Disclaimer of Liability

Weaver provides the information in this presentation for general guidance only, and it does not constitute the provision of legal advice, tax advice, accounting services, investment advice or professional consulting of any kind. The information included herein should not be used as a substitute for consultation with professional tax, accounting, legal or other competent advisers. Before making any decision or taking any action, you should consult a professional adviser who has been provided with all pertinent facts relevant to your particular situation. The information is provided "as is," with no assurance or guarantee of completeness, accuracy or timeliness of the information, and without warranty of any kind, express or implied, including but not limited to warranties of performance, merchantability and fitness for a particular purpose.
Pictures of Employee Fraud
From 1998 to 2010, used names and personal information to create 58 fictitious loans

Defrauded bank of approximately $2.4 million

Fraud detected during loan review conducted after bank sale

In June 2014, at age 65, was sentenced to 41 months in federal prison and ordered to pay restitution of $4.5 million
Former bank teller in White Plains, New York

- Participated in identity-theft ring which, from 2010 to 2014, stole personal information from bank transactions to create fake identification cards used to withdraw money directly from accounts.
- Defrauded bank customers of more than $850 thousand
- In May 2015, at age 24, was sentenced to two to six years in state prison
Sandy Jenkins Case

Former corporate controller with Collin Street Bakery in Corsicana, Texas

- Had been with company since 1998
- From 2005 to 2013, paid personal expenses through accounts payable, voided these checks, and reissued to actual vendors. Also, stole from petty cash
- Defrauded company of approximately $17 million
- Fraud discovered after an assistant discovered a check made payable to an unknown bank
- In September 2016, at age 66, was sentenced to ten years in prison and ordered to forfeit assets
Jeanne Zacherl Case

Former accounts payable manager with chemical company in Hermitage, Pennsylvania

- Had been with company for 22 years
- From 2008 to 2012, created fictitious vendors and wired funds in these vendor names to personal bank account
- Defrauded company of approximately $1.1 million, which she lost at a local casino
- Fraud discovered after bank officers notified the company of suspicious transactions in personal accounts
- In October 2013, at age 64, was sentenced to up to five years in prison
Former executive director of environmental health and safety with Kennesaw State University in Georgia

- Had been with the university since 2001
- From 2003 to 2012, created shell companies and fake contracts to submit invoices for work never performed; as director, he approved contracts and invoices
- Defrauded university of almost $1 million
- Fraud was discovered in an investigation stemming from informant’s tip
- In November 2014, was sentenced to three years in prison and ordered to pay almost $700 thousand in restitution
Former mail processor with United States Postal Service

- From 2003 to 2004, submitted **falsified jury duty documentation** and was paid for 144 days of jury service he never performed
- Fraudulently received $31 thousand in pay
- In 2006, he attempted to repeat the scam but was caught after 40 days and $7 thousand
- Fraud detected after supervisor became suspicious
- In 2008, received a short prison sentence and ordered to repay $38 thousand
Five Key Takeaways from Fraud Cases:

1. Perpetrators were “trusted” employees who were familiar with the control environment.
2. Frauds executed over period of years.
3. Individual fraudulent transactions were relatively small, or “below the radar”.
4. In non-bank environments, accounts payable was most common method of transacting fraud.
5. In bank environments, opportunities for transacting fraud are abundant (loans, teller cash, wires, transfers, accounts payable).
Banking and financial services was the industry group with the highest reported fraud cases at 17.8%.

For the cases reported, the median duration from the time the fraud commenced until it was detected was 18 months.

