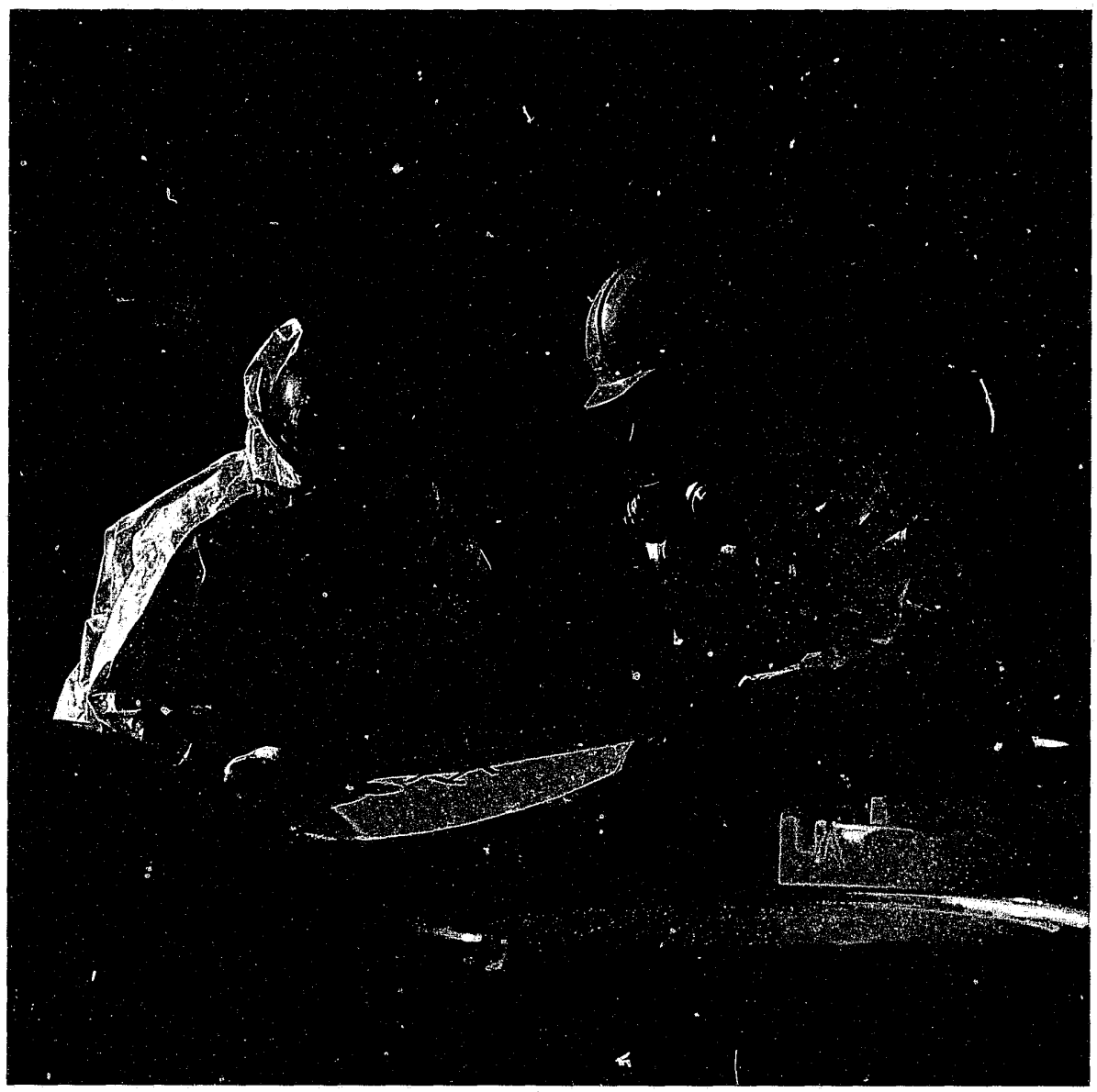


145801-04 C.1

November 1993
Volume 62
Number 11

United States
Department of Justice
Federal Bureau of
Investigation
Washington, DC 20535

Louis J. Freeh,
Director

The *FBI Law Enforcement Bulletin* (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 10th and Pennsylvania Avenue, N.W., Washington, D.C. 20535. Second-Class postage paid at Washington, D.C., and additional mailing offices. Postmaster: Send address changes to *FBI Law Enforcement Bulletin*, Federal Bureau of Investigation, Washington, D.C. 20535.

