

The Monthly Publication of the  
National Association for Bank Security

# THE ADVISOR

Administered by  
Profit Protection, LLC  
Ft. Lauderdale, FL

## 2004 COMPLIMENTARY

*Injustice anywhere is a threat to justice everywhere.*

— Martin Luther King, Jr.

## Blanket Immunity Not Afforded

The Supreme Court of Arkansas recently held, in *Bank of Eureka Springs v. Evans*, that the Annunzio-Wylie “safe harbor” provision did not afford the bank blanket immunity from liability for filing Suspicious Activity Reports (SARs). In support of this decision, the court held that the bank, which provided false information to a state prosecutor, had maliciously caused a criminal complaint to be filed against one of its borrowers. The court affirmed an earlier verdict against the bank of \$100,000 in compensatory damages and \$300,000 in punitive damages.

In this case, the borrower, who was engaged in the cattle and construction business, sought a \$460,000 loan to purchase 1,120 acres of undeveloped  
(Cont. **BLANKET IMMUNITY** on page 2)

## Security Outside

Our customers occasionally become victims of crimes that involve their financial institutions. Depending on the type of crime committed, customers can sustain losses of varying severity, and can be exposed to varying degrees of danger. It behooves us to be aware of the potential for such crimes and assume a protective attitude in order to shelter these treasured assets. One of the locations in the banking environment where customers, as well as our own treasured assets—our employees—can be confronted with danger is the bank parking lot. A few short, common-sense safety tips can dramatically advance security outside the bank for customers, and employees as well. Here are some suggestions:

- Always be alert to your surroundings, and other people around you, whether you are using the night depository or ATM, walking between the bank door and your vehicle, or walking to or from a detached facility. Thoroughly observe the area around the ATM or night depository.

(Cont. **OUTSIDE** on page 3)

## Phishing

In *Alert 2003-11*, the Office of the Comptroller of the Currency advises that the FBI’s Internet Fraud Complaint Center (IFCC) reports a steady increase in complaints about a scam called “phishing” (first reported in the September *Advisor Supplement*) or “spoofing,” which involves unsolicited e-mails directing consumers to a phony “customer service” Web site or directly asking for customer information. The customer may be sent a seemingly legitimate e-mail request for account information, often under the guise of asking him or her to verify or reconfirm confidential personal information such as account numbers, social security numbers, passwords, and other sensitive information. In the e-mail, the perpetrator uses various means to convince customers that they are receiving a legitimate message from someone whom the customer may already be doing business with, such as a bank. Techniques such as a false “from” address or the use of seemingly legitimate bank logos, Web links, and graphics may be employed

(Cont. **PHISHING** on page 6)

## Advisory Board

David Battle, CFE  
Principal  
Security Consultant/Training Specialist  
David Battle Resources  
St. Louis, Missouri

Arvin E. Clar, CFE  
Cleveland Police Department  
Financial Crimes Unit  
Cleveland, Ohio

Thomas R. Duxbury, MA  
Editor  
Profit Protection, LLC, and  
National Association for Bank Security  
Fort Lauderdale, Florida

Kathy Felder  
Principal  
Strategic Solutions, LLC  
Greensboro, North Carolina

Marcus H. Ford  
President *Emeritus*  
Profit Protection, LLC, and  
National Association for Bank Security  
Fort Lauderdale, Florida

Jay M. Friedland, Esq.  
President and CEO  
M&M Consulting, Inc.  
Brunswick, Maine

Phillips G. Gay, Jr., CRCM, CRP  
Principal  
Compliance Advisory Service  
Coral Springs, Florida

Fred A. Gwin, CPP  
Principal  
Protection of Assets Consultants  
Baton Rouge, Louisiana

Elizabeth R. Marchese  
Principal  
Bancor Security  
Davie, Florida

Boris F. Melnikoff, CPP  
Bank Security Consultant  
Atlanta, Georgia

R. Eugene (Gene) Seitz  
Retired Review Examiner  
FDIC Special Activities Section  
National Association for Bank Security  
Fort Lauderdale, Florida

Bill W. Thompson, CPP  
Principal  
Thompson Training  
Dayton, Ohio

J. Branch Walton  
President  
Profit Protection, LLC, and  
National Association for Bank Security  
Fort Lauderdale, Florida

## BLANKET IMMUNITY

(Cont. from page 1)

land. He told the bank he would clear the land in order to run cattle on it, and would use cut timber and construction income as repayment for the loan. The board of directors of the bank approved the loan for the borrower, a long-time customer.

