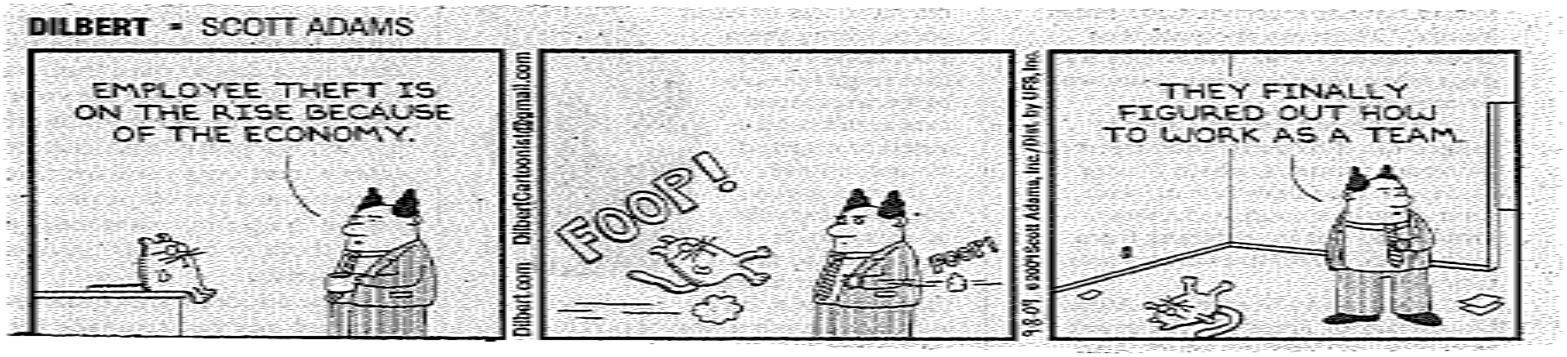
Internal Fraud Monitoring & Investigation Best Practices

By Tom Holland, CFE

The Threat Within



- **Internal fraud is an ongoing concern and by many indications is growing**

- **There are a number of factors contributing to the increase**

- **There's more at stake than the actual fraud losses**

Preventing Internal Fraud

- **Tone from the top**
- **Strong and comprehensive code of ethics**
- **Strong system of internal controls**
- **Periodic risk assessments**

Preventing Internal Fraud (continued)

Know who you hire by performing background screenings:

- **Criminal Background Screens – required by Section 19 of the Federal Deposit Insurance Act (12 U.S.C. 1829)**
  - **Federal banking agencies (i.e. Federal Reserve, Office of Thrift Supervision, etc.) enforcement sites must be verified**
  - **The Internal Fraud Prevention Service – subscription service listing individuals released by other banks for knowingly causing or attempting to cause financial loss**

- **Financial review – subject to Fair Credit Reporting Act requirements, consult your legal department**

- **Education and employment**

Detecting Internal Fraud

Reporting suspected or known unethical practices and behavior has to be an easy process:

- **Ethics hotline**

- **Promote the use of multiple channels**
  - **Internal phone numbers**
  - **Internal email**
  - **Intranet**

Detecting Internal Fraud (continued)

There is a number of internal fraud detection software tools available to detect unusual/suspicious employee activity. Optimally, the software should be able to identify suspicious transactions and/or employee behavior:

- **Transactional analysis identifies unusual/suspicious transactions regardless of who owns the account**

- **Behavioral analysis identifies patterns of activity of a system user which fall outside the range of normal activity for a pre-defined group such as tellers**

Detecting Internal Fraud (continued)

Existing management reports should also be used to identify unusual/suspicious activity involving employees. These reports include:

- **Overdraft/non-sufficient funds**
- **Kiting**
- **Large/unusual cash transactions**
- **Waived fees**

Detecting Internal Fraud (continued)

Proactive investigations should be performed in areas susceptible to fraud, identified in risk assessments, and/or not covered by internal fraud detection software. Areas where proactive investigations can be effective include:

- **Payroll**
- **Travel and expense**
- **Accounts Payable**
- **Incentive programs**

Detecting Internal Fraud (continued)

Ongoing management reviews and observations play a significant role in detecting suspicious/unusual activity.

