How Effective is Your Camera System at Preventing Loss Due to Internal Theft and Fraud?

Abstract: From the early 1990s until the middle 2000s, retailers commonly used text inserter boxes to integrate point of sale (POS) transaction data with their camera systems as a tool to control internal loss due to employee theft and fraud. Although text inserters had their drawbacks, namely being difficult to install and costly on a per terminal basis, they did have one major advantage: once the transaction data was injected into the camera signal and recorded, it created a permanent and unalterable timestamped record of what happened on the cash register. The unalterable nature of the recorded transaction formed the basis of court admissibility upon which management could take disciplinary actions ranging from counseling up to and including dismissal without fear of the subject employee asserting the defense that the transaction record was somehow altered so as to implicate him in a theft or fraud he did not commit.

Modern camera systems continue to provide the important POS integration capability to retailers, but in the transition to network data tapping and IP cameras, something important has been lost, and that is the unalterability of the old-fashioned text inserter. This paper explores the history of POS integration in the retail sector, explains why most modern camera systems fall short of producing court admissible evidence of retail fraud, and gives the reader valuable guidance in how to evaluate the strength of integrated camera systems presented by his vendors.

Internal Theft and Fraud in the Retail Environment

According to the National Retail Security Survey, retailers attribute 43% of their shrinkage to employee theft, translating into an annual employee theft price tag of $14.4 billion. Given this high level of loss, it is little wonder that the most frequently used asset control policy is POS exception-based reporting, employed by 95% of retailers. Furthermore, over 20% of retailers plan to up the ante by investing in technology upgrades including remote CCTV monitoring, CCTV integrated with POS exception reporting, and POS data mining software. There is a veritable arms race happening in the front lines of the retail environment with dishonest employees developing new and innovative schemes for defrauding their employers of cash and merchandise while retailers scramble to keep up by deploying the latest technologies and updating their business practices and training.

How Does Employee Theft Happen?

There are as many elaborations on employee theft schemes as there are retail establishments, but the basic elements typically come down to either giving away merchandise to a non-employee collaborator without charging full price or straight up skimming cash from the till. Typically, monitoring and controlling employee use of POS exception codes such as no sale, void, coupon, discount, refund, over ring, and cash drawer open is sufficient to detect the vast majority of fraudulent activity. The reason that integrating CCTV with POS exception reporting is such a hot topic in retail is doing

so yields actionable forensic evidence which positions the retailer to not only detect the fraud, but take swift and certain action including counseling, termination, prosecution, and recovery of stolen assets. This is the reason why an effective integrated CCTV solution generates high ROI for the retailer and has a payback period measured in weeks or months. In many cases, employee awareness of the installation of an effective modern integrated CCTV system is sufficient to measurably improve the retailer's weekly cash flow.

But what are the keys to making the integrated CCTV system effective? Certain attributes must be present, otherwise the only purpose the integrated CCTV system investment will serve is to give the retailer a false sense of security while the dishonest employees continue depleting his assets. Here are the key attributes of an effective integrated CCTV system:

- ✓ 100% of POS activity must be captured
- ✓ POS activity must be captured in real time
- ✓ The resultant video forensic evidence must be court admissible

The remainder of this article explores various approaches CCTV manufacturers have taken over the years to achieve these objectives. The article highlights the technologies that are particularly effective and also notes the ones to avoid. Finally, we provide a list of questions the reader can use to properly vet an integrated CCTV system proposal to protect himself from investing in an ineffective solution.

How Text Inserters Worked and Why They Were Effective

From the late 1980s until the middle 2000s, analog text inserters dominated the integrated CCTV market. Because these devices used serial data input from the cash register, they provided a "least common denominator" approach that allowed integration with a wide range of POS devices, depending on how skilled the installing technician was at building a serial cable with the correct pinouts and electrical connections to accurately read the POS data. A typical text inserter installation would require a serial data tap be installed either on a dedicated COM port on the POS or, more commonly, using a Y-cable between the POS terminal and the POS printer. Local variations such as tapping parallel printers or dealing with POS servers that provided data from all terminals in the store added complexity to the field installation.

