Travel Fund Embezzlement

The Scenario

The auditor was performing a review of system access controls for the travel office. In addition, the auditor was analyzing travel related transactions. The auditor's review included an analysis of employee bank accounts provided for travel reimbursement, which were compared to social security numbers in the agency's payroll system. The comparison identified ten travel reimbursements to personnel in the agency that never travel. As the audit continued, the auditor discovered a travel office employee who recently transferred from the agency payroll office had stolen social security numbers to open fraudulent bank accounts and deposit the unauthorized travel reimbursements. A review of personnel authorized access to the travel approval function disclosed that the employee submitting the fraudulent claims was given system access when they were substituting for a vacationing co-worker. Information Technology personnel did not follow internal policies and procedures and provide temporary access to the substitute employee with a five day account expiration; even though temporary access was requested by travel management. In addition, management was not performing periodic reviews of employee travel vouchers because staff resources were limited. Because management did not follow the internal procedures, the travel embezzlement scheme was not immediately detected.

General Comments / Lessons Learned. Auditors should be aware of the increasing use of identify theft schemes to commit fraud. Identity theft involves the use or compromise of personally identifiable information, which includes, but is not limited to, education records, criminal and medical history, financial transactions, and any information that can be used to trace an individuals identity such as their name, social security number, and place of birth. Auditors should also be alert to situations where established internal controls are not functioning, such as unauthorized system access.

FRAUD INDICATORS

- **Information technology department does not verify employee access restrictions.**
- **Information technology department does not routinely monitor access to the travel system.**
- **The organization does not have adequate controls to ensure that employees and management follow established policies and procedures.**
- **Travel and/or accounting management do not conduct periodic reviews of employee travel claims.**