•Management, and for that matter, all employees, should be aware of operational and behavioral red flags that could suggest unauthorized and/or fraudulent activity

•No one red flag is necessarily an indicator of fraud or a problem

- **Questionable activity or transactions should be researched to understand what is occurring and why**

Detecting Internal Fraud (continued)

Operational/work environment red flags:

- **General ledger activity has increased without any apparent reason**
- **Average balances in general ledger suspense/float /work-in-progress accounts have been steadily increasing**
- **There is an unusually large number of missing deposits/credits in the general ledger suspense accounts**
- **There is an unusual number of aged general ledger suspense items**
- **General ledger accounts are not reconciled or are not reconciled in a timely manner**
- **Differences identified during reconciliations are not researched or documentation supporting how differences were cleared is not available**

Detecting Internal Fraud (continued)

Operational/work environment red flags: (continued)

- General ledger fee reversals are a larger percentage/ratio than fees collected
- General ledger fees are reversed from the same account(s) month after month
- There are unusual and/or large sundry operating losses without supporting documentation
- Expenses for local purchases of supplies, staff, entertainment of customers, etc. have increased for no apparent reason
- Receipts supporting expenses are missing or not original
- There are accounts controlled by the branch where there does not appear to be an appropriate business reason

Detecting Internal Fraud (continued)

Operational/work environment red flags: (continued)

- **There are branch accounts controlled by one individual**
- **The number/dollar amount of teller shortages is much larger than the number/dollar amount of teller overages**
- **There is a large number of teller shortage reversals on pay day, after holidays or after weekends**
- **Not all branch, teller drawer keys, etc. are accounted for and/or adequately controlled**
- **Poor internal controls or disregard of internal controls**

Detecting Internal Fraud (continued)

Operational/work environment red flags: (continued)

- Sales/marketing goals are unrealistic
- There has been an unusual number of similar customer complaints or complaints involving the same individual
- Certain customers insist that only a particular employee can assist them
- Vendor payments are not supported by invoices
- Vendor addresses are Post Office boxes instead of physical addresses
- Vendor invoices are sequentially numbered

Detecting Internal Fraud (continued)

Operational/work environment red flags: (continued)

- **Too much reliance is placed on one individual (i.e. the subject matter expert) without appropriate oversight**

- **Customer information such as loan files, signature cards, etc. is not effectively controlled, particularly after hours**

Detecting Internal Fraud (continued)

Behavioral/individual red flags:

- Employee is living beyond his apparent means
- Employee suddenly comes into a large sum of money
- Employee is consistently overdrawing his account and/or writing non-sufficient fund checks
- There has been a dramatic change in the employee's life (i.e. death, illness, marriage, divorce, birth of a child, etc.)
- Change, often dramatic, in the employee's personality
- Change, often dramatic, in the employee's lifestyle

Detecting Internal Fraud (continued)

Behavioral/individual red flags: (continued)

- **Employee's attendance pattern changes**
- **Other employees have raised concern about the behavior of a particular employee**
- **Employee is willing to work overtime without pay or historically resisted working overtime but is now willing to do so**
- **Employee is unwilling to take vacation or is willing to come in and work during vacation**
- **Employee is "protective" of certain customers and insists that he is the only one to assist these customers**

Detecting Internal Fraud (continued)

Behavioral/individual red flags: (continued)

- **Employee is involved in processing transactions and/or performing duties that are not within his normal scope of responsibility**
- **Employee is knowledgeable of functions/activities that are not within his scope of responsibility or not in line with his previous work history**
- **The same employee always performs or oversees certain key functions**
- **Employee has total disregard for internal controls and transaction authorities**