For all of their associated installation headaches, the one area where text inserters were highly effective was at producing court admissible forensic evidence on the CCTV system. The reason for this is text inserters would convert the POS transaction data into an analog signal that was directly mixed with the analog video signal coming from the camera. The output of the text inserter was a modified analog video signal that had the POS text superimposed on the camera image. This modified analog video signal was fed directly into the CCTV recording device, which could be either an analog VCR or a modern DVR. Since the CCTV recording device had no intelligence, all it was

capable of doing was faithfully recording the modified analog video signal received from the text inserter box. Although this approach was low-tech by today's standards, the one big benefit was the accuracy of the text overlay on the recorded video was absolutely irrefutable and therefore constituted ironclad court admissible evidence and could be used with confidence by the retailer to prosecute and terminate dishonest employees and to recover the property they stole.

The Downside of Text Inserters

For all of their merits, text inserters came with some pretty serious downsides, including:

➢ A good quality text inserter could cost $200 or more. In a typical installation, one text inserter is required per POS terminal. The result is a rather pricey solution, with the installation cost scaling linearly with the number of POS devices at the retail location.

➢ Because of the site specific complexity of the installation process, specifically determining the correct cabling required, installing text inserters was typically labor intensive and therefore costly. Installation of text inserters was considered a specialty mastered by a limited subgroup of the technician labor pool, which further drove up the installation labor budget for a typical store.

➢ A dominant portion of text inserter installations depended on using a Y-cable connection to the POS receipt printer and passively "sniffing" transaction data by looking at the printer datastream. The problem with that approach is it required store personnel to print a receipt for each transaction. In many retail environments, the transactions are small, in cash, and the customer does not want a receipt. Forcing a receipt to be printed for each transaction resulted in another artificially high cost due to the cost of printer paper rolls, which were likely used to print a receipt which was immediately thrown away.

➢ The other problem with relying on sniffing the printer datastream is many POS terminal events were missed. Since not every POS terminal event was captured, the dishonest employee had plenty of loopholes to work with to defeat the integrated CCTV system. And although the retailer may have required his employees to print receipts, in reality employees would forget, selectively choose not to, or not be able to print the receipt (for instance the receipt printer may be broken or out of paper during a busy shift).

➢ Finally, the typical serial data capture scheme used by text inserters did not receive data in real time; instead, the text inserter would see POS transaction data only upon tendering the ticket (because tendering the sales ticket resulted in the receipt being printed).

Vendors attempted to circumvent these fundamental shortcomings using embellishments such as dedicated COM port outputs on the POS terminals, multi-

terminal POS server configurations, and tapping data off of the pole display, but the bottom-line verdict on text inserters was in addition to having high per terminal equipment and installation costs, they fell short in two key areas:

1. They did not see 100% of the POS activity
2. They did not see POS events in real-time

How Digital Camera Systems Eliminate the Need for Text Inserters

The 2000s saw a tremendous surge in innovation on integrated PC-based digital CCTV systems. Because these systems had increasingly robust on board processing capabilities, they were able to use software to replace the basic function of the text insertion box. From a data acquisition standpoint, the majority of these systems have continued to use the serial data approach pioneered by the text inserter architecture, with all of its inherent shortcomings. More advanced integrated digital CCTV systems have replaced the serial data acquisition method with direct network connections in cases where the POS server supports electronic journal output.

Where Most Digital Camera Systems Fall Short

The majority of integrated digital CCTV systems that use the serial data approach for acquiring POS transaction data share the same fundamental shortcomings that text inserters had (i.e. not seeing 100% of POS events in real time). However, the upper echelon of integrated digital CCTV systems that do support direct network connections to the POS system do properly address these shortcomings. Note that for this to be true, the network connection between the POS and CCTV systems must be "direct" and not simply a serial data tap converted to IP.

The key area where today's integrated digital CCTV systems typically fall short is in court admissibility. This is essential because the value of the integrated POS exception-based CCTV solution is to provide the retailer with court admissible evidence. Without that, the retailer leaves himself open to legal challenge of his efforts to terminate dishonest employees and recover his stolen property.