Highest reported fraud: Banking and financial services

Time from crime to report: 18 months
The median fraud loss was $145,000. With 22% of cases having losses of at least $1 million.
More than 40% of fraud cases were detected by a tip — twice the rate of any other detection method.
Hotlines Work

✓ Organizations with hotlines were much more likely to identify fraud by a tip

✓ These organizations:
  ➤ Had fraud that was 41% less costly
  ➤ Detected frauds 50% more quickly
Considering Employee Fraud in Audits
Audit Considerations

- Consider the overall **“tone” of management and general attitudes** toward internal controls

- In **brainstorming**, consider how employee fraud could be conducted within the function being audited

- Build an **employee fraud risk profile**

- **Pay attention** to behavior and lifestyle hints of employees being audited
  - Feelings of being unfairly treated
  - Having been emotionally hurt by a colleague resulting in desire for revenge
  - Having financial difficulties
  - Living a lifestyle inconsistent with salary
Audit Considerations

► Determine how cash leaves the organization
  - Accounts payable
  - Wire transfer
  - Payroll
  - Loans
  - Physical cash

► Evaluate effectiveness of disbursement-related controls
  - Dual control
  - Approval
  - Review and monitoring
  - Reconciliations
Audit Considerations

► Increase scrutiny of disbursement-related functions in which **one employee** is solely responsible
  - Job duties are not rotated
  - Tasks are not performed by a second employee if primary employee is out
  - Transactions are not subject to effective secondary review
  - Transactions are not subject to effective reconciliation and cost-center income/expense review

► Recognize the limitations of sampling, and consider **data mining**
  - Define fraud attributes
  - Analyze population for defined attributes
  - Evaluate each “hit”
Audit Considerations

► In testing, be mindful of **smaller transactions** that may not be completely “normal”

► If fraud is suspected or detected, then utilize a **qualified forensic specialist**
  - Inappropriate interview or investigation techniques could jeopardize the case against the fraudster

Above all, be skeptical...

...especially of the longest-term, most knowledgeable, most helpful and friendliest employees!
“Trust but verify.”
Managing Employee Fraud Risk
Fraud Controls

► Establish **clear code of conduct** and guidelines for conflicts of interest
  ➡ Ensure employees receive fraud and ethics training and confirm their understanding of guidelines at least annually

► Formally **consider employee fraud risk** in departmental risk assessments
  ➡ Document how employee fraud could occur and what controls mitigate that risk

► Establish an employee **fraud hotline** to report suspicious activity
  ➡ Hotline reporting should go to an independent party and/or to the audit committee
Fraud Controls

- Establish a mandatory consecutive-day vacation policy
  - Policy should require minimum number of consecutive days of vacation to be taken per year
  - Monitoring for compliance with policy can be conducted by Human Resources

- Perform reconciliations of all balance sheet and internal DDA accounts
  - Frequency should be appropriate based on level and nature of activity
  - Reconciling items should be dated and adequately documented
  - Secondary review should consider accuracy, completeness, and reasonableness of both activity and reconciling items
Fraud Controls

► Perform **analytical review** of income and expense accounts
  - Variances from budget and prior period should be subject to research and explanation to appropriate officer or committee
  - To mitigate risk of smaller transactions being undetected, establish a review and the appropriate cost center level

► Establish **disbursement controls**
  - Require tiered approval for disbursements based on amount and/or nature of disbursement; approval should consider accuracy, completeness, and validity
  - For electronic transfers (such as wire), implement system-enforced dual control

► Periodically **rotate assignments** of routine duties
Information Technology
Fraud Controls

► **Restrict system access**
  - Limit the ability to authorize, approve and override transactions to the fewest number of individuals who require the function for their job responsibilities

► **Develop segregated roles in the system**
  - Establish to prevent an individual from being able to bypass controls built into the system/application
  - Separate any one user’s ability to initiate and approve (or override) within the system

► **Use application controls**
  - Configure automated controls to require a second approval before proceeding, or triggering a supervisor approval for transactions above established thresholds
Perform **file maintenance review** related to new clients, vendors, employees

- Perform a periodic review of newly established or modified master data files for unusual changes

Perform **data analytics** over specific transactions

- Periodically review unusual activity (such as transactions that are initiated outside of normal business hours or by individuals who do not typically perform a function)

Establish and **review activity logs** for specific events

- Periodically review abnormal activities (such as overriding a control step or approval)
Discussion

James Mihills, CPA
(817) 882-7361 | james.mihills@weaver.com