Investigating Internal Fraud

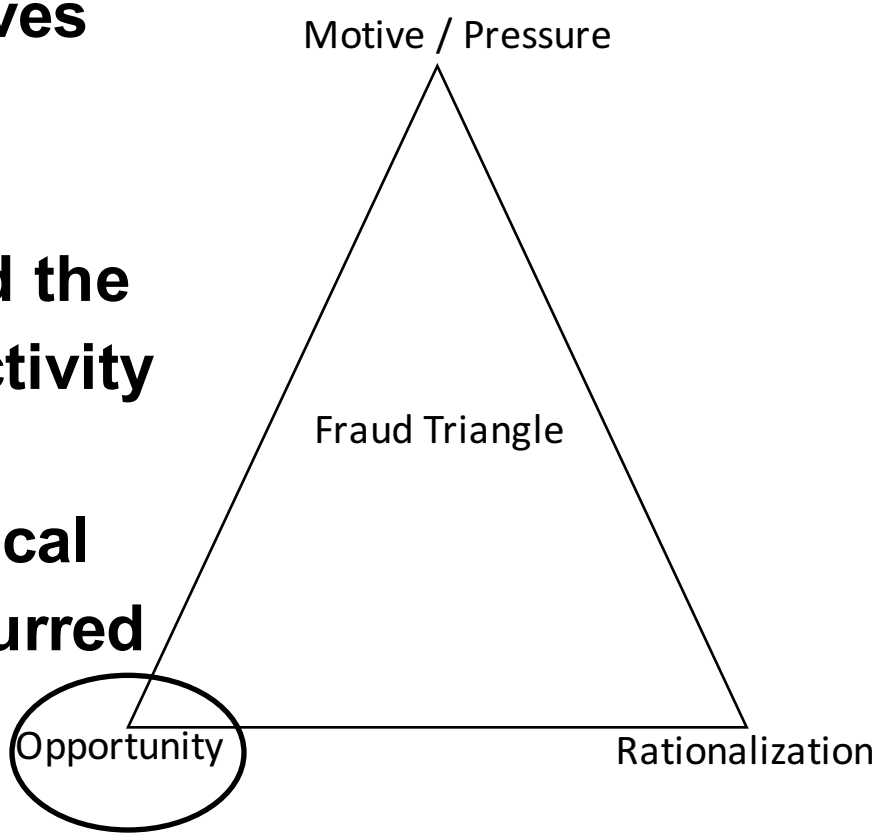
A successful internal investigation program should include the following base line requirements:

- **Independence**
- **Defined scope and responsibilities**
- **Documented standards and procedures**
- **A standard case management system**
- **Skilled staff**

Investigating Internal Fraud (continued)

There should be two objectives of every investigation:

- **Determining who committed the unethical or fraudulent activity**
- **Determining how the unethical or fraudulent activity occurred or went undetected**



Investigating Internal Fraud (continued)

Conducting the investigation …

- **The first step is developing an Investigation Plan**
  - **The Investigation Plan is the formal framework as to how the investigation will proceed**

- **The investigation fieldwork is the means by which the Investigation Plan is completed and investigation objectives are achieved**

- **Ongoing communication with key stakeholders is critical to ensuring an effective and efficient investigation**

Investigating Internal Fraud (continued)

Interviewing the investigation subject …

- **An Interview Plan should be developed for every interview**
- **Potential outcomes and actions to be taken should be discussed and agreed upon before the interview**
- **There should always be three individuals in the interview; the investigator, the subject, and the witness**
  - **At the conclusion of the interview, obtain a written statement and ask for the money**

Reporting and Analyzing Results

- **At the conclusion of every investigation, a report and, as applicable, a Suspicious Activity Report (SAR) should be prepared**
  - **The report and the SAR narrative should, in summary, tell the story of who did what, when, and how**
- **Management reports summarizing investigation activity should also be produced periodically**
- **Trend analyses should also be performed periodically to identify systemic issues not readily identified in individual investigations**

Concluding Comments …

While none of us wants to see fraud, it's going to occur; we need to proactively plan for it and manage it:

- **Set expectations … the tone from the top**
- **Establish a strong system of internal controls**
- **Know who you hire … background investigations**
- **Monitor activity … various detection tools and programs**
- **Know the signs of potential fraud … red flags**
- **Define and document your investigation program**

Questions and Contact Information

?

Tom Holland, CFE
tgholland3@msn.com
804.972.5390