"BUT I ONLY WORE IT ONCE!": THE RISING COST OF RETURN FRAUD

BY ANNE LOCKNER AND KAITLYN JOHNSON

Your customers may be thinking, "What's the harm in wearing something once and returning it?" But return fraud can have a big impact on a retailer's bottom line. The National Retail Federation estimates that return fraud will cost retailers $2.2 billion in 2016. Return fraud is particularly prevalent after the holidays, when many consumers often return items that were received as gifts without receipts or tags. Retailers estimate that 3.5% of 2016 holiday returns will be fraudulent.

Understanding *how* return fraud happens is the key to preventing it. Over 90% of retailers report that they have experienced consumers returning stolen merchandise. Another common form of retail fraud is "wardrobing," – customers purchase clothing, wear it, and then return it. Wardrobing is a common problem for retailers offering special occasion clothing, like prom dresses and suits. Wardrobing isn't limited to clothing – it often occurs in other departments, especially electronics. The customer who just purchased a 50 inch flat screen TV, for instance, might box it up and return it the day after the Super Bowl. Often these returned goods must be heavily discounted and put on clearance or "open box" sales. The fraudulent use of e-receipts is also on the rise. As more retailers offer their customers the option to have a receipt e-mailed, customers have more opportunities to alter or recreate those receipts to make fraudulent returns.

E-receipts are not the only area where technology makes it easier for customers to cheat the system. With the constant growth of online retail and the ease of checking and comparing prices online, consumers can purchase an item online or in store on sale or at a lower price. The consumer can then return that item for a refund or store credit at a *different* store that offers that item at a higher price, netting a cash or gift card gain for the customer, but often costing the store accepting the return.

It's often difficult to identify which returns are fraudulent. Even if a retailer is able to identify fraudulent returns after the fact, the dollar amount of an individual customer's fraud is likely not high enough to justify the expense of legal action. Because there is little that retailers can do once return fraud *has* occurred, prevention is key.

Retailers face enormous challenges in ensuring honest and accurate returns without sacrificing customer service and customer loyalty, but there are a few common methods that can help prevent fraudulent returns. Many retailers use external tags on apparel – especially more expensive special occasion items – to curtail wardrobing. Charging a re-stocking fee on all returns, or even just on particular items, may also discourage wardrobing and returning big-ticket purchases. Because the largest source of retail fraud is returns without a receipt, storing digital receipts that can be retrieved by the sales associate handling the return may also help curtail some fraudulent returns without a receipt or flag receipts that have been altered. Some retailers also collect driver's license or other personal information from customers making returns (with or without a receipt) to track patterns and potentially identify serial returners. Although these steps may make returns more difficult for honest (and loyal) customers, having a separate department and separate employees to handle returns may help customers differentiate between the sales side and the return side of the store, preserving more customer goodwill.

Customer relationships aren't the only concern retailers face when implementing these preventative measures. Some return policies or practices may open retailers up to consumer class actions. Retailers have already seen consumer class actions alleging that their restocking fees are unfair or that they weren't properly disclosed to customers. A Texas auto parts dealer was even sued by the Texas Attorney General. The AG alleged that, among other charges, the dealer charged customers restocking fees for defective merchandise in violation of Texas law. To mitigate this potential risk, retailers charging restocking fees should take measures to clearly communicate the fees to customers. Retailers should also avoid charging restocking fees to customers requesting an exact exchange for a defective product.

Collecting personal information from customers to track returns may also help curtail retail fraud, but retailers should be careful – the information that stores collect and retain may be subject to state or federal data privacy laws. California, for example, regulates what credit card information may be stored by retailers under the Song-Beverly Credit Card Act of 1971. Following major data breaches, stores like Target and Home Depot have recently faced consumer class action lawsuits over leaked credit card and personal information. Although those lawsuits generally involved information collected through the point-of-sale system during purchase transactions, information collected during the return process may still be a target for hackers, particularly if that information is collected on the same terminals as purchase data. This is especially true for stores that may use customer data collected during returns or purchases to mine and store additional customer data. Integrating sound data collection and privacy practices that comply with all applicable laws and reduce the risk of breach is the best way to protect retailers from this type of consumer class action.

BOSTON
LOS ANGELES
MINNEAPOLIS
NAPLES
NEW YORK
SILICON VALLEY

800 553 9910
ROBINSKAPLAN.COM

ROBINS KAPLAN LLP
REWRITING THE ODDS