

Roman Catholic Diocese of Raleigh



Financial Fraud Risk and Risk Mitigation for Parishes and Schools

Headlines

Former assistant Catholic superintendent in
Washington archdiocese accused of fraud

Woman accused of embezzling \$100K from church
in Rutherford Co.

Priest convicted of fraud, theft returns to Ottawa
ministry

Church employee embezzled more than \$400,000
from Blue Springs parish, officials say



The Data

Each year, the Association of Certified Fraud Examiners conducts a global study on occupational fraud and abuse. The 2018 study included 2,690 fraud cases from 125 countries across 23 industries.

Source: ACFE Report to the Nations 2018 Global Study Occupational Fraud and Abuse



The Data

The study identified the following:

- The average loss per fraud case = \$130,000.
- For business with 100 or more employees, the average loss = \$104,000 per fraud case.
- For small businesses of less than 100 employees, the average loss = \$200,000 per fraud case.
- Average duration of fraud scheme = 16 months.
- 89% of cases involve asset misappropriation.



The Data

- Half of the frauds identified resulted from internal control weaknesses.
- 85% of fraudsters exhibited at least one behavioral red flag; 50% exhibited multiple red flags.
- 96% of fraudsters had no prior fraud convictions.
- Initial fraud detection methods:
 - 40% tips; more than half of all tips come from employees
 - 15% internal audit
 - 13% management review

Source: ACFE Report to the Nations 2018 Global Study Occupational Fraud and Abuse

Diocese of Raleigh



The Data

- Common fraud risk areas for small organizations:
 - Check and payment tampering
 - Expense reimbursements
 - Skimming
 - Cash on hand
 - Noncash assets
 - Financial statement fraud
 - Cash larceny
 - Payroll

Source: ACFE Report to the Nations 2018 Global Study Occupational Fraud and Abuse



Internal Control Red Flags

- Lack of segregation of duties within the organization including an/a:
 - Overreliance on or trust in one individual to manage the finance process from start to finish without proper mitigating controls in place.
 - Individual who generates checks is also a check signer.
 - Insufficient or no management review of check.
disbursements and related supporting documentation, such as invoices, receipts, contracts and payroll registers.
 - Lack of management review of bank statements before they are opened and bank-to-general ledger reconciliations by a party independent of the check generation function.



Internal Control Red Flags

- Lack of financial transparency/reporting to management
- Missing or not original vendor documentation for purchases on file
- Lack of systems or logical access internal controls
- Use of bank debit cards
- Use of signature stamps



Behavioral Red Flags

- An individual who:
 - Appears to be living beyond his/her means, i.e. travel, cars, clothes, meals, etc. that are not commensurate with income.
 - Is experiencing a financial hardship.
 - Is inordinately possessive over financial records and functions.
 - Never takes a vacation or insists financial duties are put on hold while gone.
 - Is going through a divorce or experiencing family issues.
 - Exhibits a “wheeler-dealer” attitude.
 - Has unusually close relationships with vendors.



Risk Mitigation Goals

- Protect the financial assets and reputation of the parish / school
- Maintain the trust of the parish / school community
- Protect the pastor, principal, staff and volunteers from false accusations
- Provide accurate and reliable financial information
- Detect and correct errors
- Detect and address misappropriation of funds



Risk Mitigation Tools

- Zero tolerance policy on financial misconduct
- Code of Conduct and employee acknowledgment of consequences of violating policies or conducting fraudulent activity
- “Whistleblower hotline” – providing employees with the names of individuals within the organization to whom they can confide concerns regarding possible fraud
- Recognize behavioral red flags
- Prompt response to fraud allegations and action when fraud is identified



Risk Mitigation Tools

- Documented policies, procedures, and requirements
- Management governance and oversight
- Regular internal audits
- Establish a strong internal control environment including targeted preventive and detective anti-fraud controls over cash receipts and disbursements including:
 - Segregation of duties throughout the financial process, from receipt through to disbursement of funds.
 - Dual control over uncounted funds, especially offertory.
 - Timely and intact deposit of funds.