Subsequently the borrower had several financial setbacks and eventually he defaulted on the promissory note and mortgage. Then he began to consider filing for bankruptcy protection. This did not sit well with the bank. When the president and CEO was informed of his plans, he warned the borrower that he would “make his life hell” if he filed for bankruptcy. Then on a separate occasion the CEO questioned the borrower’s brother about some of the borrower’s collateral which related to another loan. The CEO closed the conversation by telling the brother to advise the borrower to “play ball” with him or he would have them both arrested.

The borrower finally filed for bankruptcy, and the CEO pursued his threat. Despite evidence that some of the borrower’s collateral had been released by the bank, and that the borrower had loaned, rather than sold, other collateral, the bank’s attorney filed a SAR with FinCEN. The SAR alleged that the borrower had wrongfully disposed of collateral held by the bank. The attorney also contacted the local prosecutor and filed a criminal complaint against the borrower.

Some time later the bank filed a second SAR alleging that the borrower had cut timber on the purchased acreage without permission from the bank. The bank also claimed that it had not received any payments on the indebtedness. Then a second criminal complaint was filed by the bank against the borrower, alleging again that the borrower had wrongfully disposed of collateral and had never made any payments on his loan, and that the bank had never given the borrower permission to harvest timber off the land. A bench warrant was issued for the borrower’s arrest and he subsequently surrendered himself to custody.

Before trial, the bank’s executive vice president contacted the prosecuting attorney and stated that the bank would be willing to settle the case in exchange for a sum of money and a land exchange. However, the trial proceeded and the borrower was not convicted because the trial court granted a motion to dismiss based on the statute of limitations. Subsequently, the borrower filed suit against the bank and the CEO for, among other things, malicious prosecution. In unsuccessfully defending against the suit, the bank alleged that its actions were protected by the statutory safe harbor. In its appeal of the decision, the Supreme Court of Arkansas affirmed that the bank’s behavior was malicious, continuous, and based on information the bank knew was false, and that it was not protected by the safe harbor. Although the court recognized that the pertinent law specifies that financial institutions are to report “any possible violation of law or regulation,” it did not agree that Congress intended the law’s safe harbor to give banks such blanket immunity that even malicious, willful criminal and civil violations of law are protected. Importantly, reasoned the court, the law requires there to be “possible” violation of law—“possible” being the operative term here—before a financial institution can claim protection of the statute. The court, viewing the evidence in the light most favorable to the borrower, decided that there was no “possible violation.”

In sum, the Arkansas Supreme Court found that the law’s safe harbor provision did not apply to the situation at hand, that safe harbor is not absolute, and that it does not protect malicious and willful activity. This holding is consistent with the decision of the 11<sup>th</sup> Circuit Court in *Lopez v. First Union National Bank of Florida* in which the 11<sup>th</sup> Circuit Court held that the safe harbor is not absolute and is subject to a “good faith” requirement. The 11<sup>th</sup> Circuit decisions establish legal precedent in the following states: Florida, Georgia, and Alabama. It should be noted that other Circuit Courts (1<sup>st</sup> and 2<sup>nd</sup> Circuit) have held that the safe harbor is absolute and not subject to a good faith requirement. ■

## OUTSIDE

(Cont. from page 1)

tory before using it. Look for suspicious persons loitering nearby, on foot and in vehicles—especially people who remain in parked cars. This applies whether you are using the ATM or night depository, or are transporting the bank's or your own cash/valuables, and especially if you are carrying a container that appears as though it might contain cash or other valuables.

- Never display cash in a bank parking lot...if possible, not even a "bank bag." Always count money in a secure place.
- Be suspicious of anyone who appears to be closely observing you outside the bank, especially when using the ATM or night depository, or when carrying a container.
- Spend as little time just outside the bank as possible.
- Be cautious of any stranger who engages you in conversation outside the bank.
- If you must conduct banking business during the hours of darkness, use discretion. Have someone accompany you.
- Park as near as possible to your destination, e.g., branch, ATM, or night depository.
- Seek a banking environment whose parking lot and exterior are well lighted; whose landscaping and other objects do not provide "hiding places"; that is located on a well-traveled street; and that generally has unobstructed visibility in all directions.

