ACCTG 533: Module 14: Asset Misappropriation Fraud

[Slide Content]:

Asset Misappropriation Fraud

[Jeanne H. Yamamura]:

Asset Misappropriation Fraud

[Slide Content]:

Asset Misappropriation Fraud

- *Theft or misuse of company assets*
- *Most common type of fraud*
- *Every type of organization*
- *Will repeat unless*
    - *Steps taken*
    - *Controls put in place*

[Jeanne H. Yamamura]:

Asset misappropriation fraud is fraud involving theft or misuse of company assets. It remains the most common type of fraud although it is not as expensive as the less frequent but much more costly financial statement fraud. It occurs in every type of organization from nonprofit to governmental to for profit and from small to large. It can occur over and over again unless steps are taken to prevent it from happening AND the controls put in place are maintained.

[Slide Content]:

2012 Report to the Nations on Occupational Fraud and Abuse

- *Median loss = $120,000*
- *12 to 36 months*
- *Discovered through tip*
- *Small Organizations*
- *55% Lack of internal controls, override of existing controls*
- *49% no recovery*

[Jeanne H. Yamamura]:

The 2012 Association of Certified Fraud Examiners (ACFE) Report to the Nation on Occupational Fraud and Abuse reported the following findings on fraud:

- The median loss for asset misappropriation was $120,000.
- The asset misappropriation frauds occurred over a long time - from 12 months to 36 months.
- Most frauds were discovered through a tip.
- Small organizations, defined as those with less than 100 employees, were the most common victims.
- Lack of internal controls and override of existing internal controls were the primary cause of 55% of the reported cases.
- 49% of the victim organizations did not recover any of their losses.

[Slide Content]:

Annual Fraud Loss

5% of revenues

[Picture Shown]

[Jeanne H. Yamamura]:

The estimate of annual losses resulting from fraud was 5% of an organization's revenues. Clearly, fraud takes a significant bite out of profits. For small organizations, a major fraud occurrence can result in the business having to close its doors. Most small businesses cannot afford any fraud loss, much less $120,000.

Because of this significance, it is important for managers to understand what asset misappropriation fraud is and how to prevent it within their organizations.

[Slide Content]:

Types of Asset Misappropriation Fraud

- *Theft of cash*
- *Submission of invoices (billing)*
- *Employee expense reimbursement*
- *Check tampering*

- *Payroll schemes*
- *Theft or misuses of company assets*

[Picture Shown]

[Jeanne H. Yamamura]:

We'll start with the types of asset misappropriation frauds.

Asset misappropriation fraud is limited only by human ingenuity. They include:

- Theft of cash (in many different ways)
- Submission of invoices for fictitious, inflated, or personal purchases. These are also known as billing schemes.
- Employee expense reimbursement for fictitious or inflated expenses
- Check tampering
- Payroll schemes
- Theft or misuse of company assets

The most common is theft of cash followed by invoice submissions.

[Slide Content]:

Fraud Perpetrators

- *Employees, managers, owners*
- *Higher authority = larger loss*
- *>75% accounting, operations, sales, senior management, customer service, purchasing*
- *2/3 male*
- *Under 26 to over 60; 54% 31 to 45*
- *HS diploma or less to post-graduate degree*
- *Clean employment history*

[Jeanne H. Yamamura]:

Who Commits Asset Misappropriation Fraud?

Anyone in an organization can commit fraud under the right circumstances. Rememeber the fraud triangle. When suffering from a real or perceived pressure, an employee with access to assets can perceive opportunity through a lack of controls and rationalize the fraud. Organizations that refuse to establish good internal controls are inviting fraud to occur.

The 2012 ACFE Report provided the following information on the fraud perpetrators:

- Frauds were committed by employees, managers, and owners.
- The higher the level of authority, the greater the loss.
- More than 75% of the frauds were committed by people working in six areas: accounting, operations, sales, senior management, customer service, and purchasing.
- 2/3 of the fraud perpetrators were male.
- Their ages ranged from under 26 to over 60. 54% were between the ages of 31 and 45.
- The educational background ran the gamut from high school diplomas or less to post graduate degrees.
- Most had clean employment histories – they had never been cited before with a fraud-related offense.

These findings simply confirm that fraud can be committed by anyone. So we need to know how best to prevent it.

