

Ending Retail Scams With RFID

RSI ID Technologies is working with a Los Angeles startup to market a tool that uses RFID to thwart fraudulent product returns that cost retailers billions.

By Mary Catherine O'Connor

Nov. 30, 2004—David Cox wasn't thinking about the 1955 Hitchcock film starring Cary Grant when designing his new product, To Catch A Thief, but he was thinking of a college classmate who paid his tuition by returning stolen items to retail stores for full refunds. To Catch A Thief is an RFID-based application created to help retailers eliminate return or exchange fraud by proving where and when a product was purchased.

"It's just too easy," says Cox, founder and chief executive officer of Los Angeles-based startup Bar Code Security Systems, of the practice of stealing high-value items or purchasing them below full retail value at discount houses, and then returning them for their full value or for store credit. "I realized that they [retailers] had no way of knowing if an item was purchased or not."

That's when Cox knew there was an opportunity for him to develop a way for retailers to eliminate fraudulent returns through a tamper-proof technology. The system, which is still in development, will encode RFID tags, attached to products, with an encrypted 18-digit ID that includes a five-digit product identifier (so that thieves could not swap the tags on two purchased items and return the one of higher value). By reading this tag, the retailer will have proof as to whether or not the item was purchased at its store.

Fraudulent returns and exchanges cost retailers in the U.S. tens of billions of dollars annually. According to Cox, it is difficult to get exact stats on how much retailers lose through return and exchange fraud, as it is usually categorized under general inventory shrinkage, which includes items stolen by employees, as well as vendor or administrative errors.

But Cox says this is the most common method for professional thieves to make money or gain goods illegally, and it is leading to significant losses at brick-and-mortar chains and online outlets, from department stores to specialty stores to consumer electronics stores. Cox also says that fraudulent retail practices are the single largest category of larceny in the United States, more than motor vehicle theft, bank robbery and household burglary combined.

As his company's name implies, Cox initially tried to create a proof-of-purchase system to correlate with bar code labels. He knew he could not do anything with the UPC number, but experimented with methods of marking or stamping bar code labels at the point of purchase. Until Cox learned about RFID, however, all of the methods he'd considered could be imitated or tampered with or copied by thieves. In 2001, Cox applied to patent his proof-of-purchase concept with a list of technology applications that include RFID (the patent is still pending). At that time he also started attending retailer conferences and trade shows to shop around his system. "People loved the idea," he says, "but in 2001, it was too early for the technology. They [retailers] weren't ready for it. Now they are."

After meeting RSI ID Technologies vice president of development, Jhon Kielty, Cox decided to partner with

the San Diego-based systems integrator to bring his idea to fruition. Developers at RSI ID wrote a software platform for the To Catch A Thief (TCAT) solution. Kielty describes this software as a very simple, Windows-based program with a sales module (for encoding the tag with an encrypted 18-digit ID) and a return module (for reading the item's tag to verify its purchase). Kielty says the next likely update to the software will be to write a store-identifying number (to correlate to the store location of purchase) and a date stamp to the tag, instead of the encrypted 18-digit number. Eventually the tag data might also include an identifier for the sales clerk who handled the transaction or the product's UPC number. This encrypted data encoded onto the tag will also be stored in a database and viewable, unencrypted, by the sales clerk.

The TCAT software is designed to be used with passive tags and readers that operate at 13.56 MHz. RSI ID decided on this frequency because it provides an optimal read range for this application. Kielty won't divulge the brand and model of the tags and readers the TCAT system will use, but he says that they are one of the most widely used makes and are ISO-compliant.

Cox and Kielty say they want the TCAT application to be as easy as possible for retailers to use, and they envision it as something that store clerks can toggle into at the point-of-sale computer terminal. Retailers would decide how to implement the solution by deciding which items to tag (though these items would likely be the most valuable at the store or the ones that the retailer is most concerned about regarding fraudulent returns) and by adjusting return policies to spell out how and why RFID will be used. Retailers would place the tags at their own discretion, but would most likely locate them in discrete parts of the product where the tag is not susceptible to physical damage. If an item were returned with a tag that showed signs of tampering or an attempt to disable it, the retailer may decide not to accept the return.

A fixed reader would be built into the sales counter to encode the tag at the time of purchase (tags on larger items that could not be placed on the counter, such as TVs or large appliances, would require a handheld device for encoding). The reader would also lock the tag, so that it could not be written over. Online purchases would be tagged and encoded at the distribution center before being shipped. When a tagged item were returned, the retailer might not issue a refund or credit if the item lacked a TCAT tag that store's records indicate the item should have, or if a TCAT tag had not been encoded.

Because the RFID tag will never contain any information identifying the purchaser, the method of payment used or any credit card information, Cox and Kielty see no privacy concerns in relation to the application. Cox also notes that by removing the burden of proof-of-purchase from the patron, this system will decrease the chances that a patron will feel as though he or she is being unfairly profiled based on his or her race or appearance. Cox explains that as an African American, he knows that customers who are attempting to return merchandise are susceptible to unfair scrutiny based on race. This product, he says, evens the playing field. He'd like to eventually see industry-wide return/exchange policy standardization that would place the burden of proof-of-purchase on the item rather than the customer. (This standardization would be dependent on the TCAT system or similar technology-enabled proof-of-purchase system becoming ubiquitous.)

Cox is in discussions with point-of-sale system developers about offering the TCAT tool with their systems. Point-of-sales systems giants like IBM and NCR are two companies that Cox and Kielty identify as target collaborators for this product offering. If and when retailers begin tagging individual items in large numbers in order to electronically monitor items on the sales floor or to use RFID at the point-of-sales system, RSI ID says the TCAT product could be integrated into the larger RFID application. If this wider tagging practice were done with EPC-complaint UHF tags, RSI ID would adjust its software to incorporate the TCAT system into the UHF tags, so that retailers would not need to have two separate tags on items.

RSI ID anticipates that some large retailers will also want to integrate the TCAT tool into their enterprise software applications. If that happens, RSI ID will develop middleware, customized to the retailer's technology specifications, in order to achieve this integration.

Pricing for the product is still under review. Cox and Kieley are in discussions with a number of retailers about the product and hope to begin pilot projects to review the technology with retailers soon.

[RFID Journal Home](#)

Copyright ©2005 RFID Journal, Inc. All Rights Reserved