.


ZEBRA

Five Extremely Subtle Types of Internal Retail Fraud

1. Sliding

2. Unauthorized manager PIN usage

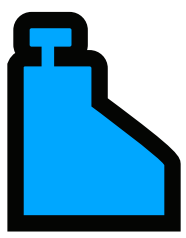


3. Loyalty fraud

4. Price switching and sweethearting

5. E-commerce customer service fraud

Fraud #1



Sliding

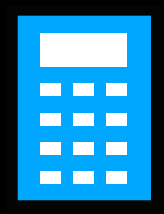
Sliding occurs when a cashier passes an item over a scanner while purposely obscuring the barcode. The customer (typically an acquaintance) is then free to bag the item and leave the store without paying for it. Confirming this activity as fraud can be tricky, whether in CCTV footage or even in person. Even if you can confirm a missed scan, it’s difficult to prove that the action was in fact sliding and not just a simple, naive mistake.

Data can help. One way to identify sliding is to analyze your per-minute or hourly scan rates for individual cashiers. This process starts with a good analytics solution like prescriptive analytics, which can “cluster” (i.e. group

based on similar characteristics) cashiers and stores to determine benchmark averages for certain KPIs like scan rates. Any cashier whose scan rate drops below the benchmark by three standard deviations is flagged as a potential slider.

Such findings are considered particularly suspicious if they occur during “high-risk” time periods (e.g. lunch hours, shopping rushes, supervisor breaks or days off, etc.). Prescriptive analytics takes circumstances like this into account when identifying fraud.

Fraud #2



Unauthorized manager PIN usage

To mitigate risk around voids, price overrides and other activities, many retailers require supervisors to enter a personal identification number (PIN) to authorize them. Unfortunately, a PIN can easily be abused if a cashier memorizes it or a manager shares it to save time. This behavior must be stopped or a single cashier could steal thousands of dollars in cash or merchandise.

There are multiple ways to identify PIN fraud using data, such as human resources data. The most advanced analytics solutions integrate data from multiple applications or vendors. This empowers you to easily visualize these separate data sets and any insights within a single interface.

To detect unauthorized manager PIN usage, you can deploy a “pattern” (an algorithm that looks for specific data behaviors) that cross-analyzes

you any time a manager's PIN is used when its owner was not scheduled to work.

Alternatively, if your managers carry mobile computers with location services, an analytics solution can check the proximity of the manager to any register at which their PIN was entered. If the manager was working elsewhere in the store at that time, asset protection is alerted.

Fraud #3

Loyalty fraud

Most retailers allow customers to enter a phone number at checkout to look up their loyalty accounts. Cashiers have been known to take advantage of this service by secretly entering their own phone numbers instead of the customer's, thereby stealing their loyalty rewards. Unless the customer is especially diligent about counting their loyalty points, this behavior often goes unnoticed.

The aforementioned benchmarking and clustering capabilities of advanced analytics can find evidence of loyalty fraud within your data. They work by analyzing your associates' own loyalty accounts for excessive points. An employee account that suddenly begins accumulating points at a faster-than-average rate is flagged for investigation.

Another type of loyalty fraud involves employees “phishing” for phone numbers associated with high-point accounts and then using the points to purchase merchandise or fuel at a massive discount.

Similar to the previous example, the right solution can be configured to flag customer accounts with an unexplained surge in point spending, especially when the purchases are known theft targets like electronics, fuel or gift cards. These accounts may have been hacked in some way and should be investigated.

Fraud #4

Price switching and sweethearting

This method is a particular favorite of organized retail crime (ORC) rings. It often involves employees in departments that sell items by weight, like meat or produce. Because they print price tags on site, it’s easy for them to attach tags for low-cost items to packages of premium products (i.e. pricing $21-per-pound beef tenderloin as chicken parts for $1.99 per pound).

In a similar approach called “sweethearting,” a cashier may scan a cheap UPC (e.g. chewing gum at 25 cents) instead of an acquaintance’s pricier product (i.e. a high-end perfume at $89).

Even if you catch these unusual behaviors in an inventory report you’ll find it difficult to link them to fraud, versus a simple change in demand.

A simple way to identify price switching involves monitoring your inventory movements. All those false sales will result in unusually high movements for the cheaper products and unusually low movements for the stolen products. Together, these two behaviors create distinct evidence of pricing fraud, especially if they are only occurring at a few stores.

An advanced analytics solution can easily detect this. Upon detecting the aforementioned sales patterns, the solution will identify which register processed most of the lower-priced items. It then pulls CCTV footage from the time of scanning, quickly empowering you to see what was really scanned and for how much. This helps you expedite your investigations and enable faster and more accurate intervention.

Fraud #5

E-commerce customer service fraud

It's a fact of e-commerce retail -- packages may go missing in transit and never reach the customer. Most retailers will replace any lost products for free. Some also send the customer a gift card or a discount on their next purchase for the trouble.

This practice carries a major risk of fraud by customer-service representatives (CSRs). Retailers have caught CSRs sending these replacement orders to themselves or acquaintances, sometimes as part of a larger ORC ring. Such incidents can quickly add up to thousands of dollars lost, making it critical to identify and stop them.

Numerous data feeds can reveal this activity before losses mount. Examples include:

- **Replacement destinations.** Replacement orders that are being shipped to the local area around a call center have an increased probability of being fraudulent. Similarly, multiple replacement orders sent to the same few addresses must be investigated immediately -- especially if they match addresses on file for current employees. Prescriptive analytics can easily identify and alert you to these anomalies.

- **Frequency of replacement.** As previously explained, advanced analytics solutions can establish benchmark averages for behaviors like order replacement. By comparing these averages for all CSRs against individual CSRs' replacement rates, a solution can easily identify anyone processing more replacement orders than expected.

Any of the above data behaviors can potentially indicate fraud. The right analytics solution can identify them and alert you to launch an investigation before losses hit critical levels.

Conclusion

The modern retail asset protection professional needs new, powerful tools to identify and eliminate internal fraud. Above all it is critical that these tools drive efficiency (i.e. empowering you to identify and resolve cases quickly, before losses mount) and effectiveness (i.e. offering a high rate of true positive alerts) to optimize labor and expedite investigations. Investing in an advanced analytics solution like prescriptive analytics can give you the competitive edge you need to uncover even the most subtle cases of fraud and protect your margins and profits.

To learn more about prescriptive analytics and how it can help asset protection combat fraud and non-compliance, visit www.zebra.com/prescriptiveanalytics or reach out to us at fran@zebra.com.

Zebra
Prescriptive Analytics™

Powered by Zebra Savanna™