

# Securing the Cash Flow

By Bill Zalud, Editor Emeritus

**S**orry, but Willie Sutton never did say that he robbed banks because “that was where the money was.” But, after his last stay in prison, he did do television commercials for Connecticut’s New Britain Bank & Trust Co. to hawk the company’s new MasterCard.

Today, the beat goes on as banks, credit unions, financial service firms, armored car carriers and thousands of automated teller machines (ATMs) are the target of robbers and internal theft but rarely burglaries.

Protection strategies are diverse and range

ference is that, today, robbery attempts have become more potentially violent and sophisticated: more guns aimed at branches, bomb threats, suspicious packages, and anthrax-like white powder attacks.

## BASIC SECURITY RESPONSES

So security strategies continue to evolve. There are the basics, of course: intrusion detection, holdup alarms, bandit barriers, bullet-resistant glass, teller lockers, safes and locks. Security video has taken on an increased role, since the days of still film cameras at bank exits. Today, cameras, often positioned behind tellers, capture images of customers and transactions to provide

Minneapolis corporate office. “My mission is to provide physical security at owned and leased properties,” he says. That includes policies, procedures, technologies and security officers – all of which may vary by location, type and hours of operation, after-hours needs and level of risk. “We set a certain level of security standards that can be applied to all the covered locations,” he adds.

For the firm’s owned, or leased and operated retail stores, McNaughton applies security video in several basic ways. “The cameras are used in a ‘dealer shop’ application where they look at the cash,” he says. “This is a cash handling business. Tellers



Security video cameras play a major role in securing bank lobbies and viewing customers and transaction.

from security officers, vault hardware and access controls to security video and computer security programs.

During Willie’s “career,” he grabbed about \$2 million in his total bank robberies. Not a bad haul in those days. Today, however, the average bank robbery hauls in just \$7,756 per incident, not a smart move that often can end in federal prison.

But, if you think that a bad economy creates more bad people who do more bad things, well, at least when it comes to financial services crimes, 2010 FBI statistics don’t show that’s the case. There were significantly fewer robberies last year as compared to pre-recession years such as 2006 and 2007, even in the face of increased numbers of bank branches. Over the years, by the way, there have been only a handful of bank burglaries.

Yet, the biggest and most troubling dif-

a level of deterrence and to satisfy forensics needs. At many financial service firms, security video works the floor as well as the backroom where security executives have increased their attention.

For example, Jim McNaughton has a laser focus on his business.

That’s a good thing for MoneyGram International, a leading money transfer company that enables consumers who are not fully served by traditional financial institutions to meet their financial needs. It has a huge international reach with more than 244,000 locations, though the vast majority of the firm’s agents, who range from big retail chains to mom-and-pops, have their own business and security responsibilities.

McNaughton is senior manager, corporate security, working out of the firm’s



Audio/visual technology can mitigate the potential of crime. The Mid-Hudson Valley Federal Credit Union in New York launched one of the world’s first 24/7 drive-up personal teller, allowing members to bank with a live teller via video portal.

can make honest mistakes or dishonest ones. The system can easily provide video to local supervisors or those farther away to review transactions to make a determination, which may lead to an investigation.” Where MoneyGram International is the sole tenant in a facility, there may be video inside and outside the building. “If we are not the sole tenant, security video is inside.” Other cameras are positioned to provide overall views.

## CAMERAS AT CORPORATE AREAS

And there are cameras at various corporate locations that help provide a safe and security working environment.

As he evolves the use of security video, McNaughton sees value in a coexistence of analog and digital video while storing and

retrieving images locally per site. “Another business benefit is the ease of review of the video. Appropriate staff members can search so much faster. It saves a lot of time.”









McNaughton works closely with his IT folks to help set up or upgrade security video and access controls, to provide Power over Ethernet to cameras where it makes sense and to help with digital video and network video recorders, to name a few collaborate measures. “But because we store video locally, there is not undo stress on the enterprise infrastructure,” he says.

He also sees the security officer force as working more closely with business goals. “For retail locations, they provide security and also reception duties.” Officers on duty after-hours operate more traditionally, on patrol looking for any concerns or trouble.

At another business that uses Salient Systems’ technology, the American Bank of Texas (ABT) employs security video for coverage including teller windows, processing rooms, ATMs, parking lots and lobbies. In all, there are over 280 IP and analog cameras at multiple facilities with both local and centralized security operations. Among features: live viewing, instant playback, alarm event alerts and full camera controls.