Tips like these work out very well as counter-top handouts and statement stuffers. They might very well be enhanced by a warm letter offering to improve customer security on an individualized basis. A letter similar to the following might be helpful.

## SAMPLE

Dear [Customer]:

Let me say at the outset how pleased ABC Bank is to be able to attend to your financial needs. We value our customers, and it is for this reason that I am writing to you.

I understand that because of the business you are in you find it necessary to come into the bank from time to time and deposit or withdraw sizable amounts of currency. Like many of our customers, you may be doing this on a very regular basis and, in fact, may have your banking down to a routine. Unfortunately, this routine can also be obvious to others more concerned about their needs than yours. You can, in fact, become a prime candidate for a robbery.

Therefore, I would like to suggest that you consider altering your banking pattern both in terms of time of day and means of transportation. It might just be worth the slight inconvenience.

You should also be aware of the fact that the bank's insurance does not cover losses from robberies which occur in our parking lots. If you are walking a considerable distance through our parking lots to your car with large amounts of currency, please contact the branch manager. He or she will be more than happy to work out alternate procedures for you.

If you have any questions, please feel free to contact me.

Very truly yours,

[customer service representative]

A gesture like this helps the customer in obvious ways, as well as the bank from a customer relations perspective. ■

## The Appearance of Legitimacy

Thirty-seven-year-old Carl Edward Fuerst recently met with a violent come-uppance after traveling throughout the Southeastern United States and hoodwinking banks out of almost \$2 million by passing counterfeit cashier's and other checks. As twenty police mobile units and a helicopter chased Fuerst for more than twenty miles, shots were exchanged. Finally, the subject drove his van into a ravine, dying probably of a combination of gunshots and the accident's impact, and demonstrating why he was considered armed and dangerous and had earned a place on the U.S. Postal Inspection Service's Most Wanted List.

What this man of a thousand aliases typically did was break into post office boxes, steal checks, print counterfeit commercial or cashier's checks (his favorite) from the information, and make them payable to the people he stole them from. However, instead of simply cashing the items, he improved his chances of success and conducted split-deposit transactions, brazenly placing a portion of the checks into the victims' accounts and requesting the rest as cash-back. This MO gave the transactions the aura of a deposit rather than an encashment, which reduced the chance of suspicion on the part of the tellers and could very well have caused some of them to overlook check-cashing limits. Fortunately, a head teller recognized Fuerst from his photograph on a Postal Inspection Service's poster and ended his career.

The relatively high rate of success of cash-back check frauds over the years, due in no small part to the appearance of legitimacy these transactions have, mandate additional diligence, even though they are so common. This becomes particularly important if the appearance of legitimacy of cashier's checks is added to the mix. Split-deposit transactions should be viewed as encashments rather than deposits, and should be subject to the appropriate procedures, such as check cashing-limits. ■

# QUESTION OF THE MONTH

## NEW ACCOUNT SECURITY

**Can you give us some examples of things to look for when opening an account that might indicate it is being opened for illegitimate purposes?**

New Account personnel have more time and are under less pressure when an account is opened to properly identify an individual than is a teller at the onset of a bank transaction with other people waiting in line for his or her service. Thus, it can be argued that new account employees are in a more advantageous position than tellers to prevent fraud. By implementing appropriate security procedures during the account opening process, new account employees can decrease the probability that bank fraud must be stopped by tellers if it is indeed going to be stopped...that busy tellers must detect the crime after a person has been granted depositor status. Therefore, truly effective fraud protection, particularly check fraud protection, starts at the new account desk. Protecting the financial institution's assets is just as important as acquiring new customers. As much care should be taken when granting a person depositor status as is taken when giving a person a loan.

### Common Warning Signs of Trouble

The following is a list of items which are considered to be of predictive value for determining if a person is attempting to open an account for fraudulent purposes. A new account representative who encounters one or more of the following while processing a new account application should be extra careful in verifying all information provided by the applicant. It is virtually impossible to lay too much stress on the importance of verification.

