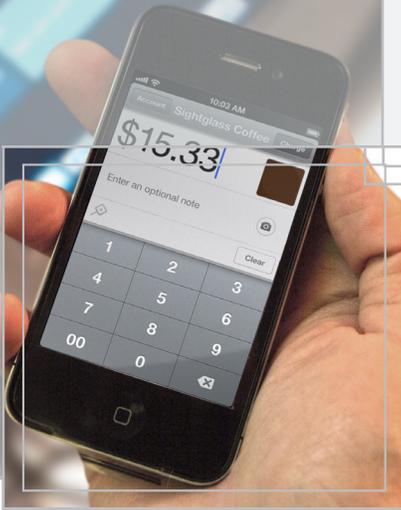


# Using Video to Combat Mobile Payment Fraud

*How a layered security strategy built on video surveillance saves lost sales for retailers*



## 3 Steps to Combat Fraud

**Incident:** Members of an ORC ring act as retail employees to skim credit card information from mobile payment devices.

**Solution:**

1. Integrate facial surveillance technology with store's POS system
2. Capture, index and catalogue the faces associated with the suspicious incident and suspects
3. Use analytics to quickly search over network of cameras to see if suspects are manipulating mobile payment devices in more than one location

The widespread use of smartphones for making mobile payments has created brand new opportunities for quick-thinking thieves. From hacking handheld devices to skimming PIN numbers, today's organized crime syndicates are cashing in fast. But while mobile payment technology can present security risks, savvy retailers are fighting back with a multi-layered strategy that unites sophisticated video surveillance with today's top anti-fraud systems.

## Mobile Mania

Mobile payments are on the rise. Global handset sales in the Q2 2011 increased 16.5% to 428 million units from a year earlier, according to a recent report from research firm Gartner. A recent study by ABI Research indicates consumers worldwide will be spending more than \$119 billion using their mobile phones by 2015. And industry giants such as Google, Verizon Wireless and Bank of America are already jumping on the mobile payment bandwagon, unveiling state-of-the-art payment solutions and platforms.

That's good news for consumers who appreciate the convenience and ease of use of mobile payment technology. After all, imagine being able to purchase a big-screen television without having to reach for your wallet and scramble for a credit card. The flipside, however, is that as mobile payments catch on among retail shoppers, the risk of fraud is likely to increase as well.

## The Cold, Hard Evidence

Shoplifting, employee or supplier fraud, organized retail crime and administrative errors cost the retail industry \$119 billion in 2011 or 1.45% of sales — a 6.6% uptick from the previous year, as reported by the Global Retail Theft Barometer. And customer theft, including shoplifting and organized retail crime, increased 13.4%, costing retailers \$51.5 billion or 43.2% of shrink.

Fortunately, there are ways to reap the benefits of mobile payments while creating a frontline defense against security threats. Forget about a single-solution approach to busting up an organized crime ring. These days, retailers require a layered security strategy that combines the sleuthing capabilities of point-of-sale (POS), exception-based reporting, RFID, PCI compliant systems, video surveillance, and other systems.

## Case In Point

Consider, for example, a network of thieves who are working undercover as retail employees. Each and every day, these workers, scattered across multiple locations, skim credit card and debit card information from mobile payment devices — data which they then imprint on gift cards and other falsified payment cards.

Years ago, a shop owner's only recourse was to catch the crook red-handed. But thanks to a layered security strategy and advances in video surveillance, there's no shortage of ways to put the bad guys behind bars, or at least out of business.





For example, by integrating facial surveillance technology with a POS system, retailers can capture, index and catalog faces and any video associated with suspected criminals. Are these thieves manipulating mobile payment devices in more than one retail location? Are ill-intentioned employees working in tandem as part of a crime syndicate? How much money is being stolen and how exactly? A layered strategy can answer all of these questions.

## Peeling Back The Layers

Another way to stop mobile payment-related internal theft is by integrating visual surveillance with exception-based reporting systems. This allows loss prevention teams to flag illegal transactions, and collect valuable video information about that transaction in minutes flat. Long gone are the days of sifting through hours upon hours of grainy videotape. Thanks to advances in video surveillance technology, investigators can pinpoint a fraudulent \$50 transaction on a Tuesday at 4pm, mine thousands of terabytes of data, and uncover a corresponding image of the assailant. Better yet, this can all be done in the time it takes to pay your credit card bill — a critical edge given the high speed at which criminals move these days.

Staying one step ahead of crime syndicates also calls for big-time collaboration. That's why many retailers are finding new ways of taking snapshots of suspects, and sharing these images with external crime-busting organizations. By pooling resources, and automatically alerting authorities to suspects using facial surveillance, organizations are building a powerful united front against mobile payment fraudsters. No wonder 43% of organizations are investing in video surveillance systems in 2011, according to a recent survey of loss prevention professionals conducted by Retail Solutions Online.

## A Multi-Pronged Approach

But busting crime is about so much more than adding a visual dimension to your arsenal of crime-fighting weapons. Sure, video surveillance technology can flag suspicious behavior, identify known offenders, and analyze patterns in transactional data. But reaping all the benefits of mobile payment technology requires a layered security strategy — one that combines business intelligence and multiple anti-fraud systems in a single, unified platform.

3VR's Video Intelligence Platform™ is the ideal solution. By revolutionizing the way video is analyzed, and correlating seamlessly with POS systems, exception-based reporting and other systems in real-time, retailers are certain to wipe the smiles off crime syndicates in minutes flat.

### Learn More:

To find out more about how 3VR can help you nab mobile payment fraudsters, visit [www.3vr.com](http://www.3vr.com) today.

**3VR Inc.**  
475 Brannan Street, Suite 430  
San Francisco, CA 94107  
877.387.6061  
[info@3vr.com](mailto:info@3vr.com)

