The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 7773

April 9, 1996

STOLEN CHECKS USED FOR FUND INVESTMENT

April 9, 1996 TO: COMPLIANCE COMMITTEE No. 8-96 MEMBERS - ONE PER COMPLEX No. 27-96 RE: STOLEN CHECKS USED FOR FUND INVESTMENT

_____ The Institute has been advised of potentially fraudulent activity involving the use of allegedly stolen checks to establish mutual fund accounts. The scheme allegedly operates as follows. An individual steals a check while the check is in transit from the payor to the payee. An individual submits the stolen check to a mutual fund complex with an account application. The application is often for a corporate account with check-writing privileges. The name listed on the account application generally matches the name of the payee on the stolen check. The address listed on the account application, however, usually does not match the address of the actual payee. When the account is established, blank check drafts are generally sent to the address of record. If the stolen investment check subsequently clears, an individual begins to write checks drawing on the new account. Since the legitimate payor and payee on the stolen check are generally unaware for some period of time that the check has been stolen, the shareholder is often able to deplete the fund account without suspicion. When the legitimate payee eventually determines that the check has been stolen, the payee often contacts the mutual fund and requests reimbursement. We understand that several fund groups have sustained significant losses as a result of this scheme. In light of this fraudulent activity, provided below are number of precautionary measures that we urge you to consider: 1. Refuse to open any accounts with third party checks. A number of fund groups refuse to open any account with a third party check, that is, a check made payable to someone other than the fund or fund group. This procedure reduces the possibility that an individual will open an account with a stolen check, since the stolen checks in this scheme are generally payable to organizations other than the fund group. 2. Refuse to open corporate accounts with third party checks. Since many of the reported incidents involve corporate fund accounts, some fund groups have reportedly adopted procedures to reject third party checks submitted to open corporate accounts. 3. Develop an account profile that prompts increased scrutiny of certain account applications accompanied by third party checks. Some fund groups have established procedures so that certain types of account applications accompanied by third party checks will be scrutinized more carefully. For example, some fund groups routinely examine corporate account applications with third party checks more closely. Since many of the reported incidents have involved the use of a post office box or suite number in New York City as the address of record, some fund organizations subject account applications with these characteristics to additional review. Some fund complexes have established procedures so that third party checks over certain threshold amounts (e.g., $50,000) are routinely confirmed with appropriate parties. 4. Examine account address and other application information. If a fund

group continues to accept third party checks to open fund accounts, the fund may wish to routinely compare the address of record listed on the account application with the address that sometimes accompanies the payee name on a check. This procedure has been one of the most successful methods of detecting third party check fraud since many corporate checks include an address with the payee name. Fund groups also may wish to compare the fund account registration with the registration on any bank accounts that are designated to receive wire transfers for any discrepancies. Fund groups may want to investigate the social security number on a suspect application by checking the number through a credit agency. 5. Confirm the establishment of the account with the payee. If a fund group is suspicious about the establishment of a new account with a third party check, the fund group can use directory assistance to verify that the telephone company listing for the payee matches the address and phone number listed on the account application. If discrepancies exist, the fund group can attempt to confirm the transaction with the payee at the number provided by directory assistance. Fund groups report that attempting to confirm information by calling the telephone number listed on an account application is not necessarily an effective method of fraud detection. In some instances of alleged third party check fraud, telephone numbers listed on account applications have been answered by answering services or by other individuals using the payee name. 6. Delay sending blank check drafts to new accountholders. In some of the reported third party check frauds, the preferred method for depleting the fraudulent accounts is through check-writing. Delaying the mailing of blank check drafts to new shareholders for a period of time after an account is opened may give the legitimate payor and payee on a stolen check more opportunity to detect the theft before the fund account is depleted. Some fund groups will not send shareholder drafts until the initial hold period on an account has expired or until good funds have been confirmed on the initial investment check. At least one fund group has revised its account application so that check-writing privileges can only be established through a subsequent written request submitted to the fund group. At least one fund group has concluded that check-writing capability will not be offered as a routine account privilege on corporate accounts. Dorothy M. Donohue Assistant Counsel

---