<b>Address</b>	No permanent address P.O. Box Mail Drop Non existent Branch not in proximity to home or job
<b>Telephone</b>	No telephone, or number does not match the one in the phone book Answering service Exchange prefix wrong for address Cellular only (becoming less of an indicator as more people are using them as their primary telephone) Pager only
<b>Identification Document</b>	No primary identification Identification does not meet standards established by the financial institution Identification issued within past 30 days or is "temporary" Signature on identification document (e.g., driver's license) does not match signature on application Individual's appearance does not match physical description on identification

<b>Social Security Number</b>	Photograph of individual does not match appearance of customer Cannot provide an SSN Number invalid Issue date does not fit age of applicant State of issue not same as claimed
<b>Applicant</b>	New in town Does not work or live in area of banking office where account is being opened Conversation produces inconsistencies with application Applicant asks that statements be held at bank
<b>Verification Process</b>	Discrepancies discovered Information provided by applicant cannot be verified
<b>Initial Check Deposit</b>	Low check number No edge perforation Less cash transaction Encashment of checks payable to a business Checks with alterations Using bank encoded (MICR) check or starter kit check

When a new account representative has a reasonable suspicion that the person who is attempting to open an account may not be who he or she purports to be, the new account person should do the following:

1. Do not get into an argument with the customer.
2. Have the customer sign the signature card.
3. Accept the opening deposit, preferably in cash, or if the opening deposit is a check, advise the customer of the extended hold that will be placed on the item in accordance with your Reg CC policy.
4. Do not give the customer a check starter kit. Inform the customer that his personalized checks will be mailed to his home in a few days.
5. Do not process the request to open the account until all information provided by the applicant is verified.
6. After the customer leaves, refer the matter to a supervisor, who should review the situation and initiate a due diligence investigation in order to verify all information provided by the new account applicant.

If the bank decides to reject the new account applicant, the new account supervisor or other institution official should send a letter to the applicant via certified mail—return receipt requested—stating simply that the bank chooses not to honor the request for the opening of the account at this time and that enclosed is either a cashier's check in the amount of the initial deposit (if it was in cash) or the applicant's personal check which was tendered as an initial deposit when the account was applied for. ■

---

## Cash...and More Cash

In one recent robbery, a man gesturing that he had a handgun passed a teller a note that demanded \$100 bills. No particular amount. Just \$100 bills. Imagine his delight when he watched the teller grab \$13,000 in cash from her top drawer. Neither a dye pack nor bait money was included in the loot. He got away scot-free.

This case and cases like it cry out for cash control procedures. Maximum cash in a teller's possession should be established as follows:

- Maximum amount needed as operating currency (unstrapped) in the top drawer, according to daily expectations based for the most part on past patterns and trends; and
- Maximum amount needed as reserve currency in a second, locked drawer (to include strapped currency).

The currency present in each drawer should be dictated by need and bank policy. If it's kept at a minimum, losses from robberies will be kept at a minimum. The second-drawer concept is a good one from a security perspective. In our over 20 years of reviewing thousands of bank robberies, only a very, very few have involved a robber's demanding money from a second drawer. The vast majority just want a fistful of cash from the top drawer right now so they can get out of the bank as quickly as possible.

The following policies, in checklist form, can limit cash exposures:

- The top cash drawer should not contain:
  - More currency than is needed to function
  - Packets of strapped currency
  - Mutilated currency
  - Foreign currency
  - Other negotiable instruments
- Each teller's daily record of starting and ending cash should be periodically reviewed.
  - Tellers should be aware of the cash procedures review.
  - When tellers commit violations of established cash limits, they should be reminded of the required limits. Violations of cash control policies should be reported to the security officer on a scheduled basis. The reports should be in written form (some banks have developed a form for this purpose) and should be submitted even though a report indicates no violations for the reporting period.
- A teller's station should be inspected and the currency should be counted on a periodic, but random, basis.

---

## Combination Punches Work Best

What do you get with sharp bankers, "extremely clear" surveillance photos, and bank robbers who insist on wearing the same clothing and carrying the same guns in multiple robberies? Speedy, career-ending (doesn't hurt to hope) arrests. That's what happened when two misguided heavyweights – this helped in the photos — decided to take on the wrong bank branch on a recent Saturday morning. The two men, one weighing 260 pounds and the other exceeding him by another 20 pounds, walked into the Palo Alto Wells Fargo branch and appeared to case the facility for a few moments before leaving. The employees recognized them immediately. Wells Fargo had distributed crystal clear surveillance photographs of the duo taken during a previous robbery to its employees. The subjects were so accommodating one wore the same clothing and the other carried the same weapon, and this showed clearly in the pictures. All these factors came together so well that police were able to arrest the two culprits as they walked away from the branch. ■

## Scam Has Its Dangers

The Nigerian advance fee fraud ("419 Fraud") has become such a serious problem in the eyes of the U.S. Government that the Secret Service has formed a special task force to fight it on an international basis. The agency estimates that in the last 14 or 15 years \$5 billion has been stolen from victims throughout the world. Tens of thousands of proven 419 Fraud telephone numbers have been accumulated by the Secret Service, and the agency continues to receive about 100 phone calls and 300 to 500 pieces of mail per day from victims or potential victims.