Based in Marble Falls, American Bank of Texas uses technology among the ways it matches its charm of a small town bank with the resources of a large financial institution.

Behind the scenes, bank management has taken a proactive approach to customer

Threat Description Improvised Explosive Device (IED)		Explosives Capacity <sup>1</sup> (TNT Equivalent)	Building Evacuation Distance <sup>2</sup>	Outdoor Evacuation Distance <sup>3</sup>
	Pipe Bomb	5 LBS	70 FT	1200 FT
	Suicide Bomber	20 LBS	110 FT	1700 FT
	Briefcase/Suitcase	50 LBS	150 FT	1850 FT
	Car	500 LBS	320 FT	1500 FT
	SUV/Van	1,000 LBS	400 FT	2400 FT
	Small Moving Van/ Delivery Truck	4,000 LBS	640 FT	3800 FT
	Moving Van/ Water Truck	10,000 LBS	860 FT	5100 FT
	Semi-Trailer	60,000 LBS	1570 FT	9300 FT

1. These capacities are based on the maximum weight of explosive material that could reasonably fit in a container of similar size.  
2. Personnel in buildings are provided a high degree of protection from death or serious injury; however, glass breakage and building debris may still cause some injuries. Unstrengthened buildings can be expected to sustain damage that approximates five percent of their replacement cost.  
3. If personnel cannot enter a building to seek shelter they must evacuate to the minimum distance recommended by Outdoor Evacuation Distance. These distance is governed by the greater hazard of fragmentation distance, glass breakage or threshold for air drum rupture.

At the point of handling an initial bomb threat, there is the potential to collect valuable information.

security, not only data security, but physical security as well. Crimes like check fraud and identity theft also pose a significant threat to financial institutions and require the latest in video surveillance. ABT branches are equipped with video surveillance security equipment and systems.

Video recording, live viewing and instant playback provide immediate, actionable information for management and law enforcement. Video can be searched by date, time, camera location, or any combination of these, or when an alarm event occurs. Video displays instantly on an alarm to catch

the attention of the security operator. Video events are then displayed in a history list in which the operator can call up live video with full camera controls and review the recording of the event side-by-side.

At the Teachers Credit Union, headquartered in South Bend, Ind., the largest credit union in Indiana with 51 locations including the 4-story corporate office, access control had been using offline computer-managed (CM) locks, placed at strategic locations such as at the outside entrance, the door to the teller line and access to the vault room.

While these locks had been easy to install,

## Suspicious Package Response Guidance

Some characteristics of suspicious packages and letters include the following:

- Excessive postage
- Handwritten or poorly typed addresses
- Incorrect titles
- Title, but no name
- Misspellings of common words
- Oily stains, discolorations or odor
- No return address
- Excessive weight
- Lopsided or uneven envelope
- Protruding wires or aluminum foil
- Visual distractions
- Ticking sound
- Excessive security material such as masking tape, string, etc.
- Marked with restrictive endorsements, such as "Personal" or "Confidential"
- Shows a city or state in the postmark that does not match the return address

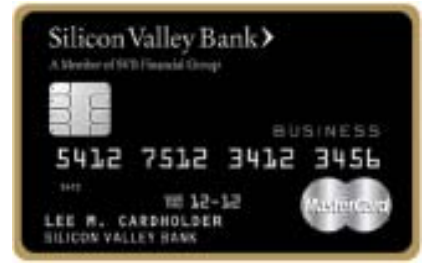
Once a suspicious letter or package has been identified, it is important to respond appropriately. Follow these three main steps:

- **Package** – Package means that you do not handle the package or letter. Leave it where it is! Isolate the area. Do not try to clean it up, move it, or place it in a plastic bag. Make a mental note of any information that might be useful (size, shape, look, address).
- **People** – Clear the area. Inform employees in the immediate area so they won't disturb the suspicious package, letter, or substance. Notify a supervisor immediately. All employees in the area near the package should wash their hands and any other exposed skin with soap and water immediately, even if they didn't touch the package or letter. The area should be cordoned off. Air conditioner, fans and equipment should be turned off.
- **Plan** – Contact security or law enforcement. Follow your emergency plan. Know who to contact if your supervisor isn't available. In an emergency – such as smoke, fumes, vapors, or employees exhibiting medical symptoms – evacuate the area and call local emergency responders.

they required significant resources to manage. Data that controlled access was downloaded to each lock individually, using a PDA. Audit trails and other information were uploaded to the PDA and transferred to a computer. The database itself was managed on the computer, allowing for response to personnel changes, lost credentials and changing access requirements. In addition,

with each branch having its own CM stand-alone access control, the growing number of branches and the widening geographic coverage of the credit union were starting to create big problems for Mike True, the credit union's director of security.