Cover photo by Steve Delaney, Environmental Protection Agency

FBI Law Enforcement BULLETIN

Features

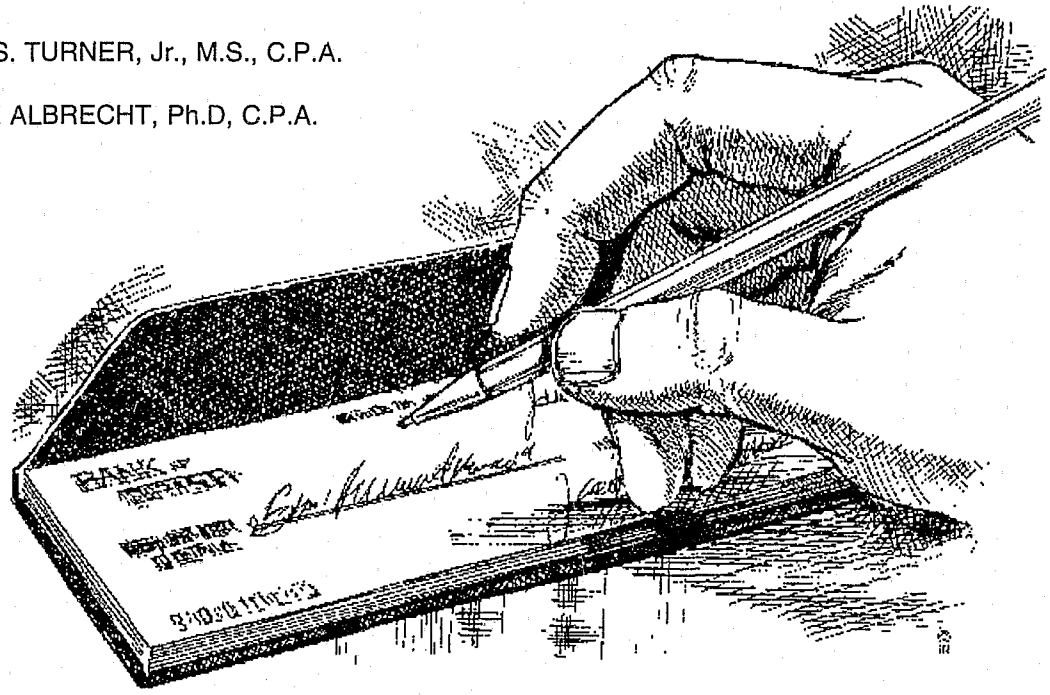
Departments

ISSN 0014-5688 USPS 383-310

145802

Check Kiting
Detection, Prosecution, and Prevention

By
JOHNNY S. TURNER, Jr., M.S., C.P.A.
and
W. STEVE ALBRECHT, Ph.D, C.P.A.



Dennis Greer (not his real name) was struggling financially. After using a $1,000 inheritance to secure an unfurnished apartment, he supported himself with a minimum-wage job that barely covered his living expenses.

With no family members or friends to turn to for assistance, and instead of seeking help through legal channels, Greer committed a fraud known as check kiting. That is, he wrote checks on one bank when there were insufficient funds in his account to cover them. To conceal the fraud, he made deposits using checks drawn on a second bank, where he maintained an account but had no money in it. The last bank to catch the fraud lost over $40,000 in less than 2 months.

Greer's kite was small compared to other kiting schemes. For example, in 1988, two individuals in New York City kited between two prominent banks. Their kite involved 15,000 checks totaling $2 billion. In another case, almost 20 banks lost over $2 million, while the perpetrator's "friends" lost $19 million.

Difficult to detect and prosecute, check kiting schemes have gained popularity in recent years. In response, more banks focus on recognizing the signs of kiting. As a result, check kiting schemes are being discovered and reported more frequently today than ever before. In fact, the number of cases reported to the FBI's Financial Institution Fraud Unit at FBI Headquarters in Washington, DC, has doubled in the past 4 years.