We've described the common characteristics of the scam on numerous occasions in the past—things like the involvement of official-looking, but fraudulent/forged, documents; requests for bank letterheads, invoices, and other banking particulars; requests for countless Nigerian "fees"; urgently encouraged confidentiality. But the Secret Service is warning especially of the potential danger connected with becoming a part of this scam. Victims are almost always asked to travel to Nigeria or a border country to complete the transaction. They are often told that a visa will not be necessary to enter the country. Members of the illegal organization may then bribe airport officials in order to pass the victims through Immigration. This is very dangerous because it is a serious offense in Nigeria, and can in turn be used to coerce more money out of the victims. Threats and even violence may be resorted to, including kidnapping and murder. This has happened in the past.

If you, or any of your colleagues or customers, are confronted with any of the many versions of the Nigerian advance fee scam, it is advised that you (or they) notify law enforcement (fraud division) right away and, if the solicitation is via e-mail, refrain from responding to the e-mail. Doing so would validate your e-mail address for the criminals and encourage them to send you more mail. ■

## PHISHING

(Cont. from page 1)

to mislead the customer. After gaining the customer's trust, the perpetrator attempts to convince the customer to provide personal information and provides one or more methods for him or her to communicate that information back. For example, the e-mail might include a link to the perpetrator's Web site that contains a form for entering personal information. Like the e-mail, the Web site is designed to trick the customer into believing it belongs to the bank. Alternatively, the e-mail might simply include an embedded form for the customer to complete. The ultimate goal of this fraud is to use customer information to gain unauthorized access to the customer's bank or financial accounts or to engage in other illegal acts.

Management may wish to consider the following actions to help prevent, detect, and respond to the threat from e-mail-related frauds:

### Prevention

- Provide notices on Web sites reminding customers that the bank will never request confidential information through e-mail and to report any such requests to the bank.
- Print warnings and notices on customer statements or other paper mailings.
- Improve authentication methods and procedures to protect against the risk of user ID and password theft from the customer through e-mail and other frauds. Authentication methods solely reliant on shared secrets (e.g., passwords) are more susceptible to phishing schemes than stronger authentication methods.
- Review and, if necessary, enhance practices for protecting confidential customer data.
- Maintain current Web site certificates and describe how the customer can authenticate the bank's Web pages by checking the properties on a secure Web page.
- Refer customers to, or use, Federal Trade Commission (FTC) resources in order to develop educational brochures to explain the red flags and risks of identity theft. The following will be helpful: FTC, "How Not to Get Hooked by the 'Phishing' Scam,"

July 2003, <http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>; FTC, "ID Theft: When Bad Things Happen to Your Good Name," September 2002, <http://www.ftc.gov/bcp/online/pubs/credit/idtheft.htm>.

### Detection

- Monitor accounts individually or in aggregate for unusual account activity such as address or phone number changes, large or a high volume of transfers, and unusual customer service requests.
- Monitor for fraudulent Web sites using variations of the bank's name.
- Establish a toll-free number for customers to verify requests for confidential information or to report suspicious e-mails.
- Train customer service staff to refer customer concerns regarding suspicious e-mail request activity to security staff.

### Response

- Incorporate notification of known e-mail-related frauds into the response program to alert customers of fraudulent requests for information and to caution them against responding.
- Establish a process to notify Internet service providers, domain name issuing companies, and law enforcement to shut down fraudulent Web sites and other Internet resources that are being used to facilitate phishing or other fraudulent e-mail practices.
- Increase suspicious activity monitoring and employ additional identity verification controls.
- If fraud is detected in connection with customer accounts, the bank should report the fraud and consider offering its customers assistance consistent with the comprehensive guidance on reporting and customer assistance given in OCC Advisory Letter 2001-4, "Identity Theft and Pretext Calling."

In the event your financial institution is a victim of an e-mail-related scam, the Office of the Comptroller of the Currency advises that you contact law enforcement and file a Suspicious Activity Report (SAR). ■

## Test Firing Surveillance Cameras

Here's another good argument for testing surveillance cameras.