[Slide Content]:

Fraud Prevention

Antifraud controls

- *Basic*
  - *Antifraud policy, code of conduct, management review, job rotation/mandatory vacation, hotline, fraud training for employees*
- *Expensive*
  - *Employee support programs, fraud training for managers and executives, external audit of FS and IC, audit committee*

[Jeanne H. Yamamura]:

The 2012 ACFE Report found that the presence of antifraud controls reduced fraud losses significantly. Organizations without antifraud controls experienced longer fraud durations and suffered losses 45% larger than organizations with antifraud controls.

Antifraud controls include very basic controls (which could easily be implemented by small organizations) as well as more expensive controls (more likely to be found only in large organizations). The basic controls included: having an antifraud policy, having a code of conduct, performing management reviews, having a job rotation/mandatory vacation policy and enforcing it, hotlines, and fraud training for employees.

More expensive controls included: employee support programs, fraud training for managers and executives, having an external audit of financial statements and internal controls, and having an independent audit committee.

[Slide Content]:

Hotline

- *Most common means of detection = tips*
- *Hotlines = more tips, more fraud detection*
- *Cost of hotline < cell phone or cable TV subscription*

[Picture Shown]

[Jeanne H. Yamamura]:

As the most common means of detecting frauds is through tips (from employees, customers and others), a hotline is quickly becoming an essential antifraud control for every organization. Organizations with hotlines received more tips and detected more frauds as a result. While it sounds expensive, the cost of hotlines is coming down – one estimate indicated that you would spend more on your cell phone or cable TV subscription than on a hotline.

[Slide Content]:

Small Businesses

- *Fraud victim more often*
- *Greater fraud losses*
- *Less ability to recover*
- *Proactive stance important*

[Picture Shown]

[Jeanne H. Yamamura]:

Small businesses are victimized by fraud more often and suffer greater fraud losses. They also have less ability to recover from fraud losses. It is important then that small businesses be more proactive in their antifraud efforts. Specifically, investing in a hotline, training employees in fraud prevention, setting the right tone at the top, and identifying the areas of greatest fraud risk and implementing controls over those areas.

[Slide Content]:

Behavioral Red Flags

- *Lifestyle*

- *Financial difficulties*
- *Vendor/customer closeness*
- *No job duty sharing*
- *No vacation*
- *Irritability, defensiveness*
- *Complaints*
- *Family/legal/addiction problems*
- *Wheeler/dealer attitude*

[Picture Shown]

[Jeanne H. Yamamura]:

Fraud perpetrators consistently exhibit one or more behavioral red flags. Fraud training should include identification of these common red flags and encourage consideration of such behavior especially when noted along with other discrepancies.

These include: living beyond one's means, experiencing financial difficulties, being unusually close to vendors or customers, reluctance to share duties, unwillingness to take vacation, irritability or defensiveness, complaints about pay or authority, family/legal/addiction problems, and a wheeler/dealer attitude.

[Slide Content]:

Cybercrime

- *Fraudulent bank transfers*
- *Lifestyle Forms & Displays, Inc.*
  - *$1.2 mm*
  - *Recovered $1.04 mm*
- *Small organizations easy target*
  - *Firewall and antivirus software*
- *Dedicated bank computer*
  - *Install operating software*
  - *Ban email access*

[Picture Shown]

[Jeanne H. Yamamura]:

The latest threat to organizations is that of cybercrime. An increasing number of organizations are reporting fraudulent bank transfers from their accounts. For example, Lifestyle Forms &

Displays, Inc. reported $1.2 million stolen through unauthorized transfers. The transfers went to the Bank of America, Wells Fargo, JP Morgan Chase, and Agricultural Bank of China in May 2012. Through diligent efforts, Lifestyle was able to recover $1.04 million. The remainder, however, was lost. This recovery is not usual. Business accounts are not covered by FDIC insurance. Banks have taken the position that it is the victim's fault for allowing the fraud to occur and thus they do not have to reimburse fraud losses.

Unfortunately, as in the case of other asset misappropriation frauds, small organizations are easier targets and thus more vulnerable to cybercrime. Their main lines of defense are typically a firewall and antivirus software. As in Lifestyle's case, these are inadequate to prevent cybercrime from occurring.

Ira Victor, an information security specialist, recommends that organizations use a dedicated computer for bank transactions. You start by installing a fresh version of the operating software, Windows or Linux, and ban any email access. This computer is then utilized solely for banking.