Fraud detection and prevention

Dr Marios Menexiadis CPA, CPIA Prof.post GRC, Adjunct Professor at National and Kapodistrian Unjiversity of Athens, Internal Audit Director Aegean Airlines,

Dr Christos Lemonakis CPA, Adjunct Professor at Hellenic Mediterranean University,

Dimitra Kotidou BSc, MBA, CPA, Chief Financial Officer Greek Film Center.

Detecting and preventing fraud is one of the biggest challenges of our times. There are so many different types of fraud as well as theft, that require consequently different methods of detection and prevention.

Although research has shown that fraud is committed by more senior positions in the management hierarchy, however, almost every department of a company can present opportunities for its employees to commit fraud.

The question is why do employees commit fraud? Is it just because of the personal benefit, because of the achievement of breaking the system, or overcoming the system? If we categorize the types of fraud, the most common ones are:

- Vendor fraud,
- Accounting fraud,
- Payroll fraud
- Asset Misappropriation,
- Bribery and Corruption,
- Data theft.

Vendor fraud can be committed by employees who act either alone or by colluding with vendors. Types of vendor fraud may include: *billing schemes (*generation of false payments to employee using the company's vendor payment system either by creating a fictitious vendor or by manipulating the account of an existing vendor), *bribery and kickbacks (*participation in a bribery scheme when the employee accepts or asks for payments from a vendor in exchange for an advantage), *check tampering (*stealing checks for payment to a vendor and alters the payee or forges the vendor's signature to deposit them in employee's personal account), *overbilling (a* vendor issues invoices to charge the company for more goods than it ships or to charge a higher price than agreed), *price fixing*.

Accounting fraud happens, when an employee manipulates the company's accounts to cover up theft or uses the company's accounts payable and receivable to steal for his benefit. Accounting fraud may include: *embezzlement, accounts payable fraud, fake supplier (*employee sets up a fake supplier and bills the company for good or services not provided), *personal purchases (*use of company funds for personal purchases, registering payments as legitimate business expenses in the accounting system), *double check fraud (*writing a check to pay an invoice and then writing a second check to the employee following by registration of disbursement in the accounting system as a payment to the same supplier), *accounts receivable fraud.*

Payroll fraud is theft from an employee via a company's payroll system. It may include: *ghost employee schemes (*fake employee or ex-employee is kept on the payroll with pay being diverted to the fraudster), *advance fraud (a*n employee requests a payroll advance

and doesn't pay it back), *timesheet fraud (a*n employee falsifies timesheets to inflate hours).

Asset misappropriation is the theft of company's assets by an employee, which is also known as insider fraud. It includes *check forgery* (forging a signature on a check made out to the employee or to someone else), *check kiting (*writing checks on an account that doesn't have sufficient funds with the expectation that the funds will be in the account before the check clears), *check tampering (*altering the payee, amount or other details on a check or creation of an unauthorized check), *inventory theft (*stealing product from a company, either by physically taking it or diverting it in some other way), *theft of cash (*stealing cash, skimming, return fraud), *theft of services (*misuse of company services or company-funded services), *expense reimbursement, expense account fraud (*use of a company expense account for personal expenses and submission of them as business-related), *procurement fraud, payment fraud* (altering payee details on checks and payables, self-authorizing payments), *workers' compensation fraud, commission fraud* (inflation of sales numbers to receive higher commissions or falsification of sales that did not occur or colluding with customers to record and collect commissions on falsified sales), *personal use of company vehicle*.

Fraud, as bribery and kickbacks, can cause more damage than the finance, since, this can deter business or affect the stock price. These frauds can include: *bribes (*paying or providing a benefit to an official to secure an advantage for the company or for the employee), *kickbacks (*receiving payments or benefits from third parties in return for business advantages or for unauthorized discounts), *shell company fraud schemes (*employee or company officer may use a shell company to launder money, pay bribes, divert assets or evade taxes).

Data theft can be disastrous for a company that relies on its intellectual property for its product or service. It can also compromise marketing and sales efforts or put the company in a precarious position with authorities when personally identifiable information is stolen (GDPR breach). Data theft may include: *trade secret theft (*proprietary information to be sold to a competitor), *theft of customer or contact lists (*copies or downloads lists of the company's contacts to either sell or use), *theft of personally identifiable information* (stealing or sharing credit card numbers, client lists to sell to other parties).

The big challenge is to find ways to discover the fraud, so this needs to apply various methods depending on the type of fraud that the internal auditors attempt to detect, however the biggest challenge is to find ways to prevent it before being committed, meaning in this way that a series of preventive controls should be in place. Either, or, the internal auditor can be a very useful tool, that can add value at the company's control system, through the various checks that he can perform, but the ultimate responsibility lies on management for the development and application of the preventive controls.

With regards to detection of vendor fraud, the internal auditor could conduct random audits of vendor files, verify the vendor's business name, tax number, phone number, address, bank account, compare vendor's addresses with employee addresses, review of vendor master file, while on a prevention level, controls applied by management may include the proper segregation of duties between the check preparer and check signer, or to rotate duties of employees in procurement.

With a view to detecting accounting fraud, the internal auditor could conduct random audits of accounts payable and accounts receivable records. On a prevention level,

controls applied by management may include proper segregation of duties between the functions of account setup and approval, an outside contractor to review and reconcile accounts at regular intervals, to rotate duties of employees in accounts payable and accounts receivable, set up an automated positive pay system to detect fraud.

With regards to detecting payroll fraud, the internal auditor could reconcile balance sheets and payroll accounts on a frequent basis, perform data analytics on payroll records to search for matching addresses, names and bank accounts, or check payroll records to ensure terminated employees have been removed from the payroll. On a prevention level, controls applied by management may include managers to approve timesheets and overtime claims, mandatory vacations for payroll employees, restriction payroll department employees to modify pay rates and hours, as well as to separate the tasks of preparing payroll checks and reconciling payroll account.

With a view to detecting asset misappropriation, the company's internal auditor could perform background checks on employees, implement checks and balances or perform random audits of company's accounts. On a prevention level, controls applied by management may include proper segregation of duties between the function of the check preparer and the check signer, the rotation of duties of accounts' employees, proper protection of checks, commissions to be paid only after goods and services been delivered, or to develop a whistleblowing channel.

With regards to bribery and corruption prevention, controls should include the development of a code of ethics, assurance that those at the top levels set an example that makes it clear that bribery and corruption are not tolerated, conduct of a risk assessment to look for areas to watch more closely as well as training of employees on bribery and corruption prevention.

Finally, with regards to data theft, prevention controls could include restriction of access to company proprietary information to only those who need it in the course of their jobs, set up of IT controls to alert management of large data downloads or transfers or downloads and transfers that occur at odd times, purchase of software that alerts management of suspicious activity on a company network, shredding documents and remove data from electronic devices before redeploying or disposing of them, use of strong passwords for all computers and devices that can access sensitive information, implementation of a clean-desk policy that prohibits employees from keeping sensitive information on their desks while they are not present.