FRAUD AND INTERNAL CONTROLS

MARCH 22, 2017 3:15 – 4:15PM

Presenters:

Jaclin B. Krumrine, PRSBA, CPA, MBA
CFO, Owen J. Roberts School District

Krista M. Gardner, CPA
Principal, Stambaugh Ness, PC

Purpose

- Learn about fraud
  - What is it?
  - Considerations
  - How can I safeguard my organization?

- What is Fraud?
  - The crime of using dishonest methods to take something valuable from another
  - Deliberate action by an individual or entity to cheat another, causing damage
    - Misrepresentation
    - Concealment
    - Improper manipulation
    - Nondisclosure of a material fact
    - Misleading conduct

Internal Fraud

- Employees commit fraud against the organization they work for
  - Payment fraud
  - Procurement fraud
  - Occupational fraud (paid for unworked hours, "time stealing")

  All levels of employees from entry level staff, to managers, officers, executives

External Fraud

- Vendors
  - Shipping scams
  - Employee collusion (bribes, kickbacks, dummy accounts)
- Customers
  - Bad checks
- Hackers
  - Accessing systems to steal funds or confidential data

- Banking
- Technology
- Internal Controls
- Communication / Education

Banking

- Is your bank's website secure?
- Work with your banking representatives to safeguard online banking
  - Debit Block Protection
  - Positive Pay
  - Account Reconcilement services
- Set up proper limitations for online transactions
  - Automatic very low limits - $1, if the account is hacked low limits help ensure safety of funds

Banking

- Only key employees should process confidential transactions (ACH, wires, transfers)
- Set up proper security levels for internal users
- Dual authorizations (can be internal layers, and/or bank layers)
  - Examine your bank's website controls
  - Segregated authentications
    - Random number generators in conjunction with confirming phone call (code by phone)
    - Second layer – District confirmation back to bank

Banking

- Paying vendors via ACH or wire?
  - Request voided check from vendor, CONFIRM account and routing number is valid with receiving bank
    - Ensure your Payee and the Account Holder are the same entity
    - Send transactions with a pre-note to ensure account information is correct
- Review online transactions a few times per week
- Know who to contact if you see anything suspicious

Technology

- Store user IDs and passwords in a safe place
  - Choose passwords carefully
  - NEVER allow a website to store your logon information
  - Change your passwords frequently (every 90 days)

Technology

- Are you where you thought you were?
  - Review the address bar, is it correct? Were you re-directed to another site?
    - Is the organization name displayed properly (i.e. Fulton Bank) and free of errors
    - Check the extension at the back of the address
    - Look for the lock symbol in the address bar indicating you are on a secure site
    - ALWAYS logout of a website rather than just closing the browser window
      - Secure sites will automatically log you out after a period of inactivity (session has timed out)

Technology

- Do not open suspicious texts, emails or pop-up windows – delete them
- Work with your IT Department to educate staff members
  - Online – key logger scams
  - Know how to spot a fake:
    - Generic greetings
    - Poor grammar and/or spelling
    - Overly official tone or forced language

Technology

- Ensure data is secure and protected
  - Employee data
  - Student data
  - Who has access?
    - Electronically
    - Paper
- Update anti-virus software frequently

Internal Controls

- Written fraud policy – ensure employees know there is zero tolerance for fraudulent behavior
- Adopt a Whistleblower policy if you don't already have one
- Set an example of honesty and ethics – ensure employees understand these expectations
- Code of Conduct – Tone at the Top

Internal Controls

- Say NO….to petty cash
  - Skimming, cash larceny
- Deposit daily
- Automate collections
  - Online solutions: meal accounts, field trips, book fines, activity fees
- Setup internal controls with segregated duties
  - Consider staff size and abilities
  - Make changes as necessary; fraud is less likely to occur or remain hidden when different sets of eyes are looking at things

Internal Controls

- Automate receivables and related cash receipts
  - Review outstanding A/R reports regularly
  - Setup controls for posting and review of transactions
  - Ensure posted transactions cannot be deleted
  - Who can post an A/R credit memo? Shouldn't be someone who is handling the cash receipts

Internal Controls

- Tax Collections – review Tax Collectors process
  - Turn collections & records over to District timely
  - Consider collecting through bank lockbox
    - Immediate investment of funds
    - Associates costs are usually very worth it – solicit several banks for competitive pricing
  - Reconcile tax collections timely so any discrepancies can be addressed before they are stale

Internal Controls

- Reconcile Bank Accounts timely
  - Segregation of duties – one employee performs reconciliation, supervisor reviews
  - Always review cashed check images – look for Check Tampering Schemes
    - Forged Maker schemes – forging an authorized signature on a company check
    - Forged Endorsement – forging the signature endorsement of an intended recipient
    - Altered Payee – changing the payee on the check to the perpetrator or accomplice
    - Authorized Maker – employees with signature authority write fraudulent checks for their own benefit

Internal Controls

- Accounts Payable – segregation of duties
  - Dependent on staff size; segregate entry and posting
  - Segregate check processing; employee who is not responsible for data entry should match and distribute checks
  - Supervisor review check run / check register
  - Include monthly check register in Board reports
    - Business Administrator / CFO perform random monthly review from Board check register

Internal Controls

- Procurement Cards
  - Set daily / monthly / per purchase limits for users
  - Review cardholder list regularly
    - Update regularly for terminated cardholders, etc.
  - Set approval codes for where each card can make a purchase
    - Example – Maintenance Dept cardholders can purchase from home improvement stores
    - Never allow cash advances to be enabled

Internal Controls

- Department Supervisor review and approval of procurement card activity on a weekly / bi-weekly basis
- Accounting supervisor review and approval of monthly activity
  - Interim Accounting staff monitoring of transactions; collection and reconciliation of receipts

Internal Controls

- Set proper security levels for internal users (in-house software and online)
- Review financial system change log / audit log periodically
- Ask your local auditors for suggestions – how can your processes be improved? Can they identify any weaknesses?
- Check with your insurance agent about what fraud coverage your district may have. Don't have any? Consider adding it!

Communication / Education

- Everyone learns from real life examples. Inform staff members of fraud attempts you've learned about at other organizations.
  - Engage – allow opportunities for staff to consider how their role in the organization can help prevent/mitigate fraudulent activity
  - Educate: yourself AND staff
    - Be aware of latest scam attempts
    - Listen….and repeat to staff. School organizations are very good about sharing their experiences.

Communication / Education

- Impersonator Scams
  - Superintendent email / Business Administrator email
  - W2 file requests
  - Insurance subscriber requests
  - Do not be afraid to confirm the origin of a request before honoring it

Communication / Education

Small changes can yield large advantages. You may not want to or be able to implement everything discussed in this presentation, but making just one improvement can make a huge difference in protecting your organization.