They knew his name. They knew where he lived. And they knew his family members. But police didn't have enough evidence to prove that Michael Raynard Purnell was the robber of at least eight banks this year, six of them in April alone. They needed evidence, like good photos.

After each robbery, tellers were shown an array of bank surveillance photographs, but none of them could ever "pinpoint" the robber. Said one of the frustrated detectives, "We had some photos from some of the other robberies, but we weren't getting any good picks from the victims. Some of the photos were taken in shadows or with dark backgrounds, and it wasn't easy to see the robber clearly."

Mr. Purnell finally had his comeuppance. After what proved to be his last robbery, he was seen leaving the branch on a blue motorcycle. A patrol officer later spotted a blue motorcycle parked outside our suspect's home and decided to patiently wait for him. When the suspect showed up with his girlfriend, he was arrested. Shortly afterward, one of his victim tellers positively identified him.

Good security is a lot of little things...like testing cameras to see if the lighting is proper, or that the cameras are pointed accurately, or that there are no obstructions, or that the tape hasn't been used so many times that it's virtually shot. Let's give law enforcement as little as possible to complain about. In the long run it will make for better security.

## Watch That Cyber Info!

We recently reviewed an e-mail hoax from the nation's heartland. The fraudulent e-mail told customers of a major bank that their accounts had been closed because they had been "compromised by outside parties." The message then instructed customers to visit a different Web site so they could verify their identities and have their accounts reinstated. This was the manner of the ploy designed to glean personal and financial information from the customers.

This bank wasted no time contacting the authorities about the scam and also placing the following statements on its Web site: "[XYZ] Bank does not collect customer e-mail addresses and does not attempt to contact customers for any reason via e-mail. [XYZ] Bank will never ask for your user ID, password, PIN, or other confidential information. You should be suspicious if asked and never give out this information unless you are certain that the site you are on is legitimate and secure." E-mail fraudsters have been imitating Web sites more and more frequently over recent months, often with success, unfortunately.

Bankers are well advised to put similar cautions to customers on their Web sites, and also in bank statements and on teller counters. Another good rule of thumb for communications security, regardless of the medium, is to avoid giving personal and financial information *unless you initiate the communication*, especially over the telephone, and then such information can be restricted by the traditional *need-to-know* principle. For example, not everyone you initiate contact with needs your SSN. ■

---

## Bank's Security Challenged in Lawsuit

One year later the triple Greer, South Carolina, bank killing remains an unsolved mystery, and police continue to deal with the task of examining and re-examining over 700 frustrating leads. One thing that is new in this case, to the dismay of the bank involved, is a lawsuit initiated by a daughter of the two customers killed in the robbery. (Teller Sylvia Holtzclaw was also killed.) In the suit, the plaintiff alleges that acts of negligence by the bank make it responsible for their parents' deaths.

Among the lawsuit's more specific allegations are that the bank, whose facility where the crime took place was a trailer close to an interstate highway:

- 1) Utilized a facility (the above-mentioned) that was not in a safe location;
- 2) Did not provide adequate security measures, i.e., did not take "reasonable measures to discover and deter criminal activity on or around the branch bank location";
- 3) Failed to properly train employees in security procedures; and
- 4) Failed to meet federal security requirements;

The associate chancellor at the university where one of the customers was employed as a student advisor expressed the feelings of many about his killing when she remarked, "I did not weep for many, many months because the anger was overwhelming," she said. "It's directed at a society where violence is so prevalent that innocent people can go into a business and never return." ■

## Failure to File

A New York-based bank pleaded guilty this fall in U.S. District Court to one count of failure to file a Suspicious Activity Report (SAR) on a Colombian money broker suspected of money laundering. The charge was brought by U.S. Immigration and Customs Enforcement (ICE) in Baltimore, Maryland, as part of its undercover money laundering investigation called Operation Laundry Chute. Pursuant to a plea bargain, the bank agreed to forfeit \$950,000 to the U.S. Government.

According to the plea agreement, a Colombian customer of the bank "helped" other Colombian customers of the institution with transactions in their accounts that were part of the foreign currency exchange business. This benevolent altruist had operated an independent foreign currency exchange since the mid-1990's. One of the problems with this kind of financial business is that foreign currency exchange organizations in Colombia have been identified by the U.S. Government as high risks for money laundering of the proceeds of illegal drug sales and other criminal activity. Colombian drug traffickers use a system known as the "Black Market Peso Exchange" to launder profits from illegal drug sales.