Risk Mitigation Tools

- Limited access to the safe and change of combination as needed.
- Checks never pre-endorsed or made out to “Cash”.
- Review and approval by the pastor or his designee, who may not also be the person who generates the checks, of:
 - Invoices, credit card statements and reimbursements before a payment is generated.
 - Bank-to-general ledger reconciliation, including a review of cancelled checks.
 - Payroll registers and salary change reports.
- Declining/destroying checking account debit cards.
- Maintaining physical assets:
 - Tracking of keys and security codes issued to access facilities.
 - Documentation and regular review of assets in inventory.



Case Study 1



Case Study 1

What happened?



Case Study 1

- Director of finance embezzled ~\$200,000 of parish funds over the course of 21 months.
- Director of finance:
 - As payroll administrator, increased his salary in the payroll system without authorization.
 - Used the parish credit card to pay for personal meals, travel and entertainment, clothing, apartment rent, and gifts.
 - Issued checks to himself for consulting work he did not perform and forged the pastor's signature on those checks.
- Several behavioral red flags were evident.



Case Study 1

- To cover up the fraud, the director of finance:
 - Manipulated entries in the accounting system throughout the majority of the scheme until the last few months when he did not enter any data for financial transactions into the accounting system at all.
 - Made unauthorized online bill payments for the credit card balance before the payment was due to allow for additional spending and make the balance due on the statement closing date appear within reason for the parish.
 - Destroyed bank and credit card statements which reflected the unauthorized online bill payments for the credit card balance due, the fraudulent checks for consulting work containing the pastor's forged signature, and the vendor names and locations at which unauthorized purchases were made.
 - Provided falsified financial reports and bank reconciliations to the pastor and parish finance council for review.



Case Study 1

- During a review of payroll documentation to familiarize himself with parish operations, the incoming pastor noticed a discrepancy between the authorized annual pay increase for the director of finance and the actual amount being paid.
- The incoming pastor also identified the lack of bank and credit card statements on file and immediately requested the documents from the vendors.
- Internal audit found checks issued by the finance administrator to himself containing the forged signature of the former pastor.



Case Study 1

**How could the fraud risks
have been avoided or
mitigated?**



Case Study 1

- Regular review of payroll registers, per Diocesan policy, and employee change and salary history reports by the pastor or finance council chair to identify unauthorized changes.
- Timely review of bank and credit card statements and bank reconciliations to identify extraordinary or unauthorized purchases/payments and forged signatures.
- Compliance with Diocesan policy for quarterly, at a minimum, management review of financial reports.
- Recognition of behavioral red flags.



Case Study 2



Case Study 2

What happened?



Case Study 2

- School principal embezzled \$18,000+ of school funds over the course of three years.
- School principal used the school credit card to make personal purchases for gift cards, electronics, clothing, food, and sports equipment for herself and her sons.
- To cover up the fraud, copies of vendor receipts were manipulated to reflect items purchased of a potential business nature.
- The school bookkeeper was circumspect of the supporting documentation and brought the concerns to the parish/school administrator's attention for further investigation.
- Staff and internal audit review found numerous instances of manipulated and manufactured receipts.



Case Study 2

**How could the fraud risks
have been avoided or
mitigated?**



Case Study 2

- Compliance with Diocesan requirement for original vendor receipts to support purchases.
- Closer review of receipts to identify purchases made out of state and during vacations.
- Review of vendor receipts received via email by the purchaser to identify discrepancies in fonts, unit prices and sales tax paid on the purchases.
- Visual confirmation of the electronics allegedly purchased per the receipts.
- Requirement that all electronics purchases be made by the IT specialist and recorded to the asset inventory.
- Recognition of behavioral red flags.



**For additional information regarding fraud risks
and risk mitigation or to report a concern,
please contact**

Christine Passaretti Norwood at 919.821.9713

Christine.Passaretti@raldioc.org

or

Russ Elmayan at 919.821.9704

Russ.Elmayan@raldioc.org