In order to prosecute these cases successfully, the FBI developed the Check Kite Analysis System (CKAS),[1] a computer program that helps law enforcement agencies to reduce the complexity of investigating kiting schemes and to prove the perpetrator's intent to defraud. This article defines check kiting,

describes detection methods, and explains how the FBI uses the CKAS to prosecute kiters successfully. Finally, it advises how financial institutions can stop kiting schemes before they start.

Check Kiting Defined

Check kiting is a systematic pattern of depositing nonsufficient funds (NSF) checks between two or more banks, resulting in the books and records of those banks showing inflated balances that permit these NSF checks to be honored rather than returned unpaid. In addition, other checks and withdrawals may be honored against these inflated balances, resulting in actual negative balances, to the extent that banks allow withdrawal of uncollected funds. Put simply, check kiting is accomplished by taking advantage of the float—that is, the time required for a check deposited in one bank to be physically presented for payment at the bank on which it was drawn.

Check kiting goes beyond check swapping, which involves merely exchanging checks between two or more bank accounts. When individuals devise check swapping schemes in order to create bragging rights to large account balances, they usually need not fear prosecution because the potential loss from one bank is offset by a matching inflated balance in another. Upon discovery, cooperating banks resolve the problem by returning the checks unpaid and eliminating artificially inflated balances among themselves. However, when individuals knowingly write checks against these balances to pay for purchases or other expenditures to third parties, they are committing a prosecutable offense known as check kiting.

Methods of Detection

Law enforcement officials need the cooperation of financial institutions in order to identify and prosecute check kiters. Obviously, banks benefit from early detection. For this reason, most banks have made efforts to discover such schemes before experiencing a loss. Traditionally, banks use some variation of what is commonly called a kiting suspect report, a standard form that is computer-generated by virtually all banks.

These reports work because kiting is almost always associated with the same warning signals. Even the most clever kiter cannot hide the signs that can accurately signal kiting activity. Together, these signals comprise the acronym "SAFE BANK":

- **S**ignature and payee on kited checks are often the same
- **A**rea abnormalities (many out-of-area checks)
- **F**requent deposits, check writing, and balance inquiries
- **E**scalating balances
- **B**ank abnormalities (deposited checks are usually drawn on the same banks)
- **A**verage length of time money remains in account is short
- **N**SF (frequent NSF problems)
- **K**eep banks from recognizing frequency of transactions by using ATM, night drop, drive up, and other branches for deposits and withdrawals.

The first kiting signal, signature and payee the same, is an indicator most often associated with cases involving a single perpetrator. Kiters working alone often use two or more types of accounts—such as

Special Agent Turner serves in the FBI's Provo, Utah, Resident Agency.

Dr. Albrecht, a certified fraud examiner, is Director of the School of Accountancy and Information Systems, Brigham Young University, Salt Lake City, Utah.

personal, custodial, or business—and kite among them. In addition, to avoid suspicion, kiters may make a memo entry at the bottom of checks to provide justification for the increasingly large amounts of the checks. One kiter, for example, wrote checks to himself with memo entries for a trip to Spain and for the purchase of furniture, a car, and even a forklift. Such actions should raise a red flag to bank officials, as individuals rarely make checks out to themselves when making purchases—they write checks payable to the merchant.

The second signal, area abnormalities, is very common, because kiters want to allow as much float time as possible. As a result, they often use banks in different cities or regions of the country. Therefore, bank authorities should question excessive or unnecessary use of out-of-town banks.

The third indicator, frequent deposits, check writing, and balance inquiries, is perhaps the most telling sign of kiting. In order to cover themselves, kiters make frequent deposits and write numerous checks. They inquire about their bank balances often in order to understand float times and to determine whether there is "money" in their accounts to support checks.

Fourth, escalating balances also signal check kiting. Because each check must be large enough to cover the one written before it, account balances usually grow very quickly. In one case, the bank lost $1.5 million in just over a month. In another, an individual who listed his job status as "unemployed" opened an account with $10, kiting it to over $45,000 in just 2 months.

The fifth signal, bank abnormalities, means that check kiters usually make deposits with checks drawn on the same bank. In conducting normal business or other transactions, it is highly unlikely that all checks being deposited will be from the same few banks. Therefore, authorities should be wary of such deposits, suspecting kiting as the motivation for them.