Thus, because the bank was fully aware of these activities (according to the plea agreement), it found itself in trouble. The institution agreed that the government could have produced evidence to prove that the total amount involved in the customer's foreign currency exchange transactions (i.e., that the amount that required SARs, according to the bank president's own admission) was between \$5 million and \$10 million. In an official statement to the press, the bank said that it accepted full responsibility for not filing the proper form, and that "in today's [post 9/11] environment it is incumbent on banks to be extremely vigilant even with clients you know well."

## ***Distributed through the following state bankers associations***

Alabama Bankers Association  
Colorado Bankers Association  
Connecticut Bankers Association  
Georgia Bankers Association  
Illinois Bankers Association  
Indiana Bankers Association  
Iowa Bankers Association  
Kansas Bankers Association  
Kentucky Bankers Association  
Louisiana Bankers Association

Maine Bankers Association  
Maryland Bankers Association  
Massachusetts Bankers Association  
MBA Insurance and Services, Inc.  
Mississippi Bankers Association  
Missouri Bankers Association  
Montana Bankers Association  
New Hampshire Bankers Association  
New Jersey Bankers Association  
New Mexico Bankers Association

North Dakota Bankers Association  
Oklahoma Bankers Association  
PBA Services Corporation  
South Carolina Bankers Association  
South Dakota Bankers Association  
Vermont Bankers Association  
Virginia Bankers Association  
West Virginia Bankers Association  
Wisconsin Bankers Association

## ***What's wrong with this picture?***

The teller is leaving for lunch and is carrying his lunch bag, no doubt anticipating a repast under some palm tree in a setting envied by many around the country, especially Minnesotans in winter. We are in the middle Florida Keys.

Wait a minute. That doesn't look like a lunch bag. How could we mistake a bank bag for a lunch bag?

The teller in this story was eventually overcome by guilt and dropped in to a police station, fully confessing to swiping the bank bag on the way out to his extended lunch hour. Then he held the bag up to the view of the desk sergeant and plopped it on the counter. Inside was almost \$100,000. (This surrender happened in the state of Washington!)

The bank is grateful, of course, for the teller's guilt and remorse. The financial recovery is attributable to that, and his decision not to blow any of the money. The problem that remains, however, is the burning question, Should a banker, on any level, be able to walk out of a bank building with \$100,000 of the institution's money under his arm?

It has been customary for us over the years to caution one another against leaving cash inadequately attended, for example, leaving armored car drop-off/pick-up shipments untended in back-room or back-hall areas, on teller counters, or on floors adjacent to the counters; stepping away from unlocked teller cash drawers; counting money carelessly; crossing parking lots unescorted with conspicuous money containers, and so on. But we usually allow ourselves to remain in the habit of thinking of "cash-and-other-valuables" control from only an external security perspective. This is a little like getting into the habit of looking at surveillance cameras as external security items only, good only for catching robbers and check and new-account fraud artists...whereas, in actuality, we've seen them used well to both catch and clear suspected embezzlers. Likewise, security of cash and other valuables must also be characterized by an expanded mindset, so that it is protected from internal criminals as well as external ones. This may require extra steps, extra paperwork, and dual (or more) control, but the end result—avoiding a \$100,000 loss—will be well worth it. The dual control principle is particularly beneficial because it affords both a check-and-balance and safety dimension to security. ■

## ***Manager Knew in Advance***

The value of unannounced audits was amply demonstrated by a recent embezzlement case in which approximately \$100,000 was stolen by a branch manager who had virtually total autonomy at her branch. Indeed, she was able to take at least \$70,000 of the stolen funds from the vault and do this for no less than a four-year period.

The plea agreement states the problem: "She did this primarily by taking increments of \$1,000 and occasionally several thousand dollars at a time. Because she knew in advance when an audit of the vault was to occur, the defendant was able to take various steps to hide the losses from the auditors." The plea agreement also indicated that the manager misused money orders to pay her personal bills and bills for relatives without providing cash to pay for the instruments at the time of the purchases. She hid this activity from the bank by not running the bank's copy of the money orders through the institution and keeping them until she had the cash to pay for the items. Sometimes the funds for the money orders were taken from customer accounts. Other times they were taken from her favorite source: the vault. ■