"Every time that some employee left the credit union or another employee was hired, we had to drive out to that branch



**Identity theft and information security are growingly important banking concerns. Silicon Valley Bank was of the first to deliver chip-enabled credit cards, with advanced chip technology, to businesses in the U.S.**

and reprogram all the locks," says True. "It was costly in time, mileage and hotels. It just wasn't working anymore. We were scrambling." It also meant that security was compromised from the time the need was reported until the lock was reprogrammed.

True knew they needed to upgrade but didn't want to have to replace all their electrified door equipment, including power supplies, closers and exits. They just might have to continue working with what they had.

But it turns out the financial service firm turned to Ingersoll Rand's Schlage bright blue IP-enabled security management system along with an AD-Series locking systems.

The tech approach "did everything that I wanted it to do," comments True. "Most importantly, since it was open architecture design, we could keep our current door hardware intact even though we were going to be integrating a wireless system."

With the wireless locks solution, True and his team have simplified control of who goes when and where because they interact with bright blue in the same way they do with any web page on the Internet. The system application is embedded on the control panel which connects easily to the credit union's present network. Adding and deleting personnel, setting up doors and assigning access based on time schedules is straightforward. If there is a new employee or an employee leaves the credit union, True and his staff can simply add or delete that person from their computers without getting out of their chairs.

## **GOING BEYOND PHYSICAL SECURITY**

"ABT's goals to protect assets, people and privacy have been enhanced with this installation. It's a powerful tool that provides fast searching and the ability to send video clips instantaneously to law enforcement and other branches," says Howard Gordon, senior vice president, information technology, American Bank of Texas.

While physical security is important at ABT and other financial service firms, there is growing attention to information security

due to national and international regulations and the fallout from headline-grabbing data breaches. Studies by the Ponemon Institute and others indicate that bank customers will quickly move their business elsewhere in the event of a data security breach, even if it did not affect them personally.

MoneyGram International, for instance, has a tool in the war against fraud: a tailored software system that monitors what it calls “send” transactions and identifies transfers that could involve fraud, enabling the firm to intervene and prevent its customers from losing money to fraudsters.

The anti-fraud tool is a rules-based automated IBM software system that analyzes the transaction data from MoneyGram’s money transfer system. Based on consumer identity management and transaction rules set by the company, the system identifies potentially fraudulent transactions and alerts MoneyGram instantaneously after the transaction has been placed. MoneyGram can then put the transaction on hold, contact the original sender and if needed, stop the fraudulent transaction from being received.

Consumer complaints of fraud in January 2011 compared to January 2010 dropped 72 percent, with the most significant reductions in Canada, Nigeria, the United States and the United Kingdom.

When it comes back to physical security needs, there are some integrators who have traditionally served the sector. These include, but are not limited to, Diebold, Niscayah and Security Corporation.

## **BOMB AND PACKAGE NEEDS**

Beyond electronic and hardware security solutions, enterprise security leaders at banking and financial service firms must contend with workplace violence and incidents that can involve armed robberies, bomb and anthrax/white powder threats.

Today, such threats call for additional defenses, according to Thomas Browning, vice president corporate compliance/chief security officer at AlliedBarton Security Services.

With some people blaming banks for a number of social and financial ills, there are threats and suspicious packages that are phoned in, mailed in and left at facilities. “Security needs to work with carriers such as the United States Postal Service, UPS, and Federal Express,” says Browning. “Screening processes and procedures need to be in place as another avenue to the corporate mailroom. Training and manual checks help with these staffers to put their smart hat on.”

Whether a phoned-in threat or suspicious package, it is essential to call local enforcement or the local emergency management team, according to Browning.

“All hazards planning is the best way to go,” says Bo Mitchell, president of 911 Consulting, which advises corporations on a variety of security topics. “You cannot prevent everything. So you and all staff

members must be prepared for every possibility. Without that, the enterprise can be liable for failure to plan or failure to train.” Federal and state regulations, court decisions and NFPA 1600 – the Standard on Disaster/Emergency Management and Business Continuity Programs – and require an emergency team and plan in place, observes Mitchell. **SECURITY**

---