

January 30, 2001

RE: FRAUD PREVENTION

DEAR CLIENTS:

A strong system of internal accounting controls is important in preventing fraud. The internal control system consists of the mechanisms that are in place to protect Company assets. The assets most vulnerable to loss include:

1. Cash,
2. Accounts Receivable,
3. Inventory and Fixed Assets,
4. Confidential Information

We have listed below some of the procedures and policies that should be considered and included in designing your system of internal accounting controls:

1. Setting a strong ethical environment in the organization. Do not discuss or allow company employees to be aware of any aggressive tax planning or paid company benefits for owners and officers.
2. In-depth employee hiring and screening practices. You should run background checks and obtain credit history information. We can recommend a company to assist you in obtaining this information.
3. Be alert for any financial or psychological burdens on employees and attempt to help them alleviate the difficulties through progressive personnel policies.
4. Segregation of duties with limited personnel. This requires some creativity in assigning personnel to specific tasks, and requires active involvement and oversight by management. The idea is to limit one employee's ability to commit and then conceal fraud or theft. For example, you wouldn't want the same employee to make deposits and prepare the bank reconciliation or make deposits and credit customer accounts.

Cash

5. Monitor your bank balance daily and be sure temporary cash balances are earning interest.
6. Insuring that the organization uses preprinted, prenumbered documents where appropriate, and that the numerical sequence is accounted for.
7. Monitor the counting of the petty cash fund on a surprise basis.
8. Make sure petty cash is kept in a locked cabinet or safe.
9. Review the bank reconciliation prepared by a competent employee that is independent of the accounting function.
10. Inspect unopened bank statements each month by someone not responsible for reconciling the bank account, making deposits, or writing checks, and review each check and the endorsement on the back.
11. Ensure that an independent record is established for incoming cash receipts, and comparing this record with the deposit.
12. Ensure that all checks received in the mail are immediately restrictively endorsed with a listing made of the checks, and comparing this record with the deposit.
13. Make sure deposits are made daily.
14. Make sure checks waiting for deposit are kept in a locked cabinet or safe.

Accounts Receivable

15. Carefully review before approving all accounts receivable write-offs, sales returns and allowances, voided checks, etc.
16. Ensure that independent follow-up is conducted to complaints from customers that invoices have been paid but not credited to their accounts.
17. Review accounts receivable aging and have management approve and review all credit memos and write off's monthly.

Accounts Payable

18. Make sure blank check stock is kept in a locked cabinet and account for checks in sequence.
19. Only pay from an original invoice, not from statements or copies.
20. Make sure you take advantage of all discounts.
21. Ensure that independent follow-up is conducted into complaints from vendors that bills have not been paid on a timely basis.
22. Ensure that vouchers are approved for payment only after a thorough review of supporting documentation.
23. Sign disbursement checks only after thoroughly reviewing supporting documentation. Paid vouchers should be canceled to prevent duplicate payment.
24. Monitor the distribution of payroll on a surprise basis.
25. Do not allow payroll rates to be modified or a new employee added if a payroll service is used by the employee responsible for generating the payroll checks.
26. Allow set up of a vendor only with password protection for someone other than the accounts payable clerk.
27. Make sure your computerized accounting system does not allow payment of an invoice twice.

Inventory and Fixed Assets

28. Periodically compare inventory and fixed assets physically on hand to inventory and fixed asset listings maintained in the accounting records.

29. Provide physical security over valuable assets, confidential information, blank business documents, and especially checks.
30. Compare recorded amounts and relationships to prior year results and budgets and investigate unanticipated differences.
31. Make sure adequate insurance is maintained for property, liability and business interruption.

Computer Security

32. Make sure procedures are in place to prevent testing of new or revised programs on live data files.
33. Ensure terminal access is limited to specified persons and that individuals have access only to those programs or files that are necessary to perform their duties.
34. Establish passwords to control terminal access. Passwords should be kept confidential, changed at regular intervals, and promptly canceled for terminated employees.
35. Establish appropriate procedures for daily back-up and off site and onsite storage of programs and data files. Back up tapes should be stored in a bank vault.
36. Ensure that all MIS personnel are covered by a blanket fidelity bond.
37. Establish off-premises storage for master files and transaction files sufficient to recreate the current master files and system and program documentation.
38. Develop contingency plans for alternative processing in the event of loss or interruption of the MIS function. Ensure the plan has been tested to determine the adequacy of alternative processing in the event of a disaster.

We at Fishman, Block + Company would be happy to discuss any questions that you might have concerning fraud prevention and would be also welcome the opportunity to assist in improving or evaluating your Company's system of internal control.

FISHMAN, BLOCK + COMPANY