> ***"When properly understood...kiting can be detected, prosecuted, and prevented."***

For example, one $2 million kite was detected when a kiter made a deposit that included numerous checks, all drawn on the same bank in which the deposit was being made. When the kiter realized he had deposited the wrong bag, he telephoned the bank and brought a substitute bag full of checks for deposit. The substitute deposit included a large number of checks, all drawn on another bank.

Many banks use the sixth signal—the average length of time money remains in an account—to determine if deposits are immediately being withdrawn. Because this may signal a kiter's taking advantage of float times, most kiting suspect reports highlight accounts where money stays in the account an average of less than 2 or 3 days.

NSF activity, the seventh signal, may or may not be present in kiting. When balances escalate dramatically, as often happens, there may be no NSF activity. Professional kiters usually understand Federal banking regulations well enough to know how long checks and deposits take to clear. However, amateur kiters often "bounce" checks because of their lack of knowledge of clearing times.

Finally, signal eight, using alternative deposit and withdrawal methods in an effort to avoid detection, is a good predictor of kiting. Unfortunately, this activity is often difficult to monitor, because most kiters avoid entering the same bank branch several times a day. Instead, they use drive-up windows, other branches, night drops, automatic teller machines, and other alternative access methods to avoid suspicion.

Banks must take full advantage of these eight signals to detect check kiting activity accurately. Kiting suspect reports should be distributed daily, and if they signal a potential kite, checks and deposits should be pulled and other kiting indicators in the "SAFE BANK" checklist investigated.

The Check Kite Analysis System

Historically, check kiting has been difficult to prosecute. This is due to its complexity, the number of documents involved, and the difficulty in proving the perpetrator's intent to defraud. However, in 1989, the FBI developed the CKAS, which uses the RBASE database software package. The CKAS has been used successfully in dozens of

CKAS EXHIBIT

Table I illustrates the use of the CKAS and is the modified version of a trial exhibit used in the previously mentioned case that involved almost 20 banks. The table summarizes the actual account balances in 13 of the banks involved. The first 7 days showed enough combined funds to cover floated checks with no potential loss to the banking system, even though several individual banks had negative daily balances. In each of the remaining 27 days, there were net combined losses, culminating in a combined loss of $1,486,586 on October 22, 1990. The exhibit together with a graph of the loss, was used to secure a successful kiting conviction in the case.

Table I

Summary of Account Balances

Date	Bank Balance	Float	Actual Balance
09/04/90	$1,088,882	$ 342,963	$ 745,869
09/05/90	1,144,356	400,312	744,044
09/06/90	1,332,041	674,150	657,891
09/07/90	1,480,415	718,900	761,515
09/10/90	1,146,706	667,450	479,256
09/11/90	1,221,262	950,198	271,064
09/12/90	975,272	714,000	261,272
09/13/90	1,103,395	1,271,000	- 167,605
09/14/90	1,286,637	1,358,850	- 72,213
09/17/90	589,195	681,000	- 91,805
09/18/90	785,519	866,965	- 81,446
09/19/90	593,645	750,165	- 156,520
09/20/90	571,043	725,950	- 154,907
09/21/90	533,091	717,000	- 183,909
* * *	* * *	* * *	* * *
10/22/90	664,414	2,151,000	-1,486,586

bank fraud cases and has, thus far, withstood all challenges in jury trials.

Investigators working suspected check kiting cases should secure—through proper legal channels—copies of checks, deposit slips, and bank statements from all the accounts they believe the suspect is using. While these documents will be used to substantiate the case, the bank statements alone should contain all the information needed to determine if kiting has occurred and whether a particular offense is prosecutable.

Investigators need only enter the date each check was deposited, the check amount, and the date the check cleared the issuing bank. The CKAS program then calculates the length of time each check spends in float, and in turn, the amount of money in float. Therefore, by subtracting the amount in float from the bank's perceived balance, the CKAS determines the true account balance, whether positive or negative.

Whether the kite involves 2 accounts or 20, the CKAS looks at the *combined* effect on the banks affected by the kite. That is, even if 2 or 3 banks out of a total of 10 being used show negative actual balances, and thus potential losses, sufficient funds may exist in the other banks to cover the floated checks. In this case, then, there would be no loss to the banking system, although individual banks may show losses because of "forced interest-free loans." Loss of revenue alone, however, does not usually meet the intent-to-defraud criteria required for criminal conviction. In order for this to occur, the combined banking system must suffer a loss, either real or potential, resulting from the kiter's use of falsely inflated balances.

