FRAUD CASE STUDY – MILITARY REFERRAL BONUSES

Case

A retired military service member, who was aware of a weak internal controls system for a military referral bonus program, took advantage of the opportunity to defraud the government of nearly $1.5 million. The military service member created a website to appear like an official military website for the AAFN Services Recruitment Program[1] and was able to gather the names of individuals who were interested in joining the military. The recruiting program was started to ensure recruitment goals were being met and it offered monetary incentives to soldiers (active and retired) that referred others to join the military.

Using information (names, addresses and Social Security numbers) of potential soldiers obtained through the fictitious website, the military service member was able to falsely claim responsibility for referring potential soldiers to join the military. As a result, the military service member received up to $2,000 for each recruit that was "referred."

After a year online, military officials flagged the existence of the website, but only after auditors and a Fraud Prevention Task Force questioned its function. The auditors also identified the recruitment program as a military program that was vulnerable to fraud because of an inadequate internal control system.

During their review, the auditors found the military service member was receiving money for recruits that had already been sponsored through a legitimate military recruiter. Other circumstances identified in this case included:

- Recruiting bonuses were frequently going into the same bank account.
- The military service member significantly made more referrals than anyone else; there was no cap on the number of referrals an individual could make.
- No one ever questioned whether the military service member had ever talked to or interacted with the potential recruits.

Federal prosecutors indicted the military service member for illegally obtaining fraudulent recruiting bonuses. The Program was discontinued and management officials were advised to enhance the controls and policies to better safeguard against future recruiting schemes if they decided to bring the Program back.

[1] The AAFN Services Recruitment Program is a fictitious program and was created solely for the purpose of this case study.

Control Activities that Should Have Been Considered and Implemented

Simple control activities that should have been considered and put in place to mitigate the fraud include:

- Establishing a cap on the number of recruits a sponsor could refer.
- Implementing requirements for the sponsor to mentor or meet with their recruit; all the perpetrator had to do was forward the names and information of the recruits to ultimately be paid.
- Flagging duplicate payments before bonuses were disbursed - lookout for duplicate names and SSNs that indicates a payment for the same recruit.

Response to Risks if the Program is Reinstated

When implementing the recruitment program, management officials failed to consider the potential for fraud. While fraud risk may be greatest when all three risk factors (pressure, opportunity, and rationalization) are present, one or more of these factors may indicate a fraud risk.

If the Program is to be launched again, management must design controls that can detect errors, and makes fraud more difficult to occur. In this case, a proper risk response may be reduction. Reduction is action taken to reduce the likelihood or magnitude of the risk involved. Examples of reduction include:

- Establishing a limit on the number of recruits a sponsor could refer.
- System checks to determine whether a recruit has already been sponsored in another recruiting program.
- Documentation verifying the recruiter and sponsors interacted with each other.

Since internal control is a dynamic process that has to be adapted continually to the risks and changes an entity faces, ongoing monitoring of the internal control system should occur to ensure the internal controls remain aligned with changing risks.

W**hat to Monitor**

- How many times a sponsor submits a referral.
- Those who significantly make more referrals than anyone else.
- Whether a recruit's name shows up in other recruiting systems.

Fraud Indicators

- Sponsors name shows up more frequently than others.
- Recruiting bonuses are repeatedly going into the same bank account.
- Duplicate payments made for a recruit with the same name and SSN.