Why are the recordings produced by the majority of today's integrated digital CCTV systems not court admissible? Because they either do not even attempt to insert the POS transaction data into the recorded video or they give the appearance of doing so, but in reality are not. Specifically, typical integrated digital CCTV systems handle POS transaction data in one of two ways:

1. It is not uncommon to see digital CCTV systems not even attempt to integrate the POS transaction data into the recorded video, instead they present a facsimile of POS receipt alongside the camera image. This is clearly not court admissible because whether or not the POS events on the receipt facsimile occurred at the

same time (or even on the same camera!) as the recorded video is subject to very liberal interpretation.

2. An emerging class of integrated digital CCTV systems stores the POS transaction data separate from the recorded video and then mixes them on playback. Although this technique produces the desired effect of displaying the camera image integrated with the POS data, it is subject to tampering or manipulation because the transaction data is stored separate from the video. By editing the transaction data file, the dishonest employee could readily cover the tracks of his larceny. Although this particular exposure may sound rather far-fetched to the retailer, the reality is the dishonest employee tends to be tech-savvy and is probing for security weaknesses in the POS system, the CCTV system, the network, and the database.

Best of Both Worlds: The "True" Networked Text Insertion Solution

The ideal integrated digital CCTV system cleanly combines direct network POS data acquisition with software-based real-time text insertion ("true" text insertion) to replace the old analog text inserter technology. This approach not only lowers equipment and installation labor costs, but also elegantly meets the 3 key requirements for a viable integrated solution:

1. Because the POS data is acquired using a direct network connection, 100% of POS events are visible to the CCTV system, including not only normal sales data, but also all exceptions and non-sales activities such as employee sign in/out and cash drawer open.

2. Since there is no dependency on serial data output or sniffing receipt printer activity, all POS events are seen by the CCTV system in real time, meaning the alignment between the activity in the recorded video and the POS data event is completely synchronized, leaving nothing to interpretation for later management action.

3. Software-based real-time text insertion results in the POS data being securely integrated with the recorded video in a "write-once" manner so that the resultant forensic evidence is every bit as court admissible as the old-style analog text inserter was.

A network-based integrated digital CCTV system featuring "true" text insertion truly gives the retailer the best of both worlds by combining the ease of implementation, high quality, and ease of use of a modern digital CCTV system without losing the vital court admissibility that the older analog technology provided so well.

Summary: What to Look for in an Integrated Camera System

Here is a list of key questions to ask your camera system vendor when selecting an integrated digital CCTV system:

- ✓ How is the POS data being acquired? Using serial data communications and/or a Y-cable? By taking serial data from the POS and converting it to IP? Or using the preferred direct network connection technique?

- ✓ Does the camera system see the POS data in real-time, as each button or function key is pressed at the POS terminal? Or does the POS system wait until the transaction is tendered to send data to the camera system?

- ✓ Exactly what POS data is reported to the CCTV system? Are all POS exceptions (e.g. void, no sale, coupon, discount, refund, over ring, etc.) captured and reported? Are other POS events such as cash drawer open or employee sign in/out captured?

- ✓ Does the CCTV system do "true" software-based text insertion that is unalterable and court admissible? If the CCTV system presents the receipt side by side with the camera image, it is not court admissible. If the CCTV system allows you to turn the text overlay on and off when viewing the recorded image, then it is not court admissible.

- ✓ Will the camera system manufacturer produce upon request an official signed affidavit attesting to the unalterable nature of the recorded video integrated with the POS transaction data? If you need an expert witness to vouch for the authenticity of your recorded evidence of the dishonest employee's larceny, you will want to have the right camera system vendor in your corner to back you up.

About Odyssey Technologies, Inc.

Odyssey Technologies, Inc. was founded in 1997 and is an early pioneer in digital video. With over 11,000 video surveillance systems installed worldwide, Odyssey differentiates itself by providing equipment, software, and services for centralizing and automating multi-site operations in Retail, Hospitality, Financial Services, and Property Management. Remote Eyes systems feature superior video compression, multi-site remote video management, and integration with point-of-sale, access control and networked transaction systems. To learn more about Odyssey Technologies, Inc., please visit us at www.remoteeyes.com or e-mail Odyssey on sales@remoteeyes.com.

Odyssey Technologies, Inc.
7526 Connelley Drive, Suite A
Hanover, Maryland 21076
(888) 291-6379
Email: sales@remoteeyes.com