Preventing Kiting

An unwritten rule of etiquette seems to exist among bankers regarding what they can ask about a deposit and when they can place holds. In an effort to prevent kiting, some geographical banking areas have adopted restricted policies regarding depositors' use of uncollected funds. They also place holds on deposits for the maximum time limit allowed by Federal regulations. However, in other geographical areas, depositers receive immediate credit for all deposits, and kites can be more easily perpetrated.

> ***"The CKAS has been used successfully in dozens of bank fraud cases and has...withstood all challenges in jury trials."***

While, ultimately, only banks themselves can prevent check kiting from occurring, law enforcement officers can help by encouraging banks to place restrictions on deposits. If banks are not willing to restrict access to funds on all deposits, they should learn and carefully monitor the eight kiting signals and restrict access in questionable accounts.

Deciding when to deny immediate access to funds is a cost/benefit tradeoff between customer service and kiting losses. Banks that fear offending or losing customers may learn the hard way that failure to place holds on accounts and/or monitor kiting systems places them at high levels of risk.

Conclusion

Check kiting is on the increase, both in terms of the number of incidents and dollars lost. However, banks can prevent losses by denying immediate access to deposited funds and by attempting to identify the "SAFE BANK" indicators of kiting. When possible, law enforcement personnel should encourage financial institutions to take such actions.

When kiting does occur, active prosecution should take place. Using the CKAS, the FBI has successfully obtained criminal convictions of check kiters. As a result, fear of criminal prosecution now faces kiters whose predecessors relied upon the complexity of their schemes to discourage overwhelmed investigators and prosecutors. When properly understood, however, kiting can be detected, prosecuted, and prevented.✦

Endnote

[1] Special Agent Johnny Turner, Provo, Utah, Resident Agency, and Special Agent Daniel D. Dubree, New York City Field Office, developed the Check Kite Analysis System, in conjunction with the Technical Services Division, FBI Headquarters, Washington, DC. Law enforcement agencies interested in the Check Kite Analysis System may contact the nearest FBI field office.

during the presentation to answer many questions. But, the interpreters kept up every step of the way. The seminar progressed as previous ones, although at times, I moved too close to the audience and blocked the participants' view of one of the interpreters. And, I sometimes positioned myself so that those who were lip reading couldn't read my lips. When this happened, however, an interpreter kindly reminded me to step back.

As the seminar progressed, I realized that these people were intently focused on my every word. They asked well-thought-out, to-the-point questions. As I listened to them, I realized that individuals who are deaf or hard of hearing do not have the same contact with the police as other citizens. In fact, the police may be turning a "deaf" ear to them.

A Need to Listen

My limited involvement with the Deaf community through this seminar was both enlightening and informative. But it also made me aware that law enforcement may be failing to meet the needs of citizens who are deaf or hard of hearing, a situation that increases their vunerability and one that shouldn't continue.

Many police departments have equipped their communication centers with telecommunication devices for the deaf (TDD) systems in recent years. But, is this enough? Not really.

The Deaf community needs direct and equal access to all the services provided by law enforcement—crime prevention, victim/witness assistance, property identification, and security surveys, to name a few. Such assistance will go a long way in helping them to protect themselves and to feel more secure. And, if prevention efforts do not reach *all* citizens, then departments fall short in delivering quality police service.

The responsibility for improving communication with the Deaf community rests with law enforcement. Everyone in the department must work toward meeting this responsibility—from patrol officers through the ranks to the chief of police. The Deaf community is calling...is law enforcement listening? ✦

Dial Law Enforcement

Law Enforcement is now available via three computer dial-up services. Authorized law enforcement practitioners and related professionals who have a personal computer and a modem can access, download, or print current issues of *Law Enforcement* in their own homes or offices by contacting these services. Those interested in obtaining information regarding these services should dial the following numbers directly:

- SEARCH Group, Inc.
  (916) 392-4640
- IACP NET
  1-800-227-9640
- CompuServe
  1-800-848-8199 (Ask for Representative 346. *Law Enforcement* is available only through their restricted law enforcement library.)