FRAUD CASE STUDY – THE TONE AT THE TOP AND FRAUD

Case

An alert employee at the Defense Reporting Office (DRO)[1] overheard a senior management official discussing employees' personal information and potentially using the information for fraudulent activity. The management official was on the phone discussing a plan to obtain credit cards in other people's names and changing the prospective victim's address on the applications. The address change was necessary so that the credit cards statements would not arrive at the victim's residence, making them unaware that the fraudulent activity was initiated. This type of fraud struck a nerve with the employee who overheard the conversation because they had become a victim of identity theft nearly two years ago.

Given the severity of the situation and who it involved, the employee decided it would be best to initiate an allegation with the DRO Hotline office. The Hotline office forwarded the allegation to the DRO personnel responsible for investigating allegations of misconduct by senior management officials. A team of auditors and investigators were assembled to determine whether the allegations could be substantiated.

Auditors found personally identifiable information (PII) maintained by DRO included, but was not limited to, education, financial transactions, address, social security number, date and place of birth, and mother's maiden name. As part of the investigation, the auditors had to determine:

- What controls were in place to protect an employee's PII and

- What standards of conduct were established at DRO to guide the directives, attitudes, and behaviors of the organization in order to achieve the entity's objectives.

The auditors determined that DRO did have policies and procedures in place for protecting the confidentiality of PII and to ensure access to PII was limited to those who had a need for the information in the performance of their official duties. However, the opportunity to commit fraud existed because management officials were capable of overriding the controls. Also, the auditors determined that DRO had not established standards of conduct to guide the attitudes and behaviors of the organization. Thus, employees were not aware of any expectations concerning integrity and ethical values.

After the investigators obtained a search warrant for the manager's computer, it was discovered the manager had accessed personnel databases numerous times and this usually occurred after working hours. The manager confessed to obtaining credit cards in eight DRO employees' names and implicated two subordinate employees. During questioning, the two employees stated they got involved in the scheme (sharing their passwords to personnel systems with the manager and providing documents containing PII), because of the conduct they observed from management and they feared retaliation if they did not participate.

[1] The Defense Reporting Office is a fictitious organization and was created only for this fraud case study.

As a result of their actions, the manager and two employees were fired from their jobs, and eventually convicted of credit card fraud and identity theft crimes.

The Tone at the Top Failed to Support the Internal Control System

The tone at the top can be either a driver or a barrier to internal control. In this case, the fraud was perpetrated by intentional override by senior management of what might otherwise appear to be effective internal controls.

Lack of Integrity and Ethical Values

The management official involved in the fraud scheme failed to demonstrate the importance of integrity and ethical values through their attitude and behavior. The following attributes should be considered because they contribute to the design, implementation, and operating effectiveness of demonstrating commitment to integrity and ethical values:

- Tone at the Top

  Management sets the tone at the top and throughout the organization by their example. Even though the opportunity to override internal controls may exist, senior management must know that it is wrong to override the controls for an unethical purpose. If not, otherwise effective internal controls cannot be relied upon to prevent, detect, or deter fraudulent activity perpetrated by senior management.

- Standards of Conduct

  Organizations should establish and use the standards of conduct as a benchmark for assessing whether the tone at the top and management's actions are those necessary and sufficient enough to maintain the highest levels of integrity. Establishing standards of conduct is vital to any organization, especially when management and employees can be faced with the pressure and opportunity to commit fraud.

- Adherence to Standards of Conduct

  Management can use established standards of conduct as the basis for evaluating adherence to integrity and ethical values across the organization. As a result, management can be able to address any deviations in a timely manner.

Auditors' Recommendations for Fraud Prevention and the Tone at the Top

Setting the appropriate tone at the top cannot come without communication. The auditors recommended that DRO establish standards of conduct to communicate to employees the expectations concerning integrity and ethical values. The standards of conduct should explicitly state what is and is not acceptable behavior. The auditors also recommended periodic training on the organization's core values, covering:

- What constitutes illegal/fraudulent behavior,
- Employees' responsibility to report fraudulent behavior,
- How to report fraudulent or suspicious behavior.

What to Monitor

- Management can use established standards of conduct as the basis for monitoring and evaluating adherence to integrity and ethical values across the organization. As a result, management can be able to address any deviations in a timely manner.

- Training requirements – Ensure employees are up to date on learning about ethical practices and their responsibility to report fraudulent behavior.

Fraud Indicators

- Management override of controls
- Sharing of passwords
- Excessive log-ins to PII/ personnel database after working hours